Metatheme

Thought Leadership. Practical Solutions.

The Failure of the Concept of Risk and Risk Management Practices in Organizations

By Chris Tsalakopoulos

Founder and CEO, Metatheme Pty Ltd

Metatheme Pty Ltd
Foundation Paper
By Chris Tsalakopoulos
Founder and CEO, Metatheme Pty Ltd

July 2005

Metatheme Pty Ltd
PO Box 7175
St Kilda Rd, Central
Melbourne, VIC 3004
AUSTRALIA

ABN 59 093 956 882
www.metatheme.com
info@metatheme.com

Notice of Liability

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this book, Metatheme Pty Ltd shall not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the computer software and hardware products described in it.

Table of Contents

Chapter 1

Introduction

1 Setting the scene

As we move through the early stages of the 21st century, the organization as an entity is facing significant new challenges. These challenges are such that the organization must re-think key aspects about the way it understands its position in relation to its goals and objectives and it must re-think the way it makes decisions. Specifically, an organization will need to take greater account of the risks, threats and issues it faces on its paths forward. It will need to integrate this view of the road ahead more intimately into its understanding of itself and its decision-making. This new way of viewing and understanding must pervade every aspect of the organizations operations, not just senior management levels.

This new way of understanding the world will also create a subtle yet significant shift in the mindset and culture of the organization. Traditional forms of assessment will be augmented by new forms of thinking and language – the thinking and language of the forward view. The only candidate model through which we can build those new forms of thinking and understanding is through the concept of risk and the practice of risk management. But an important question needs to be asked. Is risk and risk management capable of delivering?

1.1 Purpose of this document

In this paper I will discuss the unique challenges facing organizations. I will contend that these challenges will necessitate a significant shift in an organization's approach to understanding itself and making decisions. That change in understanding and decision-making will require organizations to place greater significance on understanding and dealing with risk. Through the bulk of this paper I will argue that our current thinking and practices with risk, as it is applied in organizations, is severely flawed. I will examine the current approaches and show where the problems lie. I will contend that these problems are having a significant negative effect on organizations, especially when facing the challenges of today's world. I will conclude that ultimately, in its current form, the concept of risk and the practice of risk management are not able to provide organizations with the methods and tools to build the new ways of understanding and decision-making that organizations will require.

1.2 Challenges that are creating new conditions for organizations

There are three major trends that have emerged over the last few decades that collectively have created new conditions under which organizations must now operate. These trends can be categorized as:

- Increasing change
- The role of personnel in the organization
- Greater scrutiny of the organization

1.2.1 Increasing change

Through the streamlining of world trade and the rapid advancements in information technologies over the last 15 years, barriers to entry into almost every type of market worldwide have dramatically lowered. An organization can seem to appear from nowhere and create comparable or better quality products to established players. A new player can also very quickly ramp up and compete anywhere in the world; for example, in telecommunications (Virgin), low cost airline travel (Value Jet), High-end sports cars (Pagani Zonda, Noble), specialty finance (e.g. mortgage lenders), and information technology. This in a sense creates a 'hyper-competitive' environment, where new waves of products, competitors and markets develop constantly.

In today's world, change pressures are experienced constantly throughout an organization's sphere of operation. Mass production environments, which are best suited to situations of stability and predictability, are still common and important to world economies; however, even they are exposed to constant change pressures. These days, rarely does a facet of an organization's operations remain stable for years on end. New competitors appear, or existing ones change methods, new technologies create new approaches, organizations are re-structured, new processes are implemented, regulations change, suppliers change, customer behaviors and expectations change, new products emerge, and so on it goes without respite.

The organization must be able to thrive in this environment of constant change. Unpredictability and uncertainty are the ever-present reminders of this new envi-

ronment. Adding a further element of uncertainty to our world is global terrorism. This has the ability to quickly disrupt markets and economies and force the adoption of new methods of operation for organizations (e.g. new procedures in airport operations).

1.2.2 The role of personnel in the organization

A few decades ago, roles in most organizations were highly structured and controlled. Management at the top gave the orders, and the workers below carried out the precise instructions. Workers had little discretionary power. Demarcation was clear.

Through advancements in technology in the 1980s we began to see the first major changes to the arrangements of roles in organizations. Mundane and programmable tasks were taken away from humans. In some cases this left workers obsolete, and in other cases freed them to tackle more challenging roles. Gradually, work forces began to develop more information based skills and a greater need for judgment and decision-making in their day-to-day activities.

This 'up-skilling' of the work force was also encouraged by organizations. In the face of rapidly changing markets and environments, organizations began to see greater adaptability and flexibility in work forces as a necessity to success. This led to the delegation of discretionary powers further down the chain of command. Greater investment and training in staff became a key human resource activity. Terms such as the 'knowledge worker' became in vogue. Contracting and outsourcing also grew rapidly. Those that were once not viewed as part of management fabric took on more responsibility and challenge.

Organizations required their personnel (and contractors) to be more adept to changing situations and have greater ability to adjust to new requirements.

Today as Onsman observes "we now rely more than ever on the discretionary effort of employees" (2003). The typical employee (or contractor) role will entail greater flexibility and require the executing of more judgment. "Management is everywhere" within an organization states Minztberg (2003).

1.2.3 Greater scrutiny of the organization

In the face of major corporate collapses worldwide over the last five years, governments and regulators have moved to strengthen the regulations controlling corporate behavior. We have seen the introduction of new regulations such as Sarbanes-Oxley, CLERP9 and Turnbull Guidance that aim to improve governance and bring more transparency into the way organizations operate.

In one sense it can be argued that this greater focus on corporate behavior and responsibility is cyclical, as we experienced similar strengthening of corporate regulations after the 1930's stock market disasters. It can also be observed that corporations around the world are moving more towards the narrower shareholder model rather than the broader 'stakeholder' model as those that the corporation serves (Micklethwait et al 2003, Mintzberg 2003).

But there are significant differences this time around. In industrial societies, the proportion of ordinary people owning direct shares in a company has risen significantly over the last few decades. After the losses experienced through the 'tech wreck' in 2000, the average investor is more attuned to and less tolerant of shoddy corporate behavior. The media and societies at large are far more sophisticated at recognizing cover-ups and secrecy in organizations, and are less accepting of that behavior.

Societies in general are far more environmentally and socially aware and demand that our governments and corporations behave in responsible ways. Bodies such as the Global Reporting Initiative promote sustainable reporting guidelines for organizations worldwide. Organizations are encouraged to broaden their focus beyond purely economic boundaries to encompass social and environmental dimensions (GRI, 2002). There are also many special interests groups, some with extreme or mischievous views (e.g. 'internalmemos.com' and certain environmental groups) that are media savvy and can act swiftly, damaging the reputation of an organization, or disrupting its operations. As a consequence, we are likely to see greater scrutiny of organizations (corporations and government bodies alike) continuing for some time into the future.

1.2.4 New conditions: Unique and difficult challenges for organizations

The three trends outlined above combine to present a unique and difficult challenge for organizations today. On the one-hand organizations must now operate in highly dynamic environments. They must adjust and adapt quickly. They need high levels of awareness, agility and responsiveness to changing situations and events. On the other hand, all their decision and actions are under far greater scrutiny from an increasing variety of stakeholders and interest groups. Pressure mounts on those that run organizations, as expectations demand all decisions and actions are reasonable and appropriate.

These trends create enormous stress, as they are both pulling at the organization in opposite directions. One trend requires swiftness of response, the other demands methodical and carefully calculated actions.

Adding a further dimension of stress to the organization is the third trend. An organization's core competencies, skills, knowledge, and decision-making capabilities are no longer located at a single, centralized point. These attributes permeate the whole organization, at all levels of its operations and through a diversity of personnel. Therefore, an attempt to control and carefully orchestrate decision-making and change through a central point is a near impossible task in a modern, complex organization.

1.3 Changing the nature of measurement

The language and thought of an organization is built upon its approach to measurement. What it measures and how those measures are structured helps an organization form an understanding of itself. From that understanding, the behavior of the individuals that collectively make up the organization is affected. Individuals and groups within the organization will make decisions, reward and punish based on its measures.

If the challenges are creating new conditions for organizations, how will this affect an organization's approach to measurement, and by extension how it understands itself and makes decisions? Before I attempt to answer this let's briefly look at how organizations typically measure.

1.3.1 Traditional measurement: Looking backwards

Until recently, the concept of performance measurement adequately fulfilled the aims of measuring for organizations. Performance measurement is the act of measuring backwards in time, from the present into the past. The general principles of accounting (the backbone of performance measurement) provided all the necessary data and information, such as profit and loss, balance sheet, cash flow, and related measures. These measures showed how the organization had performed over some given period of time. For example, what was the revenue from product sales for last quarter, and how did this compare to the same period last year? This type of data was deemed to be adequate for the organization to understand itself, where it stood in relation to expectations and what decisions it may need to make next.

As the environments that organizations operated in became more complex and competitive, broader measures were required for organizations to better understand their situations and what decisions needed to be made. Over the last ten years we have seen the emergence of new measures such as key performance indicators (KPIs), measures from data warehousing and data mining, triple bottom line reporting and balanced scorecards. Often, some of these newer types of measures are referred to as 'leading indicators'. For example a measure that reports on customer satisfaction may be a leading indicator for future customer sales. However, these

measures are backward looking; they are measuring events from the present into the past, for example the number of customers that are dissatisfied. These measures do not attempt to formally measure what potentially may happen in the future. Consequently, all these measures are still performance-based (backward looking) measures.

1.3.2 Forward viewing: The new measure for organizations

The unique confluence of challenges that organizations now face will cut deep into the core of how an organization measures itself. Performance measurement will no longer provide the major basis for an organization to understand itself and the decisions it may need to make. Rather, measuring what lies ahead of the organization and what could happen to it (forward measuring or forward viewing), will need to become the major contributor to understanding itself and what decisions it makes.

The reasoning behind the need for this significant change in the focus of measuring can be illustrated through a simple example. Imagine you have an objective of reaching the top of a hill. You have a path to follow and you can plan and forecast your expected time of completion. As you proceed, at certain points along the journey you can measure how you are performing, and make any decisions to adjust your actions (if required) to meet your expectations. For example, you could be a little behind a planned schedule at some point into the journey, so you decide to increase your walking pace in order to get to the top by the expected time.

Now imagine instead that the path you take is not static, that almost magically, situations and events are always changing and new ones are emerging constantly. The path is not going to stay the same as when you initially planned the journey. For example, the surface texture might start changing in front of you from hard dry ground to soft and slippery. As you move higher along the way, new forms of dangerous animals start emerging, new weather patterns emerge, and so on.

In this changing environment, while tracking performance against original plan is useful for where you are at some point in time, it is no longer the main driver or contributor to your decision-making. Performance data plays a secondary role as you develop more interest in what is evolving in front of you. You are drawn to

focus on interpreting the path ahead by measuring it in some way. You therefore become more aware of the situations evolving in front of you and what they potentially mean to your progress. Your ability to interpret emerging situations or events and adjust in anticipation is what is most important to you.

Organizations are now facing this same type of environment in today's world. An environment of constant and complex change that is also highly competitive. Organizations must therefore change the fundamental focus of their measuring systems. Measuring forward needs to become the key contributor to understanding and decision-making for organizations.

Through a highly evolved forward viewing capability, an organization can become more attuned to the constantly changing 'terrain' ahead and the different stresses and strains it places on its activities and expectations. How the organization measures forward will be critical, as the decisions it makes will be more closely scrutinized. But with a sophisticated forward viewing capability, an organization can develop a deeper understanding of the stresses and strains it faces. It can respond more appropriately, thereby enabling it to achieve the best possible results and in a manner also acceptable to those scrutinizing the organization.

Importantly, this capability also needs to be available throughout the organization, not just at a few centralized points. An organisation is a composite of many people performing many varied tasks. As discussed earlier, personnel at all levels play a greater role decision-making. Their decisions, though individually may have a small effect, will collectively have a significant bearing on what paths the organization takes and how it travels on those paths forward.

1.3.3 Forward viewing: Is risk up to the job at hand?

Currently, forward viewing is extremely underdeveloped when compared to the 'backward viewing' (performance measurement) capabilities of an organization.

The concept of risk is the only tool available with which we can measure forward. Risk is a way an individual or an organization can measure uncertainty about potential future situations and events that may have some positive or negative impact. Organizations, regulatory bodies and markets have recognized that using the concept of risk provides an organization with a better understanding of its forward view. They have also recognized that it provides a basis on which organizations can make decisions about managing the exposures they face.

The concept of risk is also seen to play a role in the demands for increased scrutiny. Regulators and markets are now compelling organizations to improve risk management practices. For example, the Turnbull Guidance (compliance requirements for London Stock Exchange) states that organizations must identify and address risks across their operations. Over the last few years, organizations around the world have begun to roll out risk management frameworks and systems across their operations. Some are doing this from scratch, while others are expanding their once specialized and insular treasury or insurance risk functions.

For guidance on the frameworks and systems to implement, organizations are following one of a number of available standards on risk management, such as Ferma (European based standard), ASNZ 4360:1999 (Australian and New Zealand standard), various guidelines for implementing Turnbull Guidance (e.g. "Implementing Turnbull" from the Institute of Chartered Accountants in England & Wales), Basel II Accord (for finance institutions), and recently the COSO model for risk management (worldwide). All of these models are by and large derived from engineering and project risk management methods, or finance risk approaches (Basel II Accord).

Superficially, risk and risk management practices can appear to provide a model through which forward viewing can be performed effectively and therefore address the challenges facing today's organizations. But is risk in its current form really up to such a challenging task?

In the following chapters I will argue that the concept of risk and risk management practices are ill equipped for such a challenge. I will argue that risk (in all its current forms) is so ill equipped that overall it will in fact mislead and create more of a cost burden on the organization than providing long term benefits. I contend that a fundamentally new approach and model is required, which will lead to the creation of a new, significantly better forward viewing capability for organizations, a capability that is the most pressing need for organizations in today's world.

Chapter 2

Introduction to Risk

2 Introduction

In the following chapters, I will discuss how the concept of risk and the process of risk management fail to provide an adequate forward viewing capability for organizations.

Fundamentally, risk and risk management fail in four key areas. These are:

- **Measuring**
  The current models of risk produce incomplete and misleading measurements of risk.
- **Identifying**
  The approaches to identifying risk are not suited to complex real-world environments.
- **Tracking Change**
  The approaches to tracking changes in risk are ill equipped for complex real-world environments.
- **Assurance**
  Rather than adding to the level of assurance about an organization as a going concern, current risk management practices can create misleading impressions about an organizations risk profile.

2.1 The basic model of risk

Before beginning a discussion on the limitation of the concept of risk, it is important to establish a general definition. However, for a word that is used so often in everyday language, it has surprisingly numerous definitions. The definitions can be varied, such as "the possibility of loss, injury or other adverse circumstance" (The New Shorter Oxford Dictionary, 1993), "chance that something will happen that will impact on objectives. It is measured in terms of consequence and likelihood" (Australian and New Zealand Standard for Risk Management, 4360:1999), and for risks in financial environments, they explicitly consider the variability in a potential positive and negative outcome as risk, in phrases such as a "measure of volatility" in an asset (Choucy et al 2001).

I will propose that Eugene Rosa (2003) has put forward the most robust definition of risk. The definition states;

> **"Risk is a situation or an event where something of human value is at stake, and where the outcome is uncertain".**

This definition is important because it establishes a number of important fundamentals about the notion of risk. At this stage of the paper, I will raise just one of these. That is, uncertainty is a necessary condition to experience risk; if there is no uncertainty there isn't any risk. This may seem like an obvious point, but as we shall see shortly, it has significant implications when applied to real world situations.

Working from this definition, let's put the model of risk in action to show how it works in a simple example. Say I am considering playing a gambling game with a fair die, where I bet $10 on the outcome of a 'snake eye' (number one). In this game, if the number one rolled, I would double my money, but if any other number appeared I would lose my $10. If I assess the risk of losing my $10, in other words my 'human value', I would come up with a five in six chance of losing my $10 (or in other words an 83% chance of losing $10).

From Rosa's definition, we have a risk because uncertainty is present in relation to losing $10.

The way we measured uncertainty in this situation is through probability, and it has worked quite well. All the uncertainty has been fully accommodated in the probability expression. There is no other uncertainty apparent. For example, I do not have to concern myself with any uncertainty about whether or not the six-sided die will turn into a 12-sided die half way through the roll.

The fundamental point in this case is that the risk expression (probability of losing $10 = 83%) is a complete representation of the risk in this situation. I do not need any more information embedded or represented in the risk expression. I can therefore confidently make a decision about whether I choose to proceed with this game. I may conclude that the risk is too high (for a gain of $10), and suggest that the odds have to be at least 50/50 for me to proceed, and clearly in this game they are not.

Chapter 3

Measuring

3 The incomplete and misleading expression of risk

When we move away from highly controlled ‘closed systems’ such as a dice game to real world situations, a significant problem emerges with the way we express risk and make decisions with risk.

Consider that someone in an organization states that there is a significant risk from a situation emerging with a key supplier. This person believes there is a high likelihood (say greater than 50% chance) that the organization could face a $1million impact from a potential disruption at this key supplier. If this supplier is unable to deliver key raw material, the organization cannot produce its product and will experience cost and revenue problems.

The person assessing the risk of supplier failure could have used a variety of ways to derive his measurement. For example he could have used a statistical assessment or a judgment (arrived at after observations and discussion with his team). The person could also have expressed his results in a number of ways, for example, simple probability and impact figures (e.g. 50% likelihood and $1million impact), a distribution range from a scenario model, or a qualitative expression that combines the likelihood and consequence to provide an overall statement, such as “high risk”.

When we compare this example with the die game we face a stark contrast. If we attempt to measure the uncertainty in relation to a $1milion loss, we find that probability cannot produce a complete representation of all the relevant uncertainty in this situation. This is because the supplier situation is not a simple physical system, it is a complex ‘soft’ system, to use a phrased coined by Checkland (1981). In this case we are ignorant of the many key uncertainties at play, such as complex human emotions and interactions unfolding at the supplier. We cannot model these complex uncertainties within this situation with the same degree of reliability (or completeness) as we can in a dice game. The supplier situation is not a stable physical environment that we can control and test. There is no history of identical situations that have played out over and over again that can be put into a statistical model.

We can make assumptions and add ‘weighting factors’ to create an approximate model, but this moves us further away from the real situation and creates more uncertainty.

Fundamentally, probability cannot adequately deal with the complex uncertainties present in this situation. It cannot fully accommodate the uncertainties through any method used to derive a result. Therefore, probability will always produce an incomplete representation of risk in a real world situation. It is incomplete because, under the Rosa definition of risk, there is a significant proportion of uncertainty that has not been represented in any risk expression we put forward. Under any current approach, the risk expression cannot make a simple yet rigorous statement on the overall uncertainty faced in a real world situation. In real world situations we are always faced with expressions of risk that, to some degree, are incomplete.

3.1 Other definitions of risk

It is worth noting that some definitions of risk, particularly in technical fields, attempt to divorce uncertainty and risk. They will claim that only the uncertainty that can be measured quantitatively through probability is used to express risk, while the remaining ‘un-measurable’ uncertainty is not part of the risk definition or expression. This thinking is derived from scientific environments where it is important to identify uncertainty as a separate entity to the measurement result. For example ‘random error’ is identified separately to the measurement result and maybe controlled and treated separately. In fact, the COSO model for risk management supports this view of uncertainty and risk by stating that uncertainty “emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.” Yet in contradiction to this, COSO also accepts qualitative expressions of likelihood as part of risk, in which uncertainty is present and unaccounted for through any precise method. (COSO, 2004)

Unfortunately, this definition of risk is nothing short of useless in real world situations. This is because, as shown in the supplier risk example above, a significant proportion of the uncertainty will not be represented in a risk expression. And according to this rigid definition of risk, the unmeasured uncertainty has nothing to

do with the risk in this situation. Therefore the notion of risk becomes meaningless, because one of the most important aspects about this situation is the uncertainty, yet there is no place for it in this narrow definition of risk.

This is another reason why Rosa's definition of risk is far more relevant and meaningful to real world situations. It teaches us to accept the importance of uncertainty (in all its forms) in risk and forces us to focus on the fact that our expressions of risk are often incomplete.

3.2 Incomplete risk expressions: Creating a significant cost burden for organizations

The incompleteness in all real world risk expressions presents a significant problem for organizations and their decision-making. This problem can be demonstrated when we compare a performance measure to a risk measure. When I look at performance figures such as a statement about revenue or cost in an organization, I am looking at 'hard' data. I can focus my decisions and actions in response to the performance data appropriately. For example, cost data might show "costs have gone up $1million last quarter in division X" when compared to the previous quarter. In this example the meaning of the measure is clear. $1million increase in costs doesn't mean "$3milion increase in revenue", it means what it says. Therefore, my decisions and actions can have a focus commensurate to the cost statement. For example, I may enact a program to lower the costs in division X next quarter by $1million.

In the supplier risk example however, I am faced with a significant dilemma. The meaning of the risk expression (e.g. 50% likelihood of $1million loss, or 'high risk') is not clear. It is an incomplete and potentially misleading representation of the risk in this situation because it has not accounted for all the uncertainty. The risk expression is either:

- *An overestimate of the risk:* Accordingly, my decision and actions would be an over-reaction to the risk. This means I will be spending more than I need to.
- *An underestimate of the risk:* Accordingly, my decisions and actions would be an under reaction to the risk. The organization therefore remains over exposed to the threat; and if the supplier did fail, the organization would suffer an unexpected cost.
- *About right:* Accordingly, my decisions and actions would be an appropriate response to the risk situation.

In two out of the three possible outcomes in this risk situation, I am going to get it wrong and add extra cost or unexpected exposure to the organization. The unfortunate aspect of this limitation of current risk models for an organization is that the organization does not face only a few of these risk situations. Across any large organization, at any one time it will be facing thousands of situations and events that will have risks associated with them. As a consequence, it is reasonable to assume that in two thirds of cases where decisions are made involving risk, an extra cost or unexpected exposure is placed on the organization.

If the cost and exposure from misleading interpretations of risk is collated across thousands of situations and events, it maybe found that the organization is carrying an unexpectedly large cost and exposure burden. This is a significant burden for an organization to be carrying in today's challenging and competitive world.

To draw this back to our analogy of climbing the hill with the constantly changing environment, we would be misreading the 'terrain' two thirds of the time. We would be making many minor miscalculations, which cause minor delays. Collectively, these minor delays would significantly slow progress. Occasionally we would be making a major miscalculation, which could set us back a fair bit. Overall, we are employing a rudimentary technique of viewing forward, but we are probably only marginally better off than someone who would be only using performance data and information (viewing the present and backwards from the present).

One might argue the cost burden faced by organizations is a consequence of a complex and dynamic real world. Can we really substantially improve our understanding of what lies ahead of us? Naturally we cannot know the future; problems will always arise, no matter what we do. The question is rather, can we do substantially better than what is possible with the approaches we use now?

3.3 Recognition of subjectivity in risk

I have proposed that our current methods of expressing risk are incomplete. This can be interpreted as another way of stating that the way we understand and develop knowledge about a risk is subjective. If we cannot fully accommodate the notion of risk within a cardinal framework, then any interpretation or measurement we put forward must be subjective. Rosa's definition of risk also supports this fundamental notion. In fact much of the social science analysis of risk rejects any 'objective' quantification of risk (Slovic, 2000).

Even amongst the more technically inclined proponents of risk accept its subjectivity. One of the key architects of the subjective theory of probability, Bruno DeFinetti, goes as far as stating that probability is always subjective, and that 'objective' probability is a metaphysical concept devoid of meaning (1937). More recently, Rene Shultz (one time editor of the Journal of Finance and the Journal of Financial Economics) has stated that risk is part of the social sciences (2001). In other words, it cannot provide the accuracy, precision and objectivity evident in the physical sciences. Crouhy et al in their comprehensive publication "Risk Management" (2001) admit that the task of measuring 'operating risk' (term used to refer to risks other than market and credit related risks in financial institutions) involves 80% art and only 20% science.

3.4 Attempts to deal with subjectivity in risk

A common knee-jerk reaction to the subjectivity in risk has been to perform more analysis. As Slovic observes, this misses the point (Slovic, 2000). No amount of technical analysis, delphi group assessments, or tests and experiments will remove the subjectivity. In real world situations, subjectivity in risk is always apparent. The level of subjectivity will also vary substantially from one risk situation to another. It can also vary significantly within the same risk situation over time. As I will discuss later, the level of subjectivity has a huge bearing on decision-making.

There have also been attempts to recognize the subjectivity (or incompleteness) in risk measurements, in order to provide more information about a risk situation. Examples include a measure for the uncertainties in a stated probability measure, by applying another probability value to represent these other uncertainties, which was proposed in the Nuclear Regulatory Commission Rasmussen Report (1975); others referenced by Ritche and Marshall (1993) noted that Billot (1991) proposed the need for a cognitive model outside of probability; while Felter and Durson (1998) proposed applying a value to measure factors affecting precision in risk assessments in toxicology. However, all of these approaches have significant shortcomings. They fail to express the subjectivity adequately and are ultimately not robust and practical enough to be used regularly in organizations by a variety of personnel and across a wide variety of risk situations.

3.5 A predicament for organizations but no help from the standards

So where does this leave organizations, who are dutifully rolling out risk management frameworks and systems that adhere to one of the recognized standards? As discussed above, organizations are faced with a significant cost burden from misreading and misinterpreting the exposures they face through the use of current risk models. What do the risk management standards have to say and offer about this predicament? The standards say and offer very little, because they are based off the same flawed risk models as discussed above.

What the risk management standards do say on the subjectivity (or incompleteness) of the risk expression tends to fall into one of two approaches. That is, they either stress the need for thoroughly analyzing a risk situation so that you get quality results (COSO, 2004; Basel II Accord, 2001), or if you cannot apply an appropriate quantitative approach, then use a 'qualitative measure', in other words, a qualitative statement about the exposure, such as 'high risk' or 'moderate risk' (ASNZ: 4360, 1999; COSO, 2004; Implementing Turnbull, 1999).

These two approaches are not solutions of any substance. Firstly, while doing more analysis can be helpful in many situations, as discussed above, it will not remove the subjectivity (or incompleteness) in most cases. There is no direct correlation between the amount of analysis performed and the reliability of the result. Reliability is dependent on a number of factors, especially the environment of the situation being assessed. But more importantly, decision makers have a limited amount of time, resources and money to apply to the consideration of risk in any given situation. They cannot spend forever undertaking detailed analysis of each and every risk situation in the vain hope of achieving precise risk measures. Decisions need to be made and activities need to move on.

Secondly, using a ‘qualitative measure’ for complex real world situations is not a solution either. It is simply taking a best guess at something we think we cannot measure. But how valuable is that ‘best guess’ is anyone’s guess, as there is nothing in the standards to help here. Ultimately, this approach encourages sloppy thinking and practices, as it is too simple to label something as ‘high risk’, ‘moderate risk’, or ‘strong possibility’ and so on, and only cause more confusion and misinterpretation. Data presented by Conrow (2000) shows how significant the misinterpretation can become. He also cites numerous examples of significant confusion and misinterpretation from the US intelligence community about estimates of probabilities and risk.

3.5.1 Definitions for likelihood don't address problems

In an attempt to remove ambiguity from qualitative measures of risk, in some cases a definition is provided along with a qualitative statement about the likelihood. The FERMA risk management classification of probability of occurrence (Table 1) is typical of this type of approach.

Estimation	Description	Indicators
High (Probable)	Likely to occur each year or more than a 25% chance of occurrence	Potential of it occurring several times within the time period (e.g. ten years). Has occurred recently.
Medium (Possible)	Likely to occur in a ten year time period or less than a 25% chance of occurrence	Could occur more than once with the time period (e.g. ten years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low (Remote)	Not likely to occur in a ten year period or less than a 2% chance of occurrence	Has not occurred Unlikely to occur

Table 1: Probability of Occurrence (Taken from FERMA 2003)

The problem with this type of model is that it is fundamentally flawed on at least two counts. Firstly, such a model does not take into account that different risk situations can create different perceptions of a likelihood estimate. For example, lets say I run an airline corporation. In this corporation, I am facing 2 different risks, both of which have similar potential impacts (very big). The first risk, a major disruption to a key supplier, has been rated with a 30% chance of occurrence, or could occur several times over a ten-year period. Under the FERMA model this risk would be a 'high' probability of occurrence. However, I would more likely view this risk as a 'medium' or even 'low' likelihood of occurrence, because suppliers are often outside of our control, and their environments are very complex and difficult to predict. The second risk I face is that one of our main fleet of aircraft could crash, which lets say has being estimated at 20% chance, (or 'could occur more than once' within a ten year period). Under the FERMA model this risk would be a 'medium' probability of occurrence. However, I would be alarmed at this level of exposure, and would certainly not regard this probability of occurrence as 'medium', nor would I regard it as 'high', but rather 'extremely high'! Therefore, even with two simple examples I cannot get any consistency in perception of risk within this model. Significantly, prioritizing my decisions and responses across possibly hundreds or thousands of risks is severely compromised.

Secondly, this model is fundamentally flawed because it still fails to address the subjectivity (incompleteness) in the risk expression. We have no rigorous attempt to address the uncertainty not accommodated within the likelihood statement or expression. We are yet again left with estimates or guesses about the likelihood of occurrence, with no credible evaluation of their worth and what that worth means to the organization.

3.5.2 The risk matrix of confusion

Another prominent form of measurement for qualitative risks, and one that is often used as a method of prioritizing risks, is the risk matrix model. The 'qualitative risk analysis matrix', taken from the AS/NZS 4360: risk management standard (Table 2) is a typical example.

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Moderate	L	M	H	E	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

Table 2: Qualitative risk analysis matrix (Taken from AS/NZS: Risk Management, 1999)

Legend for Table 2

E: Extreme risk; immediate action required
H: High risk; senior management attention needed
M: moderate risk; management responsibility must be specified
L: Low risk; manage by routine procedures

Amongst the available measuring approaches in the risk management standards, the matrix model for qualitative risks is the tool that produces the most misleading results. This is because two subjective values are combined to produce a third subjective value, which is meant to represent the initial subjective values. In other words, another layer of subjectivity is created, further diluting the link back to the originally perceived risk.

This combination approach is based off a mathematical view of risk. The original models of risk, which were derived in a mathematical framework, allow for the combination of the likelihood and impact (consequence) to produce an overall measure. In a cardinal environment, this is perfectly acceptable, because we are combining two numeric values to attain the product of these values. In fact in a cardinal risk environment, it is preferable to combine the constituents of risk into an overall product because we can sometimes be misled about the true overall value of the risk. Research conducted by Kahneman, Slovic and Tversky (1987) has shown that humans will place different values on identical risks. For example, when people are offered a chance of winning (or losing) money in a choice between two bets (e.g. $1000 at 2% or $80 at 25%), studies show that people will prefer one bet over the other, when mathematically, there is no difference.

But the real world experience of risk is not a cardinal environment, and we therefore need to view the constituents of risk (the uncertainty and impact) separately. As discussed, we have significant aspects of the uncertainty not accommodated within any expression we put forward to represent it. Even if we can express it, it will not be in a cardinal form. Therefore, combining the value for uncertainty with an impact value to derive an overall result can only create further confusion and misunderstanding.

In fact I would contend that Kahneman, Slovic and Tversky's research supports a belief that humans are intuitively wired to recognize subjective risk. This is because the research results show that humans are reacting to the constituents of the risk expression rather than to its product. In a subjective environment this is exactly what you would want to happen, because an overall value would tend to hide or obscure the true nature of the exposure.

3.6 The misunderstood effect of subjectivity in risk and decision-making

As discussed in the preceding sections, subjectivity (or incompleteness) in risk expressions have been recognized, and some attempts have been made to address it. However all approaches to date either misunderstand the effects of subjectivity, and or do not know how to deal with it in a rigorous way for decision-making.

To illustrate the point lets look at a simple example. If someone told me that there is an 80% chance that I will get robbed if I went outside today, I would want to understand information about the components of the risk claim (that is, the 80% and getting robbed). I would want to understand how effectively the 80% represents the uncertainty in getting robbed. Is the 80% a guess? Is the 80% claim based off a highly reliable assessment, or is the 80% claim somewhere in between (i.e. there is some validity to it)?

The information I garner surrounding the claim of 80% will be the key factor in determining what decision I make and actions I perform. Importantly, my decisions and actions will vary significantly based on the information about the 80% claim. If the 80% claim was highly subjective (e.g. a personal opinion with no supporting evidence), I would react a certain way. If the 80% claim was reliable my decisions and actions would be very different. If the 80% claim had some validity (i.e. a moderate level of subjectivity) I would react differently again. In total, that is three different decisions and actions based on three different levels of subjectivity in the components of the risk claim. Yet this change in subjectivity cannot be incorporated in any rigorous way into the components of any risk expression.

If I apply a mathematical or matrix approach to producing a risk measure for this risk situation, the '80%' and the 'getting robbed' are combined to produce an overall measure. Yet the most important information, the subjectivity in the risk claim is ignored. In all statistical approaches, again, the subjectivity cannot be accommodated. As we also saw in definition of likelihood approaches (section 3.5.1 – "Definitions for likelihood don't address problems") the fundamental problems are still there. In any current form of measuring risk, I am likely to be misled by the measure that is put forward to represent the risk situation that I face. This will affect my decision-making, and as discussed in section 3.2 – "Incomplete risk expressions", this creates a significant cost burden for organizations. In two out of three cases I will either overreact to the risk, or unwittingly face a higher exposure than I was lead to believe.

In an organizational environment where many hundreds or thousands of risks are faced, this creates many problems. An organization has a finite amount of time, money and resources available to deal with the risks it faces. Prioritizing decisions and actions is critical, yet under these methods of risk measurement the quality of the decisions and actions is severely compromised.

3.7 Managing risk: An emerging crisis

While many have recognized the shortcomings with our current approaches to measuring risk, at best, it has only been dealt with in a superficial way. Consequently, a simmering discomfort with the way we understand and handle risk is gradually spilling over, creating major concerns. Prominent commentators on risk have been recently voicing their objections. Carlo Jaeger, et al in their work "risk, uncertainty and rational action" have expressed that there is a "crisis in risk management" (2001). Paul Slovic (2000) observes a breakdown in trust and an increase in conflicts between organizations, society and governments through the use of current risk management practices as a mechanism to understand and handle risks; while 2002 Nobel Economist Daniel Kahneman no longer accepts that decision analysis, one of the tenets of the risk model, works in the real world (Strategy-Business: 2003).

The problems with how we understand and deal with risks do not lie purely with the way we measure risk, but it is none the less a very significant problem. How can we price risk when it is 80% art? How can we decide which risks need addressing now, and how much we spend on addressing them, when most of the risk measures are likely to be misleading? Often this predicament is simply ignored, and we happily regard risk information (a forward measure) as if it were hard data, such as a performance cost figure (backward measure). We then use these extremely rubbery figures to make significant decisions, decisions that can cost large sums of money and affect people's lives. No wonder some believe there is a crisis in risk management.

Chapter 4

Identifying

4 We are ill-equipped for the real world

One of the least discussed aspects in the literature on risk is identification of risk. In this chapter I will discuss two aspects of risk identification, namely:

- The components that constitute a unique risk
- Approaches used to identify risks in organizations

I will show that to date, the approach to these two aspects of risk identification has been cursory at best. Accordingly, I will show that this lack of attention to, and detail in, current risk identification concepts has created significant problems in how organizations understand and deal with risks.

4.1 Current thinking on what constitutes a unique risk

Current approaches to identifying risks work on the assumption that risks are simple self-contained entities or events with clear boundaries that separate them from non-risk aspects of an environment. Therefore, under this belief, identifying risks is simply a process of finding or spotting them within an environment or situation, as if one were to sift through a plate of wheat and pick out and remove the bad grains. If you see a risk, then just identify it by naming it; for example ‘supplier risk’, ‘risk of production line breakdown’, ‘credit risk’, ‘cash flow risk’ and so on.

The model of what constitutes a unique risk has worked well historically because the concept of risk was mostly applied to situations where identifying and classifying risks were easy. For example it is easy to identify the (downside) risk in the die game discussed in section 2.1 – “The basic model of risk”. This is simply the “risk of losing $10” (which as we saw was about 83%). This is a clear, unambiguous identification of the risk in this situation. Similarly, in the fields of finance and insurance, the simple approach to identifying risks is also applied successfully. This is because fixed categories of risk are easy to establish, such as ‘interest rate risk’ and ‘commodity price risk’. These risks have clear, static boundaries and meanings, just like a bad grain in a plate of good grains.

4.1.1 Risk management standards toe the line

All the risk management standards continue this line of thinking about what constitutes a unique risk. The standards take the view that a risk is identified solely through the definition (based on which ever one they use) of risk. In other words, if something bad could happen, we name the negative event and estimate or analyze the likelihood of it occurring and the potential consequences - and that's about it, the risk is identified. No other dimension or attribute needs to be used to uniquely identify the risk. Some approaches will capture other information about the risk, such as who owns it, the related business activity, and a general source category for the risk (AS/NZS 4360:1999), or in some cases, even a detailed cause-effect fault-tree analysis (Bowden, et al, 2001). However, this other information is not regarded as key to the uniqueness of the risk, it just provides additional information.

4.2 Approaches used to identify risks in organizations

Unlike the belief about what constitutes a unique risk, the approaches and processes organizations will use to identify risks can vary significantly. The approaches used can range from ad-hoc practices through to highly structured methods. Most approaches can be classified into one (or more) of four categories. These are briefly discussed in the following subsections.

4.2.1 Top-down identification approaches

Most standards in risk management support a top-down approach to the process of identifying risks. For example, senior management, or even the board of directors initially identify key risks, and then gradually, down the chain of command, other risks can be identified (COSO, 2004; Institute of Chartered Accounts, England & Wales, 1999). In a variation of the top-down approach, it is often suggested that as a first step key strategies, assets, process and or drivers for the organizations are identified. As a next step, risks that could affect these key aspects of the organization are subsequently identified.

The top-down approach often leads to organizations focusing on identifying a small set of strategic or major risks to the organization, and concentrating mitigation efforts around these risks. These risks tend to number between half a dozen or so through to about forty or fifty. The general line of thought behind this top-down approach is that an organization can more effectively concentrate on dealing with its major risks, and while there may be significantly greater numbers of smaller risks at lower levels within the organization, ignoring these risks (or at least giving them a lower priority in terms of identifying, assessing and managing) is an acceptable path to take.

4.2.2 Linked risks and cause and effect models

One approach sometimes used in identifying risks is through a cause and effect model. This model is based on the belief that risks occur through a series of linked events that can be identified through analysis and traced back to a root cause (or causes).

For example, a risk event such as 'supplier failure' is identified as the end event, and from this, other events that may cause this event to occur are identified. In the end, a potentially very complex chain or web of linking events leading to the end event 'supplier failure' is identified. Each linking event in the chain is assessed for possible failure (e.g. likelihood of occurrence), and through appropriate mathematical logic, an overall likelihood of failure for the end event is calculated or surmised. Possible weak points in the sequence of events can also be identified. Mitigation strategies can be employed to target weak points in the chain, and or deal with the overall end event.

This cause and effect approach can also be reversed. That is, you start with an initiating event and work forward, through a sequence of linked events (which may fan out to many other events) until you arrive at an end set of risk events. For example, a breakdown in a key assembly line could trigger a whole set of different end risk events, such as delays in product production, inability to sell stock, drop in revenue, change in competitor actions, loss of key customers.

This approach is based on probabilistic risk analysis (PRA), a model initially developed for aerospace and nuclear industries in the 1970s. It is a method designed to quantify the risks in complex engineering systems. For example, an end event such as some type of nuclear reactor failure is traced back through component systems. Each component is assessed for failure, usually through statistical data on the component's failure rate. Where reliable data on failure rates is not available, 'synthetic' probabilities are derived, which may come from generic data, expert opinion or case histories (Bier, 1997).

PRA also has links to scenario modeling, which is often used in organizations. Scenario modeling or planning is also a cause and effect modeling tool, and has been used as a way of identifying risks. For example, a workshop could be conducted with appropriate personnel who brainstorm what are the possible behavior responses of a customer, supplier, or competitor, and what cascading effects (risks) will each potential action have on the organization.

4.2.3 Identification by categories and classifications

Often, organizations will derive categories or classifications of risk types as one of the starting points to identifying risks. For example, an organization might start with a category or classification system such as strategic, technological, legal, financial, and so on. These categories may also be split further into sub-categories. From this point, the organization will then identify the risks it faces via each category.

Within banking environments, the role of the category can go even further. Some banking institutions will rely on identifying operating risks through pre-defined categories. Pre-defined categories used by banks include theft & fraud, transaction processing, rouge trading, model risk, lawsuits, etc. Banks using this model believe that the operating risks they face can be placed into one of the pre-existing categories (Peccia, 2001).

One of the perceived benefits of this approach is that sufficient levels of data can be amassed within each category. With a sufficient level of data, a bank is able to more easily derive a statistical model that represents the risk it faces in each cate-

gory of operating risk. From these statistical models, a bank will aim produce quantitative measures for the level of operating risk it faces on a day to day basis (for example, through Value at Risk or 'VaR'). Through this approach, a bank perceives that it has 'priced' its operating risk, and can therefore insure its exposure, thereby maintaining its exposure at or below accepted levels.

4.2.4 Models avoiding individual risk identification

Some recent approaches attempt to move away from identification of individual risks at a tactical level and move towards an identification of vulnerabilities or potential 'discontinuities' within an organization's broader sphere of operation. Sometimes termed 'enterprise resilience', this model is based on a top-down approach to building an integrated and networked picture of the organization's operations, from suppliers through to customers. As part of building this picture, key earnings drivers and the processes, technologies and capabilities that support them are identified (Starr, et al, 2003). From this picture, interdependencies, vulnerabilities and risks associated with the key earnings drivers can be identified and prioritized. Through this high-level networked map of the organization, areas that need attention can be treated or strengthened so that they are more resilient to disruption.

For example, through this approach it might be discovered that an organization that relies on its supply chain for earnings has vulnerability because its key raw material arrives through a single wharf loading point. If this loading point were to fail, the organization's earnings would be severely damaged. Yet a second loading point, which remains under utilized, could be upgraded slightly to provide 'resilience' in case the main loading dock failed.

4.3 Problems in our thinking about identifying risks

Superficially, the model of what constitutes a unique risk and the different approaches used in identifying them can appear reasonable and adequate. However, if we delve deeper into the nature of an organization, the nature of risk, and the relationships between the two, we find a significant disparity between our thinking about risk identification and the way risks emerge and behave in organizations. This disparity leads to significant problems in how we understand and deal with risks.

4.3.1 An organization is a soft system

An organization is a complex soft system, that is, at its core this type of environment is based on human interactions. Even though there may be clear objectives, processes and controls within an organization, and even though there may be significant levels of automation, human interfaces and interactions pervade every facet of the organization's operations. Without human interactions you do not have an organization.

As a soft system, an organization is the opposite of a 'hard' system, which has no human component (Checkland, 1981). A hard system is highly structured and behaves predictably. The interfaces are highly controlled and the possible behaviors and changes are known (or can be relatively easily derived). For example, a bridge or simple mechanical device is a hard system. The changes experienced in such physical constructions over time can be relatively easily understood and predicted.

4.3.2 The nature and relationships between an organization and risk

As a complex soft system, an organization will experience constant change through its human interactions. Change is rarely contained within one small locale, instead it cascades forward affecting other areas or facets of the organization. Change is often propelled forward by the organization's reaction to the initial change, creating another layer of change.

Unexpected stresses and opportunities are situations that generate change. These situations will occur constantly throughout an organization's sphere of operation. An emerging situation or event can cause some aspect of the organization's environment to evolve and morph in complex and unpredictable ways. Sometimes these effects are minor, other times more significant. For example, a new customer surfaces with new requirements forcing some work changes; a key supplier suffers difficulties, which slows production and causes process changes; a contract negotiation stalls unexpectedly; an organizational re-alignment creates unexpected difficulties in operations; a technical breakdown generates pressure and change in distribution; economic conditions change in a major new market, and so on ad infinitum.

Let's now look at a fundamental aspect of risk. Risk is a human experience. If there is no human involvement, there is no risk. This aspect of risk is also very clear in Rosa's definition of risk, which states that 'human value' must be at stake in some way for risk to be present. Therefore, if risk is a human experience, it is closely tied to the interactions in human systems (soft systems). It then follows that risk will exhibit the same complex and chaotic patterns as the human interactions it is derived from. In other words, in an organizational environment, risk will emerge and evolve in complex and unpredictable ways.

4.3.3 A simple example risk situation in an organization

Mindful of this fundamental nature of risk in organizations, I will explore through a few simple examples the problems that can arise when we apply our current models and thinking about identifying risks.

Consider the human system interactions at a procurement department within a fictitious organization. This procurement department is responsible for managing suppliers and ensuring timely delivery of key supplies that are used by the organization to produce an end product. Even though there are standards and processes in place to govern the interactions, on a day-to-day basis there is virtually an infinite array of interactions, events and situations that could unfold in unpredictable ways.

Let's say this organization has established a category or definition of 'supplier risk' (e.g. a significant disruption to key supplies), which is used by procurement to represent the possibility of such an event occurring. As interactions evolve over time in and around the procurement department, an example range of the potential threats perceived could be:

1. The procurement manager, who knows supplier 'A' well, perceives a potential problem emerging within the supplier's operations, which could cause a major disruption to supplies. The manager also has a concern about an emerging strike threat in the distribution channel between supplier 'A' and the organization, which may also cause a disruption to supplies, but a different type of disruption to the first threat (e.g. bigger or smaller, or different material).

2. A seemingly insignificant change to the processes at the loading dock has caused a procurement operational employee to see new risks at the dock area. He perceives there is a risk of a disruption to supplies getting into the processing division through an accident or spillage due to the way unloading is performed. The operational employee also works closely with supplier 'A' and he notices another issue (potentially unrelated to the above threats) brewing between supplier 'A" and one of its partners, which could also cause delays in supply delivery.

3. A finance person who works closely with the procurement department notices a potential legal dispute brewing between supplier 'B' and another party, which could have legal implications for the organization and also delay supply deliveries. The legal situation might also affect suppler 'A'. The finance employee also perceives a cash flow risk to the organization through delays or disruptions to supplies. This is because delays will affect production, therefore sales, therefore cash coming into the door.

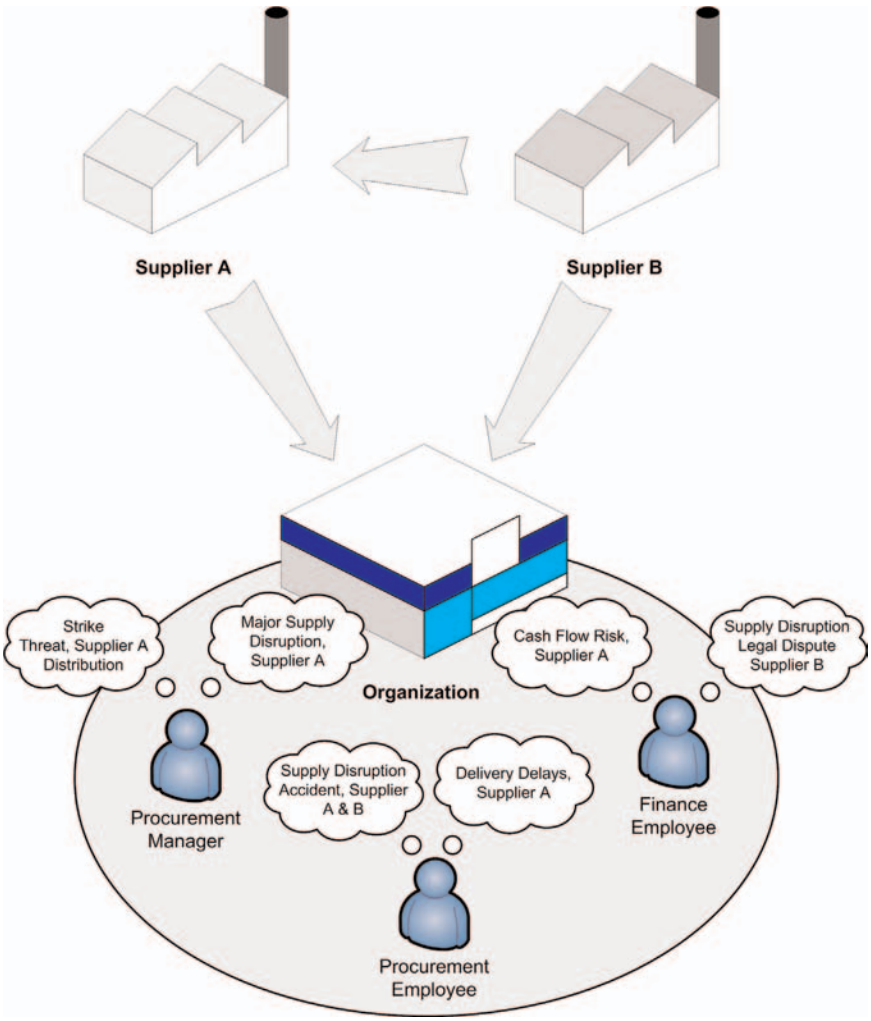

Figure 1: Procurement Example

4.4 Problems with the model for unique risk

As discussed in section 4.1 – "Current thinking on what constitutes a unique risk", identifying a unique risk simply involves naming the event (whichever way you like) and assigning values for the risk (e.g. likelihood and impact). Though it might not be clear at first glance, this model for identifying risk is designed for hard systems. For example, a game of dice is a form of a hard system (assuming, of course, that the dice are fair and the rolls are random). This is because the content, the processes and the rules of the game are fixed and simple. Therefore, the nature of risk in this game doesn't change. The risk in this game is always the same, if your numbers don't come up you lose. The nature of the risk event doesn't morph into complex and unpredictable arrangements. Therefore, we do not require anything other than a simple model for identifying a risk in a hard system.

However, if we apply the simple model for risk identification to the procurement example (a soft system), significant problems start to emerge. Importantly, we find that a fundamental principle behind the simple model for risk identification no longer applies. This principle is that the boundaries that separate a risk from other risks and non-risk situations are clear and static.

In the procurement example, how do we determine what is 'supplier risk', and what is another risk"? Is the strike threat in the distribution channel a supplier risk, or is it 'distribution channel risk', or is it 'strike risk', or something else? Are the loading dock issues (spillage or safety incident) 'supplier risk' or something else? What about the dispute between supplier 'A' and one of its partners? What about the cash flow risk example, is this supplier risk, is it 'cash flow risk', or is it something else? Couldn't they all be 'cash flow risk' potentially? But is this a helpful way to identify them? For example, defining the legal dispute between supplier 'B' and a third party as 'cash flow risk' blurs and confuses our understanding of the situation. Yet the same argument applies if we define all these risk situations as 'supplier risk'.

Another approach to this situation might be to let everyone identify the risks as they see them. But once again, problems emerge. For example, our finance person identifies 'cash flow risk' as potential delays in supplies. But what has she included in his definition and what has she excluded? Are all the risk situations described in this procurement environment included, or only some? Has she included the health and safety issues or not? Is she even aware of all the risk situations? What do the procurement manager and the procurement operational employee identify as risk? Won't their risk situations already be accounted for in the finance person's risks? Won't there be overlap between their examples of risks? Where and how do you draw the line? Moreover, how can you possibly maintain that line, when new and different situations are constantly emerging that haven't been thought of previously? In this procurement environment example, there are many overlaps and linkages between the risk situations that are either hidden or only partly evident.

As can be seen from the above discussion, the simple model for risk identification creates many problems. These problems create misleading and confusing impressions about the risks in the procurement department example and consequently will also produce misleading calculations on the size of the risks. The important point to note about this procurement example and the problems it raises about risk identification is that this is just one simple example in one small part of an organization. If you expand this examination across an entire organization the confusion and problems created can become mind-boggling.

In the following sections (4.5 – 4.8) I will discuss problems with the identification approaches described in section 4.2 – "Approaches used to identify risks in organizations".

4.5 Problems with top-down identification approaches

A perceived benefit of the top-down approach to identifying risks is that it tends to avoid the problems discussed in the previous section by concentrating on the major risks facing the organization. Therefore, the complexities that arise from trying to identify many smaller risks are avoided. While on the surface this approach appears reasonable, it is based on several fundamental misunderstandings that create a number of problems for organizations. These misunderstandings relate to the nature and behavior of risks in organizations. They can be described as:

- The misunderstood effect of 'minor' risks on an organization
- The misunderstood concept of major or strategic risks

4.5.1 The misunderstood effect of minor risks on an organization

Minor risks collate into a very big risk exposure.

Risks that are often deemed as 'minor' in relation to the organization as a whole in fact play a substantial role in the successes and failures of an organization. For example, if some of the risks identified in the procurement example were to occur, they might have an impact of only $50,000 or so in overall cost. In a large organization with revenues of, say, $5billion and upwards, spending time on trying to identify and deal with these risks might not be an effective path to take when there may be other much larger risks that need attention. However, the problem with this type of reasoning is that a large organization faces a large number of these 'small' risks, probably many thousands of them across its operations. And if you multiply $50,000 or $100,000 by several thousand you end up with a very big risk exposure. Therefore, using a very rough estimate, a large organization may be carrying hundreds of millions of dollars worth of risk exposure, which has either being misjudged as 'small' and given low priority, or completely neglected through any formal process.

The 1000s of minor cost items are not ignored when producing performance views, why should the 1000s of 'minor' risk be ignored when building forward views?

When an organization measures financial costs in an area of its operations it does not just capture the five or ten major cost items, and ignore the 1000s of other 'minor' cost transactions, it captures them all. If only a few major cost items were captured, a fragmented and misleading view of performance for that area of the organization would be produced. Yet strangely, the same thinking doesn't apply to producing the forward view for an organization when using top-down approaches to identifying risks. Through top-down approaches we capture 10 or 20 risks and we present this as the key risks the organization faces in its forward view. The clear implication here is that the thousands of other risks do not matter. You would never hear an accountant talk like this about cost data.

Top-down approaches are by nature designed to ignore the majority of risks facing an organization. Relying on the flawed logic of top-down approaches will result in a fragmented and misleading view of the exposures facing the organization.

Minor risks can quickly cascade into a major disruption.

As discussed in section 4.3.2 – "The nature and relationships between an organization and risk", an organization is continually faced with new experiences, situations and events unfolding across its sphere of operation. Risks will therefore not emerge in neat categories and clearly telegraph their intent. It is often at the edges or small pockets in our organizations from where a big risk can quickly emerge. Minor risks can very quickly cascade into larger risks, and then on to major incidents, which can seriously disrupt an organization. For example, the seemingly small process change at the loading docks in our procurement example that created the 'minor' risk relating to a spillage or injury incident could emerge as a major incident that shuts down the supply process for a significant period of time.

Given that there are potentially thousands of these 'minor' risk situations across an organization, an organization cannot possibly capture the important risks it faces by running a top-down identification process based around a few workshops with sen-

ior management once a quarter or half yearly.

Leaving operations personnel to deal with minor risks on their own creates more problems.

An argument sometimes used for the problem of a large number of 'lower level' risks is that personnel at these levels will address these risks as part of their job specification. In other words, personnel are expected to recognize and deal with issues and risks as part of the process of doing their jobs properly. This thinking is flawed on two counts. Firstly, personnel are likely to be less attuned to, or concerned about risks than they should be if they have no formal mechanism to guide and prompt their thinking and perceptions. They are therefore likely to react to a risk at a later stage in its development, for example, when the risk is a lot bigger (requiring more effort and cost to treat), or when it no longer is a risk and has become a problem (requiring even greater effort and cost to treat).

Secondly, there is the problem of measurement. As discussed in chapter 3 – "Measuring", a majority of measurements of the size of the risk are likely to be misleading. As discussed in this chapter, in two out of three cases the assessment of the risk is either an overestimate or underestimate. Accordingly, personnel will either overact or under react to most of the risks they perceive. Therefore, leaving personnel on their own to deal with risks is creating a further cost to the organization.

4.5.2 The misunderstood concept of major or strategic risks

Major risks are perceived as potential events that could disrupt or affect an organization in a severe way. Often these major risks can be referred to as 'strategic risks' because if they were to occur, the consequential effects would be long term impact across many aspects of an organization's operations. When defining major or strategic risk, organizations will tend to weigh the potential consequential effects of the risk more than its likelihood of occurrence. Therefore, if there is at least 'some' chance it could occur, and its consequential effects are very large, organizations will tend to identify these as major or strategic risks.

It is often believed that these types of risks can be relatively easily 'spotted' or identified, there are typically few of them in number (i.e. in the tens) and that senior personnel are generally the ones who should identify them. However, there is a significant misunderstanding in the risk management literature about the nature of these risks, which is creating a dangerous illusion about the risks an organization faces. This misunderstanding can be easily demonstrated through our procurement 'supplier risk' example.

The problem with the concept of major or strategic risk through a simple situation.

Under any top-down approach to identifying major or strategic risk, senior management at our fictitious organization would have identified 'major disruption to key supplies' (or something like this) as a key risk. They would recognize (and rightly so) that any major disruption to key supplies would have a significant impact on the organization's ability to meet its objectives. From this 'identified' major or strategic risk, the organization would attempt to put in place controls to mitigate this risk. For example, strengthen the links to its key suppliers; build a level of redundancy in the supply chain, and so on.

The problem with this approach is that the risk of 'major disruption to key supplies' is not a single, easy to identify unique risk. In this case the 'major risk' is more accurately an area of risk in which many risks are potentially present. Yes, there could be a generic disruption with supplies that could be labeled 'major dis-

ruption to key supplies', but the type and range of major disruptions could be immense (as indicated in section 4.3.3 – "A simple example risk situation in an organization"). Therefore how can our fictitious organization effectively manage or mitigate this 'risk area' without understanding the types of major failures or disruptions that could occur? The only way the organization could understand the types of failure and disruptions that could occur is by understanding the types of risks it faces in this area.

In the procurement example we saw many different types of 'supplier risk', for example, legal disputes, health and safety issues, strike threats and distressed supplier organizations. All of these risks could potentially manifest through a variety of ways and locations. Any one or combination of these could lead to a major disruption. How could senior management be aware of these risks? How can the organization tailor appropriate control activities or treatments, without detailed knowledge of these lower level exposures? Relying on senior management provides a superficial high-level view, from which the organization can only develop superficial high-level treatments. These are treatments that will be unaware of the true nature and evolution of the exposures in the procurement division. As a consequence, these treatments will be ineffective and costly.

In an attempt to deal with this, we are forced to move back towards a 'bottom up' approach to understanding the exposures facing an organization. In other words, personnel at the coalface identify the types of exposures facing their particular activities, as they perceive them over time. However, if we take this approach we return to the problems outline in section 4.4 – "Problems with the model for unique risk". Under current models and thinking in risk management, there appears to be an impasse.

I will now explore the problems with major or strategic risk through a more complex example in order to further highlight key failings in current top-down thinking and practices.

The problem with the concept of major or strategic risk through a complex situation

Let's say there is a European luxury sports car manufacturer, which is considering moving into a new market segment. This car manufacturer (who we will call 'Sparc') is a market leader in high-end sports cars. Sparc perceives that its product range is somewhat limited, relative to many of its competitors. It fears that its opportunities for long term growth will be stifled through a product range that only targets a small niche within a very large car buyer market. Sparc also fears that other much bigger car manufacturers are encroaching on its traditional space.

Sparc management are considering a move into the sports utility vehicle (SUV) market. An SUV is a very different type of vehicle for Sparc to produce. However, Sparc management feel that there is an enormous opportunity for growth across the world, and especially in the US market. They believe they can leverage off their sporting brand and produce an SUV that can find a strong niche in this market.

The SUV market is not a green field environment. There are many SUV models already on the market, and several other luxury sports car makers already have SUVs released on the market, or are about to release models.

Sparc has conducted some preliminary groundwork. They have developed designs, built basic prototypes, assessed the market behavior, investigated the required set up in their factories to produce the vehicle, and developed numerous forecasts and budgets.

Sparc is ready to proceed with this major new strategic initiative. It would be fair to assume that the risks that could de-rail this initiative would be of critical importance. Sparc will therefore have a keen interest in understanding the major or strategic risks it faces, and ways to deal with them effectively. Sparc will likely apply a top-down approach to understanding and dealing with the major risks it faces.

Before I consider any top-down approach to risk identification, I will perform a simple analysis on Sparc's proposed new venture to get a general understanding of the risks Sparc may be facing. To manufacture and market a new model vehicle

into a worldwide market requires a very complex mix of activities and decisions over an extended period of time, and through the backdrop of an uncertain and rapidly changing world. Many situations and events could emerge and evolve in complex ways and generate significant risks. Some of these situations and events have been highlighted through example events below.

Competitor Actions

Event/Situation: Pricing
Competitors begin a new aggressive pricing strategy in key markets; this sets new expectations on price. This affects expected profitability for Sparc. Competitor pricing varies unexpectedly across different regions, creating further pricing and therefore profitability pressures on Sparc's new product.

Event/Situation: New Models
Competitors release new models that set new or different expectations in SUV market. This undermines sales volume for Sparc's SUV.

Event/Situation: Marketing Strategies
Competitors develop new marketing campaigns that prove successful in key markets. This creates greater pressure on expected sales for Sparc in these markets. Sparc have to counter with new approaches to market, cost increases in marketing are the result.

Market Trends

Event/Situation: General SUV Market Trends
SUV market preferences begin to change. Following some bad SUV press, smaller style SUVs are now the growing SUV preference. This affects Sparc as their SUV is in the large style.

Event/Situation: Preference Changes by Region
Customer preference changes vary across markets, unexpectedly. Some markets begin to lose their fascination with SUVs, while others begin to prefer different styles of SUVs, while some others don't change their expectations. This effects Sparc sales volume projections across different markets, causing extra cost overheads and revenue pressures.

Product Design

Event/Situation: Issues with Aesthetics
The Sparc design is not liked in certain markets. Indifferent press to design affects sales

Event/Situation: Issues with Regulations
Regulatory changes in some key markets cause issues with aspects of design. Example, ride height, emissions, noise, dimensions. This slows delivery to these markets, as costly adjustments need to be made.

Event/Situation: Fraud/theft issues
Key information on designs goes missing or is stolen prior to the release of Sparc's SUV. This creates concerns and issues potentially affecting the organizations plans and reputation. The missing information comes out in the press, giving competitors more time to develop their responses. The press, without contextual information, misunderstand the designs and ridicules them. Sparc is forced to put time and money into clarifying and defending the designs.

Brand Backlash

Unexpected levels of backlash against Sparc's core product models develop in some markets. In some markets, the SUV is perceived as a 'sell out' to the company's core principals as a sports car manufacturer. Coupled with negative press in some of these markets, there is a growing belief amongst potential buyers that the true sports quality is no longer there in the brand. A significant alluring quality in the brand has been its exclusiveness as a purely sports car manufacturer.

Production

Event/Situation: Supplier Issues
Various unexpected supplier problems develop over time. For example, supplier distress, supplier and Sparc disputes, industrial action at the supplier, supplier product quality issues, wrong product, and so on. All of these situations create delays in production. This adds unexpected costs to the production process, and also causes Sparc to miss delivery dates to key markets, which impacts sales.

Event/Situation: Manufacturing Issues
Various unexpected problems surface in the manufacturing process for the SUV. For example, various industrial disputes, different stresses and strains in processes cause breakdowns in machinery, safety accidents, damage to key machinery through unexpected accidents, and so on. This adds unexpected costs to the production process and slows delivery of product to markets. This also impacts sales.

Event/Situation: Infrastructure & Support Issues
Various problems and issues with computer support systems. For example, breakdowns and miscalculations in programs, which affect product, delays in administration are also experienced. This creates further delays and adds costs to the production environments.

Event/Situation: Distribution Issues
Various unexpected problems and issues across distribution channels and environments develop over time. For example, a major incident at a key distribution channel slows delivery of product to major market. This slows sales, frustrates potential customers in this market. Competitors take advantage and some sales are lost.

Product Recalls

Several unexpected faults emerge that require a product recall in some key markets. Bad press further exacerbates the situations, and aggressive competition looks to take advantage. This adds further costs and slows sales of product in some key markets.

Financial

Event/Situation: Currencies
Unexpected currency movements create pricing pressure on product in key markets. Local competitors in this market are able to take advantage and price more aggressively. This slows sales and impacts profit margins.

Event/Situation: Oil Prices
Large hike in oil prices starts to discourage potential SUV buyers. A shift in market preferences emerges in some key markets away from SUVs. This affects Sparc's projected sales volumes in these markets.

Even though the above examples are a simple high-level analysis of possible risk situations, it can be seen that by further decomposition of each situation, there would be many thousands of potential risk situations that could significantly disrupt Sparc's SUV venture. Moreover, each of these thousands of risk situations can combine and cascade together in many complex ways, creating potentially hundreds of thousands of risk situations; any one of which could have a major negative effect on Sparc.

These are not widely unrealistic risk situations. It is quite reasonable that any of these combinations could occur. For example, design issues, combined with changes in market trends in some key markets (e.g. growing preference for smaller SUVs), combined with currency changes (causing pricing issues) and combined with new tactics by local competitors in these key foreign market could lead to significant negative effects on Sparc.

How do Sparc know which of these 100,000 risks should be looked at and which ones to leave, when they could all be potentially significant? How do Sparc prioritize and determine a 'top 10' or 'top 50'? The answer is, under any current approach to risk management, they can't.

Through a top-down approach to identifying the 'major' risks, Sparc management would have come up with a list of obvious choices. Though these choices would have been defined as unique risks, most of them would in fact be 'areas of risk'. In other words an identified major risk would in fact be a composite of possibly many hundreds of risk – risks that would be poorly understood and any one of which (or any combination of these risks) could have a significant impact on Sparc. Any mitigation strategies subsequently developed from these high-level risks would likely be highly ineffective and costly. Sparc management would in a sense be deluding themselves about the major risks they would face in undertaking this significant strategic objective.

In some instances, major risks can be clearly identified through a simple top-down exercise with senior management. For example, in cases where a commodity is used as a major component in the input or output stage in a business operation or venture, the variations in the price of the commodity can have significant cost implications. In these cases, it is not difficult to identify the scenario and its end effects. It is also not difficult to devise effective mitigation strategies that directly target this major risk (for example hedging the risk through a market contract).

However, in most situations the majority of the 'major' risks in a complex organization (or new venture) cannot be clearly understood through a top-down process with senior management. This is a fundamental consequence of the real world. A top-down approach works on the assumption that it is assessing an environment that is relatively stable and predictable, in other words, a hard system. Organizations, and the major activities organizations undertake, are highly complex and experience unpredictable change – they are complex soft systems. By extension, risk in organizations behaves the same way.

Top-down approaches can provide important contextual information about the risks an organization faces, but relying on these approaches to do any more than this can be a dangerous and misleading exercise.

4.6 Problems with cause and effect models

Cause and effect models such as PRA and derivatives of this approach can in some cases be a useful tool for identifying risks and their structures. These approaches purport to "unravel a relatively complex event to derive a component of simpler component events, whose probabilities and consequences have a better prospect of being estimated" (Bowden, et al, 2001). However, applying cause and effect models in soft systems (such as an organizational environment) must be used with caution. This is because they can create a misleading illusion about what risks are present, the nature of these risks and their behavior.

Cause and effect models are built on several key assumptions. These are:

- The linkages between steps in a cause and effect chain are fixed and static
- There is a clear start and end point in the cause and effect chain
- Reductionism will provide a more accurate measure for determining the overall likelihood of an event occurring.

While these assumptions will generally hold true for a hard system such as a mechanical or electronic machine, they do not hold for the complex interactions that take place in organizations. The incompatibility of these assumptions with a soft system can be demonstrated through the procurement example in section 4.3.3 – "A simple example risk situation in an organization".

Steps in cause-effect chain are not fixed or static.

In the procurement example, a cause-effect chain can be constructed from supplier failure through to cash flow risk. For example:

- Supplier failure ➜ Stop in supplies ➜ Stop in production ➜ Stop in sales ➜ Stop in positive cash flow

If we delve into one of the links between any of the above events, we find that the links are neither static nor fixed. For example, if we examine the link between 'supplier failure' and 'stop in production' we will likely find many layers of very complex cause and effect sequences. For example, a financial related problem, a technical breakdown, a safety accident, or a legal dispute with another customer could be the form of 'supplier failure' that creates the link to 'stop in supplies'.

These examples of 'lower-level' links will continually change over time. At some point in time a dominant link could emerge that could create the event 'stop in suppliers', while at a later point in time, that same link could subside and have little effect on the next event. Each of these 'lower-level' links will themselves comprise of many links; for example, within 'financial related problem' there are potentially numerous situations and events that can create the financial problem. Yet there is no sequence or order to how these candidate links between 'supplier failure' and 'stop in supplies' will behave. The influence of any one or composite of these links on 'stop in supplies' will fluctuate constantly over time.

As a result, attempting to derive a stable and meaningful quantitative value for the link between supplier failure and stop in suppliers becomes a virtually impossible task. Accordingly, this predicament continues for all other links in the chain.

There is no definitive start and end point

Superficially, the start and end points in the above cause-effect chain seem correct. But within a soft system, there are no definitive start and end points. By nature, they can cascade and loop in complex ways. A simple linear view of cause and effect will not easily bring you to the logical start and end of a chain. For example, why not consider the steps before 'supplier failure'? There could be a number of important factors that could initiate a 'supplier failure' such as emerging problems with a key customer, change in economic conditions, actions by a new competitor, and so on. We could just as reasonably start the chain at 'stop in production'. Accordingly, why end at 'stop in positive cash flow'? What about subsequent events triggered from the loss of positive cash flow, such as insolvency problems or reputation damage? Key 'end events' such as loss of key customers or safety accidents (caused by cost cutting measures to shore up cash flow) could also manifest from 'stop in positive cash flow'. Therefore, without a clear logical (or physical) start and end point, the derived figures for the likelihood of failure are somewhat arbitrary.

Reductionism will not automatically provide more accurate measure of risk

As can be seen from the above discussion, breaking down the risk situation into smaller components (such as a cause-effect chain) will tend to uncover more complexities, rather than simplify the situation. Attempting to derive a probability measure for underlying 'lower-level' links is more difficult. This is because the lower level link/event is likely more unique, therefore less suited to a statistical or mathematical interpretation.

4.7 Problems with risk identification by categories and classifications

As discussed in section 4.2.3 – "Identification by categories and classifications", risk categories are often used in organizations as a guide to identifying risks. I also mentioned that the category approach has taken on a far more significant role in finance and banking institutions. While there may be some legitimacy to using a more elaborate category approach for finance and banking environments, there are fundamental shortcomings with the category approach. These shortcomings can create a number of problems that significantly undermine the value of this approach to identifying and measuring risk.

Categories: Where do you draw the line?

In section 4.4 – "Problems with the model for unique risk", I examined the problems with applying traditional identification approaches to identifying risks within a soft system. Establishing meaningful boundaries between risks in a soft system is near impossible. Soft systems produce layers upon layers of risks that interconnect and overlap through complex arrangements that are constantly changing. The use of categories as the means of identifying risks further exacerbates the problems. This is because the category method is a far cruder approach to identifying risks than any other approach. Categories will tend to be small in number, for example, in finance environments some banks use eleven categories (or 'loss types') for operating risk (Peccia, 2001).

With fewer ways of identifying risks, gaps will be greater. Certain risk situations and events will not be picked up through any organizational system, or if they are, they will be wrongly identified through one of the existing categories.

Overlapping situations will be significant as many risk situations could easily fit into more than one category. For example, we saw in section 4.4 – "Problems with the model for unique risk", several risks could have easily been placed within any one of 'cash flow risk' or 'supplier risk' or 'health and safety risk' categories. With a crude high-level category system as a means of identifying risks, the placement of risks that potentially fill multiple categories will be arbitrary across the candidate

categories. This is because there will be no formal system to recognize and sort risk identities at lower levels.

Category method creates isolation and alienation.

As discussed in section 4.2.3 – "Identification by categories and classifications", category approaches to identifying risks are usually employed so that large volumes of data can be amassed and analyzed statistically. The analysis of the risk data will typically involve using specialists outside of the business operations (e.g. risk managers, actuaries, external consultants). This approach has a dual negative effect on the organization.

Firstly, the statistical specialist will be isolated from the complexities and nuances of the business operations that their analysis is supposed to represent. They will be driven by the needs of the formulas, rather than the true nature and behavior of the exposures faced by the business operation. Yet this need to quantify uncertainty creates an illusion of certainty about the future. This is a dangerous sentiment in a world that is becoming increasingly complex and interconnected (Jaeger, et al, 2001). Quantifying requires a high degree of specialization and abstraction. This removes the risk assessment from reality; encourages overconfidence by the assessor, and the exclusion of relevant information (Nowotny, 1976).

Secondly, the business operations will be alienated from the risk assessment process. The business personnel will understand intuitively that the risks they face are complex and dynamic. The simplistic statistical representation of the exposures they face, produced by outsiders, will not accord with what they intuitively understand.

Category approaches encourage backward viewing, instead of forward viewing

Rather than being attuned to the constantly changing situations and events faced by the organization, which can generate new experiences of risk, the category approach forces a backward viewing ethos on the organization. This is because, in the quest for 'valid' measures, users of category approaches are pre-occupied with the process of amassing historical data on risk failures.

By emphasizing a backward viewing approach to risk, the organization is limiting its ability to develop effective responses to deal with risk. Specifically, the organization will limit its ability to devise tailored and effective responses to treat emerging or changing risk experiences. Instead, the organization will predominately rely on crude insurance models to hedge a 'priced' risk, be that through the financial markets or capital reserves.

These insurance or hedging models of treatment are designed to work on generic exposure 'templates'. That is, the exposure is classified and defined in general terms only. These approaches work well where the risk category is stable and large amounts of data can be relatively easily gathered. For example, 'risk of lung cancer through regular smoking'. This is an easy to understand category, for which statistical data can be easily generated and a level of risk can be derived and priced.

When we look at the risks and the way they can emerge through the procurement example or the Sparc example, we find a complex soft system. An environment in which risk is constantly emerging and morphing into new and unpredictable forms, where relationships between risks are complex and always changing. This is not an appropriate environment for category identification models.

4.8 Problems with models avoiding individual risk identification

While this approach can provide a high-level understanding of the flows, infrastructure and vulnerabilities across an organization, it suffers from a number of problems that limit its value as a means of understanding the nature and behavior of risks facing an organization. This is because methods of identifying risks or 'discontinuities' that fall under this approach are another form of top-down risk identification.

As discussed in section 4.5.2 – "The misunderstood concept of major or strategic risks", senior management will not be fully attuned to the nature and behavior of risks facing their operations. They may well be able to identify potential discontinuities or vulnerabilities, but that is not a difficult job to do. The difficulty comes when deciding what to do about it. In section 4.5.2 I proposed that a major or strategic risk is often an 'area of risk' where many hundreds of risks could reside. This also applies to definitions such as 'discontinuities' or 'vulnerabilities'. Therefore, without knowledge of what those risks are and how they behave or where and when they emerge, mitigating their effects can become a costly and ineffective exercise.

For example, let's consider the loading wharf example in section 4.2.4 – "Models avoiding individual risk identification". In this example, it was proposed that an identified vulnerability to the organization could have been overcome by upgrading a second wharf, thereby improving the 'resilience' in the supply of raw materials. On the surface, this approach can appear reasonable. However, there are potentially hundreds or thousands of risks at a wharf operation, most of which management, or those performing a vulnerability analysis, would not be aware of. Therefore, how can the organization make an effective decision on how to build resilience in the raw material distribution? Say the upgrade of the second wharf cost $500,000. How do management know whether or not the $500,000 is a reasonable investment, when they don't understand the intimate nature of the risks they face in the first wharf? The risks they face in the first wharf may be treatable for a lot less than $500,000, and still provide the same level of overall resilience to the supply of raw material.

Some approaches suggest running regular workshops with management and 'war gaming' scenarios to flesh out the different ways disruption could occur (Star, et al 2003). However, this approach still leaves an organization with problems. Firstly, management would struggle to get any core business work done, because they would forever be in workshops 'war gaming' their business operations. And secondly, as the organization starts uncovering more and more risks, they would be faced with the same problem of risk identification as outlined in section 4.4 – "Problems with the model for unique risk".

4.9 Poorly identified risks create 'unexpected' problems

If the shortcomings with risk identification, as I have outlined in the preceding sections are accepted, then a broader question needs to be asked. That question is; if risk identification is in such a sorry state, shouldn't organizations be failing constantly? Wouldn't there be risks emerging 'out of nowhere' and constantly derailing organizations throughout the world? In fact, organizations do fail constantly throughout the world. Even organizations that are generally prosperous experience many major disruptions to their operations and plans through their lifetimes. In many of these cases, there were warning signs (or risks) flagging the danger, which where not properly understood, or understood by a few and not by the organization's measuring systems.

I would also argue that another important sign of poor risk awareness can be recognized through the 'unexpected' problems that constantly pop up throughout an organization's operations and plans. Individually, these problems are not necessarily major events. They are often small incidents or situations causing a delay here; a small cost overrun over there and continual stresses and strains across the organization's processes.

In the procurement example an employee perceived a risk at the loading docks – a potential accident or spillage. This risk, if it were to occur would become a problem (i.e. an event that has happened). The problem may only result in a small delay, say a half day slow down at inbound goods, and the cost to the company, though not easily traceable, might have been about $50,000. Local management would have likely passed off this event as an 'unexpected problem'. Staff and management would work quickly to repair any damage and get back on track.

Because the cost impact may not have been easily traceable, the causes of this problem are not clearly identified in any information system. The risk aspect to this problem would remain hidden from the organization's consciousness. The potential savings that could have been made by recognizing the risk and either mitigating or avoiding it, before it became a problem do not register.

Situations as described above are not are rare events. There would typically be many of these situations occurring constantly throughout an organization. Collectively they can place a significant cost burden on an organization. But this cost burden is not well recognized. Often, the organization's personnel absorb the cost by working harder to overcome the hurdles created by the unexpected problems. Therefore, the overall effects from many of these unexpected problems do not register in any formal way through the organization's system, but ultimately, the stresses and strains on organizational personnel and processes stifles performance.

While organizations may not have formal systems to track the cost from unexpected problems, they do recognize that they face a constant flow of unexpected problems. This is why when hiring people, organizations will place a significant value on good 'problem solving skills'. 'Problems will always pop up, and we need to be able to solve them quickly and effectively', so goes the thinking of the organization.

However, the key point about unexpected problems that is often missed is that before an unexpected problem existed there was a risk of that problem occurring. In many cases, the risk was recognized by someone or group in the organization, but not the organization's measuring systems. A new mantra for organizations, appropriate to today's world may be to place more value on risk awareness and management skills; but awareness is only achieved through an ability to identify.

4.10 Identifying risk in organizations requires new thinking

In summary, it is important to note that organizations fail and succeed for all sorts of reasons. Sometimes the success or failure is in the control of management; sometimes it is not. It would be fanciful to believe that with a significantly improved approach to risk identification organizations will never fail or have unexpected problems. However, the key question to ask is, if organizations had a fundamentally better approach to understanding and dealing with risk, would not their success be greater (or more consistent), and would not their failures be less damaging?

As I discussed, current approaches to risk identification are fundamentally flawed. They are designed for identifying risks in hard systems, rather than identifying risks in the complex environments that organizations operate in. Most of the problems with the approaches to identifying risks stem from an inability to clearly define what constitutes a unique risk and how a unique risk may relate to other similar risks.

A new model is required for defining the uniqueness of a risk; a model that is cognizant of the nature and behavior of risk in complex systems; a model which can deal with the complex relationships, gaps, overlaps and confusions that plague current approaches to risk identification; and a model that can directly involve potentially thousands of personnel, with diverse skills and backgrounds, in the risk identification process.

Chapter 5

Tracking Change

5 Inability to deal with change in organizations

As discussed in section 4.3.1 – "An organization is a soft system", an organization, with its complex levels of human interactions will experience change continuously throughout its sphere of operation. Risk, which is closely tied to human interactions, will display that same level of change in an organizational environment.

How do the models of risk and risk management take account of the changes experienced by risk in a complex soft system such as an organization? The COSO enterprise risk management framework, for example, doesn't place much emphasis on change in risk. It describes activities such as 'monitoring', but these relate to attempting to assess the overall effectiveness of the risk management program itself, rather than any process or model to understand change in risk (COSO, 2004). The AS/NZS 4360:1999 risk management standard, under 'monitoring and review' briefly discusses the need to monitor risks. It states that risks should be reviewed regularly as part of any risk management treatment plan (AS/NZS 4360, 1999).

While some of the risk management literature may talk about the need to regularly review risks, there is little evidence to show any appreciation of the complex nature of change in risk and what this can mean to an organization. There is no model or new thinking that recognizes risk as part of a complex soft system.

5.1 Changes experienced by risk

The types of changes that risk can experience in an organizational environment can be categorized as follows:

- Change that alters the size of a risk
- Change that generates new layers of risk.

5.1.1 Change that alters the size of a risk

The 'size' of the risk can, in a general sense, be defined by the likelihood of its occurrence, and by the potential impact or consequential effects. These two aspects of the size of the risk can be affected through two different change actions.

The first type of change action that can alter the size of a risk is through the underlying conditions which generate the risk. These conditions can change such that the risk's likelihood of occurrence and or potential impact can get either bigger or smaller. For example, in the fictitious procurement department (section 4.3.3 – "A simple example risk situation in an organization") the risk of supplier 'A' failing can change due to the underlying conditions which generated the risk. Supplier A's distress levels might increase appreciably due to failure of a major financing deal it was hoping would protect it from insolvency. The failure of the financing deal is a change in the underlying conditions. In this case the likelihood of the failure (and the potential impact) may increase significantly.

The second type of change action that can alter the size of the risk can occur through the organization responding to the exposure in some way. For example, the organization may attempt to treat or mitigate the risk of supplier A failing by setting up an option for back up supplies from another supplier, or maintaining a higher level of inventory of the raw material. Through these types of actions the organization will change (lower) the size (potential impact) of the risk. That is, the back up supplies (either through another supplier or through in house reserves) will be used if there is a failure of supplier A, thereby mitigating its potential effects on the organization.

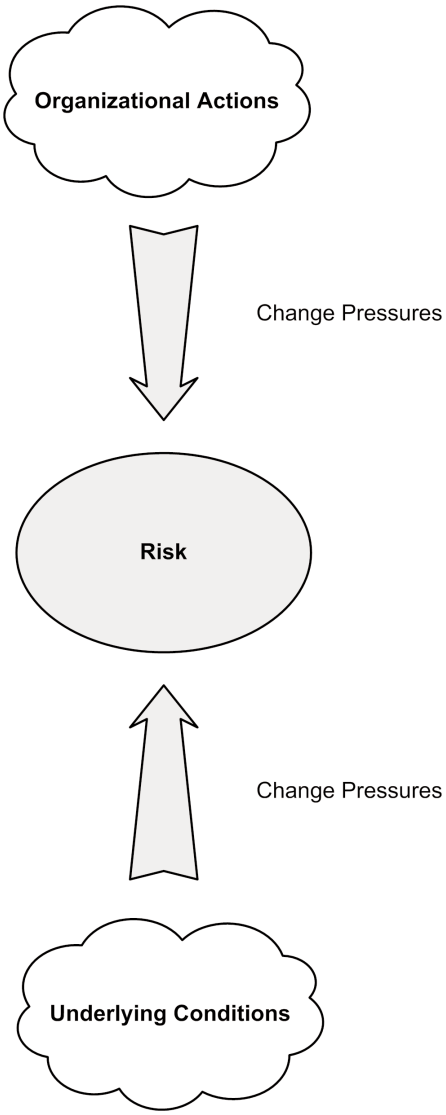

Figure 2: Risk change pressure

The critical point in relation to these types of change experienced through the size of the risk is that the change is not experienced in a simple serial way. In other words, the underlying conditions don't change once and remain stable so that a treatment can be applied to the risk; and the risk does not remain stable at a new level (size) after the treatment has been applied. Both these forces of change will interact through the risk in complex and unpredictable ways. This complex environment of change has significant ramifications in an organization, yet the ramifications are poorly understood.

The ramifications can be shown through the procurement department example. Let's say the organization has recognized there is a risk to the disruption of supplies through its main supplier incurring some problems. In response the organization is putting in place a backup strategy to maintain continuity of supplies. The organization has assessed that the back up response will work up to a certain level, which it has based on the perceived size of the threat to the supply of raw materials. During implementation of the back up strategy, the underlying conditions that set the size of the risk change. There are two possible ways the underlying conditions could change. In one scenario the risk could go down significantly. It could be that the key supplier has sorted out its financial issues. In a second scenario the risk could become far greater. The key supplier could now be facing major problems, which could shut down its operations for a prolonged period of time.

The question that now needs to be asked is how appropriate is the supply continuity strategy under the changed conditions? In one scenario, the continuity strategy is 'overkill'. The conditions for the supplier have changed for the better, probably in a sustained way. Therefore, in this case the organization will be spending too much effort and cost relative to the threat it faces. In the second scenario, the continuity strategy is insufficient. The conditions for the supplier have changed for the worse, and the backup strategy is incapable of serving its aims. Therefore if the risk were to occur, the organization will still be faced with extra costs and revenue losses.

It could be argued that it's important to have a backup strategy in place, irrespective of the current condition of the supplier, because things could change for the better or worse in the future, or another type of failure could occur elsewhere in the supply chain for which the back up strategy could be used. But the problem with this type of thinking is that the backup strategy was designed for a certain type and size of failure, therefore, it is not going to be effective and efficient for other types of failures. It will either be too much or not enough.

It could also be argued that if the organization follows risk management (or good general management) principles and performs regular reviews, then it could adjust its continuity strategy to suit the prevailing conditions. However, this line of thinking is too simplistic, and ultimately flawed. How often are 'regular reviews' of risk response strategies conducted in an organizational environment; quarterly, half yearly, yearly? Irrespective of the period of review, the problem with the periodic approach is that it assumes a consistency in the cycle of change experienced by an organization. That is, if a review is conducted half yearly, then the underlying assumption is that any significant change will occur at that time interval. Therefore, the review process will pick up the change at the appropriate time. The problem with this thinking is that change does not occur in an orderly fashion within an organizational environment. As a complex soft system, it faces continuous and unpredictable change. The whole world could change before the period of review is due.

The critical point that must be noted in this discussion is that an organization does not have a few risks that are subject to continuous and complex change to contend with, it faces many hundreds or thousands of changing risks. Therefore, most of its responses to the risks it faces are, at any point in time, likely to be an overkill or insufficient. Under any current risk management or general management practice, this level of change is virtually impossible to track and manage effectively.

5.1.2 Change that generates new layers of risks

Often, change can generate new risks (or layers of risk) within the one situation or event. For example, in the procurement division (section 4.3.3 – "A simple example risk situation in an organization"), a procurement employee sees new risks emerging through a change in the process at the loading docks. For example, the change could be:

- A new way of moving raw material into the organization
- A change in the composition of the raw material brought into the loading docks (e.g. a more volatile component, or a new component that becomes volatile if it mixes, through an accident, with other raw material)
- The raw material is packaged differently, which could potentially create a blockage or bottle neck problems through an accident

Prior to any change in the procurement loading operations, let's say the organization perceived that a minor or moderate incident (e.g. a spillage of raw material, or breaking of packaging) might cause a minor or moderate injury to staff. After a minor change in some aspect of the procurement operation (as described above) new layers of risk emerge in the same potential situation or event. For example, there may now be significant revenue losses and cash flow implications, because a moderate accident, under the changed situation, could shut down the inbound goods process for several days, and or the nature or extent of the injuries could be very different.

After this minor change in the procurement operations, the organization faces new significant risks it is unaware of and therefore ill prepared for. As with the first category of change (discussed in the preceding section), this type of change is not limited to a few risks in one small area of an organization. New and emerging layers of risk manifest continuously throughout an organization. A periodic review of risks across the organization (e.g. a quarterly review), especially using any one of the current risk identification process, will probably not pick up these risks. More disturbingly, during the gaps in time between the reviews, the nature of exposure can change significantly, such that the organization is exposed to significant new risks. At times these new risks can become 'unexpected problems'. In other words the organization suffers from incidents that arise 'from nowhere', incidents that were once risks that the organization's risk monitoring process was unable to recognize.

5.2 The underestimated effect of change in an organization

When the level of change that is experienced throughout an organization is considered, and the effects this has on the risks faced, there is little that can be said in support of current risk management models. At their foundation they take the view, which I suspect unknowingly, that organizations are hard systems. Therefore, they believe that top-down models are appropriate ways to identify risks, and periodic reviews are all that is needed to deal with change in risk.

In today's world of increasing change, the risk profile of organizations is also experiencing increasing change. However, our current risk models are practices are unable to track this level of change. This can leave organizations with a significant cost burden. A cost burned that manifest through;

- Emerging unrecognized risks, that later manifest as 'unexpected' problems. Therefore, adding an unexpected cost to the organization.
- Inappropriate responses to known risks: The nature and size of the risk changes significantly, yet the response has not adjusted. Therefore the response is either overkill (too costly), or the organization is unknowingly over exposed.

Again, under current risk thinking and practices, the organization is on a potentially dangerous and misleading path.

Chapter 6

Assurance

6 Assurance through risk management: A poorly understood concept

In section 1.2.3 – "Greater scrutiny of the organization", I stated that organizations will need to deal with greater levels of scrutiny in today's world. Ultimately, the scrutiny is about building higher levels of trust in the statements and claims organizations make about their performance and their expectations.

Risk management's role in adding to the level of faith and trust that can be placed in an organization's claims has gained momentum in recent times. For example, standards in performance reporting require organizations to demonstrate that they have an adequate risk management process in place. This requirement is evident to some degree in the USA through Sarbanes-Oxley 404 (though it doesn't explicitly ask for organizations to have in place risk management systems) and 10K filings. More specific risk management requirements are evident in Europe and the UK, for example the Turnbull Guidance requirements for UK listed companies.

Understanding the threats and dangers an organization faces and how it deals with them would appear to be a logical extension of the reporting requirements for organizations. It would provide an important insight into the potential future performance of the organization. It will also provide higher levels of transparency into the organization and how it operated.

However, risk management's role as a process that improves the level of assurance in an organization's statements and claims has not undergone any critical examination. As discussed in chapter 3, risk measurements produced under current practices are incomplete and misleading. In chapter 4, I discussed how risk identification approaches have major limitations. In chapter 5 I discussed how approaches to understanding and tracking change in risk also have major limitations. Therefore, how can an organization easily demonstrate to stakeholders that the risks it reports are a reasonable reflection of the exposures it truly faces? The simple answer is it can't. This failure of current risk measurement approaches is a disturbing state of affairs for those that rely on risk management as a means of providing higher levels of assurance.

6.1 Testing the validity of hard data vs. risk measures (soft information)

An example of the failure of risk to work as a mechanism for providing higher levels of assurance can be shown through a comparison to the reporting of performance data. Testing the validity of a result that is based on 'hard data' such an event that has happened, can be a relatively easy process. For example, a cost figure for a division of an organization over the last quarter can be regarded as 'hard data'. This is because this is an event that has happened, and there will be a known process through which 'cost' is determined (such as personnel costs, equipment costs, etc.). Therefore, to test the validity of the stated cost figure, components that made up the figure, such as equipment cost, personnel cost, etc. can be checked and summed together over the last quarter. The result produced from this summing can then be compared to the originally quoted cost figure. If they match, the reported figure is valid; if not, then the originally reported figure is in question.

Conversely, a result based on soft information, such as a risk value, poses a much more difficult problem. There is currently no simple method to test the validity of a risk result. This is because there is no agreed frame of reference through which to conduct a test of validity. For example, a risk assessment result that states that there is a 'high risk' of a major competitor entering a market space could have been derived through any number of methods or approaches. It could have been a guesstimate by someone in a marketing department; or it could have been made through a statistical assessment of competitor behavior in different market conditions by a group of people from finance, or it could have been derived through any number of other approaches. There is no way of universally determining validity in this situation. One person may say that the result is valid, while another person may judge that the result is not valid, because the other person believes the approach used is not thorough enough.

6.2 Are your risk claims defensible?

In light of this failing in risk and risk management, executives and directors in major corporations must ask themselves a critical question:

- "Given that our organization has met regulatory requirements for risk management, if a major incident or disruption were to occur that may or may not be related to a reported risk, and if we were held up to scrutiny, do we have a sound basis to defend our decisions and actions?"

This question would be difficult to answer precisely without moving into the complexities and subtleties of the legal frameworks within different nations. However, in most cases executives will need to demonstrate that their decisions and actions were reasonable in relation to the nature of the information available prior to the incident or disruption. 'We met our regulatory or compliance requirements' is a statement that can often be a brittle defense.

The problems that arise from relying on a defense of having met regulatory or compliance requirements can be shown through the procurement example. In this example, a procurement employee perceived a risk at the loading docks (i.e. a potential accident causing significant delays, damage and or injury). Let's assume that the organization has in place a risk management process that is fully compliant with any current standard. Following on from my discussions about the flaws in risk management thinking and practice, there are five possible outcomes from the procurement employee's information about this risk situation. These are;

1. The organization's risks systems cannot identify the risk, or the risk is hidden or confused with other 'supply' risks.

2. The organization's risks systems capture the risk but due to the incomplete measuring approaches, the systems underestimate the size of the risk.

3. The organization's risks systems capture the risk and represent its size appropriately, but the situation changes over time, the risk becomes much bigger and the organization's systems do not pick up the change in information because a review is not due in that area for another month.

4. The organization's risks systems capture the risk but due to the incomplete measuring approaches, the systems overestimate the size of the risk.

5. The organization's risks systems capture the risk and the systems represent its size appropriately.

Now, let's assume that the potential incident occurs, in a manner and to the extent perceived by the procurement employee.

Out of the five possible outcomes, and assuming the organization has implemented a treatment for this risk commensurate to its reported size, then only outcome five provides a reasonably legal defense. Outcome four also provides a reasonable legal defense, however this is at an excessive cost to the organization. This is because the size of the risk was overestimated (through poor measurement) and the organization overspent on the treatment. In outcomes four and five the worst of the potential consequences from the incident have been avoided. The mitigation strategies did their job, and while some minor injuries and delays may have occurred, management has a strong case to support their decisions and actions.

Unfortunately, there are three other possible outcomes that the organization would have more likely faced, and none of these are positive for management. In each of these cases the organization would have faced a major incident – people could have been seriously injured and operations would have been disrupted for a prolonged period of time.

In these three cases, if management's decisions and actions were brought under scrutiny they would have a difficult job defending themselves. In each outcome there is damming evidence. At least one experienced employee had information that warned about this incident, yet the organization's systems

1. Did not provide the employee(s) with a capability to identify the information in a meaningful way, or

2. Misrepresented the information by significantly underestimated the threat, or

3. Did not react to new information.

In these cases, it is likely that management will be deemed responsible for the types of processes and systems it has put in place in its organization. It would have to explain why it did not act on information that was available in its organization, or why at least did it not provide the appropriate mechanisms to bring that information to the attention of the appropriate people.

For management to claim that it has met regulatory compliance as its only form of defense, in the face of a major incident that has caused serious injuries, or cost the company many millions of dollars will not wash with any aggrieved parties. "Do you rely on compliance as the sole means of understanding the challenges and threats facing the business you are put in change of", might be the thorny question asked.

Moreover, as we move forward into the 21st century, those that feel aggrieved by an organization's actions are not likely to become less litigious or less sophisticated about their claims against organizations.

6.3 The problem of agency risk

There are numerous examples across the world of organizations that were believed to have advanced risk management approaches yet experienced major failures or disruptions. A classic modern example is Enron corp. Enrorn were purported to have a high quality approach to risk management. They were regarded as innovative and lauded by many (McLean and Elkind, 2003). Their so-called advanced approaches and methods in risk did not help the senior executives defend their decisions and actions after Enron's spectacular collapse.

Interestingly, there have been a number of high profile corporate failures where the risk expertise of the organization was highly regarded. Sheedy, in her paper "applying an agency framework to operational risk management" (1999) regards many of these types of failures as a failure to deal with 'agency risk', rather than business or operating risks. Agency risk is the risk of employees or managers (agents), who are supposed to act on behalf of the company owners (e.g. shareholders), pursuing a personal interest that is in conflict with the company's interests. Examples of agency risk include Barings Bank, Long Term Capital Management, and the Procter & Gamble/Bankers Trust financial product contract.

While there have been many suggested improvements in how to deal with agency risk, particularly for financial institutions, there is a fundamental condition that is present in all organizations that can still generate significant agency risk. That condition is the natural behavior of human beings in groups and organizations. In an organization or society we can at times be political, tribal and emotive. Organizational processes and systems are often undermined when our personal interests give rise to extreme political, tribal or emotive behavior.

6.4 New risk thinking and practice is required to provide new levels of assurance

Given our human frailties and the significant flaws in risk thinking and practices, how can owners, executives and management achieve a high level of confidence in an organization's operations and future directions? For the agency risk problem, I believe the answer resides at the point at which risk information is born; that 'point' is the place where the individual and groups of individuals perform their duties for the organization. At these points people experience and perceive many layers and perspectives of risk first hand.

The individuals and groups within an organization are like thousands of 'intelligent receptors' of information. Humans have the unique capacity to apply levels of intelligence and perception far in advance of any data capture system. While some individuals may use their intelligence to collude to undermine the organization, they can rarely work in total isolation. At every point they face other individuals that, through their intelligence and perception can perceive the dangers. As long as these other individuals have the capacity to capture their concerns in a meaningful way, the agency risk can be identified. This is by far the best defense against agency risk, as it doesn't rely on a fixed, unconscious process as a means of trapping agency risk.

For the general problem of defensibility, again the answer lies with empowering individuals and groups throughout the organization to capture risk information in meaningful ways. Risk situations constantly emerge throughout an organization. Individuals and groups are the ones most capable of recognizing and recording them. However, enabling personnel at all levels to capture risk information in meaningful ways is hampered by the fundamental problems in measuring risk, identifying risk and tracking complex change in risk.

If these fundamental problems are solved, building significantly higher levels of trust in organizations can be achieved through what would ultimately be a new way of understanding and dealing with risk.

Chapter 7

Conclusion

7 Conculsion

As I have discussed in the preceding sections, the concept of risk and risk management practices are designed for hard systems. In section 4.3.1 – “An organization is a soft system”, I stated that a hard system has a relatively high level of stability and predictability. It may undergo change, but the change will tend to occur through known patterns or cycles. By contrast, soft systems have many complex layers and interactions. They will undergo complex changes that are often unpredictable. This is the world of a modern organization. A risk management approach based on hard system thinking will therefore have significant limitations when applied within an organization.

Specifically, this major miss-match in systems thinking has led to significant problems in the way risks are measured, identified and how changes in risk are tracked over time. Ultimately, these problems can affect decision-making, leading to substantial costs impacts through misleading impression about the risks faced by an organization.

7.1 Risk Management: A 1960's model of management

If we examine the approaches used in risk management from a broader management perspective, we find that it has close ties to some traditional management philosophies. Specifically, risk management practices are closely aligned to what Mintzberg refers to as 'planning school' strategic management (Mintzberg et al, 1998). Planning school approaches to management are characterized by:

- Rigid decomposition of goals and objectives to detail levels across an organization
- Extensive planning and control systems
- Reliance on 'hard' data, and the exclusion of the often more important 'soft' information

Mintzberg noted the main problems facing the planning school's approach to managing strategy in an organization is its inability to deal with soft data, change, innovation, emerging strategies and its fixation with performance against plan, such that it becomes more important than performance of the organization.

Ultimately, its biggest failing is that it created a misleading illusion of certainty and predictability about the world, or as Mintzberg aptly states "As human beings, we often believe that we have captured a process by simply breaking it into its component parts and specified procedures for each. Yet all too often, that just breeds a certain mindlessness" (Mintzberg et al, 1998).

Conclusion

Though still in use today, planning school approaches are not as prevalent or accepted as they once were in the 1960's – a time when organizations operated in a world with greater stability and predictability.

Aspects of planning school thinking that underpin current risk management practices are evident through:

- Current approaches to identifying risks (e.g. top-down, cause-effect or category approaches),
- The reliance on mathematical and numeric expressions of risk and an inability to handle soft information
- A strong focus on 'compliance' as a method of dealing with risk. Compliance can only work effectively where a given environment is stable, well understood and virtually the same across many different organizations. This is rare situation in organizational environments.

Planning school thinking is most evident in risk management through the way the risk management process is applied in most organizations. Typically, the risk management process is used during the planning stages of a project, operation, initiative, etc. True to planning school thinking, risk management in these situations resides in the hands of a few who dictate the identification approach, conduct the assessment and define the values. There is less emphasis on risks management through the execution stage (other than simple forms of 'monitoring'). Significantly, the coal-face of the organization, the hundreds or thousands of personnel that will execute the plan, operation or initiative have little direct input into the risk management process, especially during the execution process.

In the Sparc example in section 4.5.2 – "The misunderstood concept of major or strategic risks", we saw how the automobile manufacturer was faced with a difficult decision on whether to proceed with a major new initiative. As discussed, a planning stage risk assessment process would likely have given Sparc a cursory understanding of the risks they faced. Success or failure of the SUV strategy would not be clearly evident at the starting line. The complexities, permutations and combinations are too great. Deriving a simple value or set of values that somehow would show if the risks are above or below a threshold (e.g. 'risk appetite'), which could then feed into a 'go-no-go' decision for the SUV strategy is fantasy.

In reality there are very few simple go-no-go decisions for major undertakings. Perhaps if a shoe manufacturer suddenly wanted to move into aircraft manufacturing, a simple assessment of the risks might allow management to confidently arrive at a decision on whether to proceed with this venture or not. Often, organizations are faced with situations similar to what Sparc faces – where the undertaking is complex, the opportunity is big, the risks are plentiful and the future is uncertain. Indeed, this is an organization's reason for its existence, it regularly needs to undertake risky new initiatives or projects which are designed in some way to benefit the business.

It is important to point out that I am not belittling planning in general. Planning is a critical first step for any major undertaking; and the better the planning the better that first step will be, but it is the first step, in a sequence of many many steps. The critical subsequent steps will in large part determine how well Sparc succeeds or fails in its new initiative, in other words, how well Sparc executes its initiative.

7.2 Building resilience to change and uncertainty

To achieve the best possible result in a complex and rapidly changing world, Sparc will need to develop high levels of awareness and responsiveness to change. It will need to anticipate, adapt and adjust effectively to emerging situations and events across all aspects of its operations.

Adapting and adjusting a complex initiative such as the rollout of a major new product line is not achieved solely through quarterly or half-yearly decisions by senior management. As discussed in section 4.5.2 – "The misunderstood concept of major or strategic risks", Sparc faces many thousands of risks that either individually or through a sequence of risks could have a significant impact on its success or failure. Sparc cannot know or anticipate most of these risks at the planning stages of the initiative. To execute its initiative effectively Sparc will need to arm its personnel throughout the organization (its coal-face) with a new thinking and approach to

- Identifying risks, threats or issues
- Measuring and interpreting the size of a risk
- Tracking complex changes in the 'terrain' of risks faced

Armed with a new approach to understanding and dealing with risk, decision-making at all levels of the organization would be performed with new forms of information. Emerging risks and threats to the business would be dealt with more rapidly and effectively, while the size and flow of 'unexpected problems' would reduce. There would be a greater connectedness across the organization. Sharing of knowledge and learning about what is emerging and how to deal with it will improve dramatically. Confidence and trust in Sparc management's ability understand the challenges it faces would be strengthened through Sparc's ability to easily demonstrate its understanding of its 'forward view'.

The value of developing a capability to anticipate and adjust in a highly dynamic world has gained momentum in recent times. Hamel (2003) refers to this capability as 'strategic resilience', which he describes as an organization's "capacity to adjust its strategies as it works towards a long-term mission". To be able to perform this function effectively an organization requires new ways of understanding what lies ahead on its paths towards its goals and objectives.

7.3 Moving forward with greater clarity and vision

Currently around the world organizations are using and implementing the traditional hard system based risk management practices. Yet in many cases I suspect that they are a little uneasy about the supposed value these approaches purport to bring, but are perhaps unable to clearly articulate where the limitations lie and what they mean to their organizations.

I believe a significant layer of value awaits those organizations that can break through the shackles of traditional thinking and embrace a fundamentally new way of understanding and dealing with risk. This new breakthrough may no longer be appropriately labeled 'risk management', because the way it would be used and operate through an organization would be vastly different to current risk management practices. Armed with this new 'forward viewing' capability, an organization can face the uncertainty and risk of today's world with greater confidence in its ability to generate value.

This new forward viewing (forward management) capability needs to be added to every facet of an organization's operations. It needs to be a skill that is devolved into the coal-face. It will not be a compliance driven (box ticking) exercise. It will not be a purely mathematical or statistical approach driven by an esoteric risk management department. It will not be a fixed set of measurements or 'key performance indicators'. The measures of this new approach will need to be flexible and 'organic'; they will emerge and evolve along with the organization and the changes it experiences.

Whatever a new approach to risk in organizations may be called, one thing is clear — current risk management thinking and practices are in need of urgent and funda-

Appendix A: References

Onsman, H. 2003. “The art of managing uncertainty” Sydney NSW. McGraw-Hill.

Mintzberg, H. 2004. “Managers, not MBA's : a hard look at the soft practice of managing and management development” . San Francisco, CA : Berrett-Koehler

Micklethwait, J. and Wooldridge, A.. 2003. “The company : a short history of a revolutionary idea”. New York : Modern Library

www.globalreporting.org

The institute of Chartered Accountants in England and Wales. 1999: “Implementing Turnbull. A boardroom briefing” The Centre for Business Performance.

Standards Association of Australia. 1999. “AS/NZS 4360:1999. Risk Management” Strathfield NSW. Standards Association of Australia.

Federation of European risk management associations: 2002 “A risk management standard” www.ferma-ossa.org

The Committee of Sponsoring Organizations of the Treadway Commission: 2004 “Enterprise Risk Management Framework” The Committee of Sponsoring Organizations of the Treadway Commission.

The Shorter Oxford Dictionary: 1993 Edited by Lesley Brown. Oxford. Clarendon Press.

Crouchy, M. and Dan, G. and Mark, R. 2001: “Risk Management” New York. McGraw-Hill

Rosa, E. 2003: “ The logical structure of the social amplification of the risk framework: Metatheorectical foundations and policy implications” pp47-89. “The social amplification of risk” Editors Pidgeon, N. Kasperson, R. Slovic, P. Cambridge University Press.

References

Checkland, P. 1981: “Systems thinking, systems practice” Chichester. John Wiley & Sons.

Slovic, P. 2000: “The perception of risk”. London. Earthscan Publications Ltd.

De Finetti, B. 1937: “Foresight: Its logical laws, its subjective sources”. Editors Kyburg H. and Smokler, E. “Studies in subjective probability”, Wiley 1964

Stulz, R. 2001: “Why risk management is not rocker science”. pp294-300. “Mastering Risk Volume1” Editor Pickford, J. Person Education Limited.

Rasmussen N. et al. Reactor Safety Study: An assessment of accident risks in US commercial nuclear power plants. U.S. Nuclear Regulatory Commission, WASH-1400, NUREG-75/014, 1975

Ritchie, B. and Marshall, D.:1993 “Business risk management”. London : Chapman & Hall.

Felter, S. and Dourson, M. 1998 “The inexact science of risk assessment (and implications for risk management” . Human and Ecological risk assessment: Vol4, No.2, pp245-251

Conrow, E. 2000: “Effective risk management” Virginia. American Institute of Aeronautics and Astronautics Inc.

Kahenman, D. Slovic, P. Tversky A. (Editors) 1982: “Judgement under uncertainty: Heuristics and biases” . Cambridge. Cambridge University Press

Jaeger, C. Renn, O. Rosa, E. Webler, T. 2001 “Risk, uncertainty, and rational action” London. Earthscan Publications Ltd.

Schrage, M “Daniel Kahnemann: The thought leader interview”. Pp121-126. “Strategy+Business” Issue 33 Winter 2003. Booz Allen Hamilton.

Bowden, A. and Lane, and M. Martin, J: 2001 “Triple bottom line risk management” New York. John Wiley and Sons Inc.

Bier, V. “An overview of probabilistic risk analysis for complex engineering systems”. pp67-83. “Fundamentals of risk analysis and risk management” 1997 editor Vlasta, M. Ohio. Lewis Publishers.

Peccia, T. “Design an operational risk framework from the bottom-up perspective” pp200-218. Mastering Risk: Volume 2: Applications” Editor Alexander, C. Person Education Limited.

Starr, R and Newfrock, J. Delurey, M. “Enterprise Resilience: Managing risk in a networked economy” pp70-79 “Strategy+Business” Issue 30. Booz Allen Hamilton.

Mintzberg, H. and Ahlstrand, B. Lampel, J. 1998: “Strategy Safari” New York. Free Press.

Hamel, G. and Valikangas, L. “The quest for resilience” pp52-63 Harvard Business Review. September 2003. Harvard Business Review

Mclean, B. Elkind, P. 2003 “The smartest guys in the room”. Camberwell, Penguin Books

Sheedy, E. 1999 “Applying an agency framework to operational risk management”. Applied Finance Centre, Macquarie University. No. 22

Metatheme

Thought Leadership. Practical Solutions.

Metatheme USA

410 Highpoint Forest Drive
Covington, GA 30016
USA

Ph. +1 678 333 5718
usa@metatheme.com

Metatheme Australia

PO Box 7175
St Kilda Rd Central
Melbourne, VIC 3004
AUSTRALIA

Ph +61 (0) 417 323 584
australia@metatheme.com