A Systems approach to Enterprise Risk Management in High-tech Industry

by

Atul Sharma

B.E. Computer Science & Engineering (1995)
Panjab University, India

M.S. Computer Science (1998)
University of New Brunswick, Canada

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

February 2005

Signature of Author _____

Atul Sharma
System Design and Management Program
February 2005

Certified by _____

Paul Carlile
Thesis Supervisor
Associate Professor of Information Systems and Organization Studies

This page is intentionally left blank

ABSTRACT

The high-tech industry is showing increased interest in developing an enterprise wide approach to risk management. There are three reasons for this increased interest; first as the industry has matured, as evidenced by slower growth, increasing consolidation and global competition, managing "costs" has moved to center stage; second, technology product life cycles have progressively shrunk leading to increased technology strategy risk; and third larger events such as 9/11 and corporate scandals have created an awareness of new risks to be managed. In these changed circumstances, the old days of rapid growth and localized & reactive risk management techniques need to be replaced with a capacity to understand risks and manage them effectively across the entire enterprise.

Although, risk management has been practiced in the high-tech industry for some time the approaches are based on silo techniques such as insurance, finance, strategy or operations. The challenge is that these varied approaches fall short of holistic risk management and further maintain risk silos that generate additional risks to the organization. To address these silos and develop an enterprise risk management approach we have devised a *"generic"* and *"scalable"* risk management framework that could be used by a firm irrespective of its current risk management maturity to achieve a higher level of risk management sophistication.

Our approach is based on a three step process; identifying the risks in each of the organizational silos, analyzing their gaps and thereafter developing common risk language and measurement capability across the whole enterprise to close these gaps. To accomplish these three steps a firm can use a 3-T knowledge management assessment framework and a 4-R risk management process methodology. We have also devised a risk management maturity model that helps a firm assess its current risk management sophistication, determine the level of maturity the firm would like to target and so clarify the next steps to get there. We combine these frameworks and methodologies together to create what we call Integrative Corporate Risk Management (ICRM) architecture to help high-tech firms develop a state of the art enterprise risk management capability.

ACKNOWLEDGEMENTS

First and foremost, I sincerely thank Prof. Paul Carlile – my thesis advisor, for his constant support, guidance and involvement. I had come to MIT to learn management skills that would help me succeed in the world of business & technology. Little did I know that my first class, an organizational behavior class by Prof. Carlile would help me realize that business is not about managing business, finance or technology; it's about *"people"*.

As I walk out of MIT- understanding people and channeling their motivations & dreams towards a corporate and social vision is a goal I will relentlessly pursue. Thanks Prof. Carlile for giving me this insight. I also appreciate Prof. Carlile's immense patience during the thesis process. Not only did he spend considerable time helping me understand key points, but he didn't mind revisiting the hypotheses whenever I had doubts.

I got the motivation to work on enterprise risk management while doing my summer 2004 internship at Cisco Systems. I was fortunate enough to work on an enterprise risk management project at Cisco that was sponsored by the CIO and CFO's office. The goal of the project was to propose an enterprise risk management pilot to two members of Cisco's top corporate leadership; Randy Pond (Sr. VP –Operations, Processes, IT & direct report to CEO) and David Holland (VP – Finance & direct report to CFO). Thanks Randy and David, for giving me the chance.

Although my Cisco experience gave me a chance to interact with a lot of great people but two personalities stand out in terms of their impact; Chris Kite, my Sr. Director and Ray Gale, my manager. *"Chris can give John Chambers a run for his money"* – I heard this statement a few times at Cisco; and I guess the statement says it all. I sincerely thank her for

giving me a chance to work closely with her and learn a lot. I wish, like her, I could combine solid leadership, perfect articulation, speed of thinking and alliance building in one person!

Ray was my hiring manager and he motivated me to do thesis work that would address enterprise risk management problem for the high-tech industry. I was amazed by his sound judgment about solutions that would work, and that won't. His discipline, clear thinking and a focus towards bigger picture; while being perfectly rational was a result of his rich experience. While interacting with him, I realized that you learn certain things only through experience. I am glad that through numerous discussions, I had a chance to learn from him about various aspects of business and life. Also, my special thanks to Carol Ann McDevitt, a very energetic and smart MIT SDM'02 alum who was instrumental in arranging my internship. I also offer my sincere thanks to Martha Doherty and numerous Cisco Directors and VP's for their risk management insight that helped me refine my learning.

I especially thank my wife for her constant encouragement and support during the MIT experience. During the harrowing process of making a "final" decision out of my B-school options, I would bug her everyday with pros and cons about various schools. Finally, she was fed up with my discussions and said – "*just go to MIT. Period*" I am glad I listened to her, because there is no other place like MIT.

I also thank my parents, sister, mother-in-law, father-in-law and brother-in-law for their constant encouragement. Finally, thanks to all my friends and staff at SDM for their help & cooperation.

DISCLAIMER

Risk management being a sensitive topic, this work does not attempt to go into the risk details of Cisco Systems and it does not use any Cisco specific information. Nevertheless, this work does use the learning that I did at Cisco Systems and thereafter to achieve a bigger goal – The goal of helping the high-tech industry achieve superior risk management.

Readers are advised not to draw any company specific risk management information from this work, and indeed encouraged to use this work as a framework & roadmap to tackle risk management within their firms.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Background

Enterprise Risk management in the high-tech world is a recent phenomenon compared to other industries like financial services and energy. Although most high-tech firms[1] have some risk management in place, but most of these practices, at best, are silos based with little or no process integration across the firm. This bottoms-up approach with a focus on immediate business hazards and their mitigation misses the bigger risk management picture; and missing this holistic approach leads to a non-alignment of risk-reward relationship, with respect to corporate business strategy. As a result – firms tend to under-estimate or over-estimate the amount of risk they can handle and do not know how to manage the amount of risk they can safely handle, while maintaining an optimal risk-reward relationship.

Historically, this risk management approach in firms has been attributed to a business unit culture. In a business unit culture, most business units emerge as a result of acquisitions, whereby the business unit is given enough independence to maintain its rapid pre-acquisition growth rate. Until year 2000, most of these businesses units at major firms were enjoying rapid growth and had little risk management culture because of their start-up DNA. Also, in absence of a corporate level risk management mandate and strategy, most business units devised their own minimal risk mitigation plans. As a result, in the post 9/11 world, when firms started focusing on corporate level process integration exercises, and stronger risk management practices, they did not know how to combine these silos based practices that worked for decades.

Add to this the confusion around operational risk management in the industry. Operational risk management in its broadest sense is the risk around the operational activities of

[1] Hereafter, the large high-tech firms will be called "firms" for sake of consistency

a firm. A combination of operational, strategic and financial risk management at the firm level is called enterprise risk management. Although financial and strategic risk management have a long history but, operational risk management is a relatively new field and firms have little knowledge about it. This varying state of sophistication amongst risk management functions i.e., strategic, financial and operational makes it complex for the firms to address the risk management issue, holistically at the enterprise level. This complexity is further compounded by the fact that all risks can not be viewed in the same fashion and can not be mitigated in the same way; for example – analyzing supply chain risk is very different than analyzing emerging technologies investment risk. The current risk management approaches in the industry are based on the strategic consulting, insurance, financial or informational risk management models; and these models are inadequate to handle the complex field of enterprise risk management. This inadequacy in handling risk management could be removed by having risk management processes that integrate all the business functions of a firm. The biggest gap in the above approaches is a lack sophisticated risk management approach to handle operational risk management and its integration with strategic, financial and informational risk management.

As a result, firms find themselves at a loss when it comes to implementing risk management at the enterprise level i.e., *enterprise risk management* (ERM). These firms do not know how to use risk management to tie together the risks faced by their myriad business functions and put an enterprise risk management solution in place. They fail to realize that true ERM could only be achieved by a seamless integration of strategic, financial, informational and operational risk management.

Also, the variance in the risk management sophistication of the business functions of the firm requires disparate risk management frameworks for each function; hence leading to a

"silos" based risk management practice. In fact, these silos could vary in their maturity, complexity and life-cycle, leading to a rigid organization culture. The "silos" based risk management practice is the lowest level of risk management on the enterprise level, while a "fully integrated" risk management is the highest level of risk management that firms can achieve.

The goal of a firm should be to move from a silos based risk management practice to a fully integrated risk management practice. This journey from "silos" to "full integration" can be viewed as the movement of a firm on a risk management sophistication curve. The risk management sophistication curve is maturity curve that helps a firm identify its risk management maturity. The "silos" based risk management practice is at the bottom of this curve, while a "fully integrated" risk management practice is at the top of the curve. Chapter two explains the risk management curve in details. In summary, the goal of this work is to help firms move up this risk management curve using a generic framework.

1.2 Objective

The objective of this work is to devise a *"generic"* and *"scalable"* risk management framework, using a holistic approach that could be used by any high-tech firm, irrespective of its risk management sophistication to achieve a higher level of risk management sophistication.

1.3 Approach

After discussing our objective for this work, it is imperative to discuss the approach that we undertook to achieve our goal. We have followed a customer focused approach to solve the risk management problem that could be readily implemented in the real world irrespective of the risk management sophistication of the firm in question. Risk management in the high-tech industry is

an evolving field and without a discipline approach it's fairly easy to end up tackling a lot of issues in different directions at the same time. To keep a disciplined focus around our goal, we divided our customer focused approach into following phases:

- **Problem Analysis Phase**: The risk management problem in the high-tech world is not a defined and scope-bounded problem. Different firms have different risk management sophistication levels and therefore infer different meanings from the term ERM. A firm that has a mature and sophisticated risk management practice would define ERM as a risk management practice that's integrated across the firm combining major business functions, through uniform firm wide processes. On contrary, a firm that has a rudimentary risk management practice in place would assume ERM synonymous to having hazard mitigation practices across all its business functions, without these practices being integrated across the firm through uniform risk processes. Therefore, in the problem analysis phase we focused on *"firm analysis"* to find out how firms relate their current risk management maturity levels to their perceived notion of most sophisticated risk management level.

  Thereafter we focused on *"goal analysis"* to find out if all firms had similar risk management goals or if these goals differed based on the firm's strategy, business model and risk appetite. Using the firm analysis and goal analysis, we were able to devise a generic and scalable risk management maturity model that helped us categorize the risk management sophistication of a firm on a risk management maturity curve. A brief introduction about this maturity curve is given in Chapter 2, while Chapter 4 has the exhaustive treatment. We accomplished the problem analysis part through surveys, interviews and interactions with managers from the high-tech world.

- **Data Collection Phase:** The author during his summer stint along with a Cisco Systems' team extensively interviewed more than twenty-five senior-management leaders about risk management. This stint helped the author collect a lot of primary data about risk management in communications industry. The author has refrained from using any Cisco specific data for this work, but has used invaluable lessons that were learnt during this experience. These lessons are not specific to the communications industry and are applicable in a broad sense to the whole high-tech industry.

  Subsequently, the author interviewed leaders from other industries as well viz., financial services, healthcare etc., to add to the richness of data. Apart from this basic data collection, the author did extensive literature survey and brainstormed with academics and industry experts to get a holistic view of risk management practice within high-tech industry.

- **Solution Analysis Phase**: In the solution analysis phase, we analyzed the current risk management approaches prevalent in the industry and did *"gap analysis"* to find out their shortcomings. These approaches are covered in section 2.3 of Chapter 2. Once the gaps were identified, we focused on filling these gaps. As an example we discovered that firms used similar risk analysis methods to analyze unrelated risks. For example, they would use a "estimated loss and its likelihood" approach to analyze the supply chain as well as IT risk; which according to us should be treated very differently. Therefore, we spent considerable energy to devise business specific risk analysis methods. Therefore, in a nutshell in the solutions analysis phase, we did a gap analysis of prevalent risk management methodologies and came up with solutions for the missing pieces.

- **Framework Construction & Application Phase:** After the solution analysis phase, we spent considerable energy in finding a generic framework that could yield a uniform risk management solution in any situation irrespective of the risk management maturity of a firm. Majority of our conceptual work is around this framework and is introduced in Chapter 4. The conceptual work is followed by analytical analysis through the use of a case study in Chapter 5. In this chapter we apply our framework to a typical high-tech firm and find out the risks faced by the firm, subsequently we do the risk analysis of a few of these risks and follow up with risk mitigation and risk monitoring stages.

1.4 Structure of Thesis

The structure of the thesis is as explained below.

- **Chapter 2 "Background"** discusses the historical evolution of risk along with risk management in the high-tech world and the current risk management approaches.
- **Chapter 3 "Literature Review"** discusses literature related to organizational change and Paul Carlile's 3-Lenses and 3-T framework. Also, the chapter discusses the value at risk methodology apart from common integrative risk management techniques.
- **Chapter 4 "Risk Management Frameworks"** discusses the frameworks and methodologies that we have proposed. The chapter starts with the introduction of risk maturity model and goes into the details of various business specific risk analysis frameworks, before introducing the firm level – ICRM (Integrative Corporate Risk Management) framework.
- **Chapter 5 "Case Study"** applies the frameworks introduced in Chapter 4 to a typical high-tech firm. A detailed risk identification and risk analysis exercise is carried out to explain the usage of the frameworks introduced in the earlier chapter.

- **Chapter 6 "Methods & Approach"** discusses our problem analysis and solution analysis approach in details. The chapter starts with a discussion about firm and goal analysis and discusses gap analysis as a part of the solutions approach.
- **Chapter 7 "Results, Discussion & Conclusion"** lists out the results, goes into the relevant discussion and concludes our understanding based on the work.
- **Chapter 8 "Recommendations & Future Work"** details our recommendations and the future work that could be carried over, based on our work.

1.5 Chapter Summary

The chapter laid the foundation for our work and discussed the background, objective and approach related to our work. It also discussed the "silos" based risk management problem and the varying risk management maturity levels of various firms. We discussed that silos based risk management is the most basic level of risk management, while "fully integrated" model of risk management is the most advanced level, and firms need to move from this basic level of risk management to the advanced level. Subsequently, we outlined our objective of finding a generic framework, based on knowledge and risk management to help firms achieve advanced levels of risk management. Finally, the chapter concluded with a short summary of the chapters ahead.

2 BACKGROUND

2.1 Evolution of Historical view of risk

"In the face of every risk lies a hidden opportunity"

-Ancient Indian & Chinese saying

Risk has been an integral part of human life since ancient times. Ancient Greeks recognized risk and uncertainty in their day to day lives but the analytical understanding of risk was fairly limited because roman numerals were not conducive to computation. It was believed, and in fact it is still believed by a lot of people that events and fate is controlled by god. In ancient Greece, Zeus, Poseidon and Hades rolled dice for the universe. Therefore, there was risk recognition from 1200-300 B.C, but there were no means of measuring it. (Bernstein, 1992)

From 1000-1200 B.C., the Hindu-Arabic base 10 numeric system came into existence. This formed the foundation for pushing mathematics from a counting method to a tool for quantifying scientific and abstract thought. During the renaissance period (1400 A.D – 1650 A.D), Italian and French mathematicians like Pascal and Fermat studied mathematical puzzles and games of chance. This was the period when theory of probability came into existence, first attempt to predict the future were made and interestingly first primitive "insurance policies" were sold!

The 1650 A.D to 1800 A.D period witnessed application of probability to social sciences, development of mortality tables and expansion of insurance opportunities. Great Britain in fact

used "annuity" contracts for the first time to finance its global domination efforts and Lloyds of London was willing to underwrite almost any type of risk.

In the 1900's came into existence the path breaking theories like Markowitz's "Modern Portfolio Theory" and Black-Scholes "Option Pricing Theory". The portfolio theory espoused the value of diversification and revolutionized the Wall Street and the general practice of corporate finance through Capital Asset Pricing Model (CAPM) and other risk pricing models. Similarly, the option pricing theory came up with a mathematically elegant approach to valuing "side bets" or derivatives. This theory helped in formalizing models for hedging exposures against market exposures and helped development of various applications for business decision analysis.

In the 21st century, and that too in the post 9/11 world, businesses are facing increased complexity in terms of globalization, competition, regulations, new innovations & technology life cycles. Businesses are now exposed to new types of risks and traditional insurance markets do not provide solutions to cover these new risk paradigms. Therefore, businesses are adopting a comprehensive risk management approach. The goal is adopting this comprehensive enterprise level approach is to find the optimal balance of risk-reward relationship with respect to financial, operational and technological issues.

At present a few industries like financial services, energy (in particular oil exploration within energy) etc., have developed advanced risk management practices while the high-tech industry, on the whole hasn't achieved much sophistication in the area of risk management. On a cursory analysis, this lack of sophistication could be attributed to relative lack of industry maturity within high-tech, but there are various reasons for this lack of sophistication. In the

following paragraphs we cover the current state of risk management in the high-tech industry; the reasons for the lack of risk management sophistication. We also cover the prevalent risk management solution approaches, the gaps in these approaches and finally – we discuss the characteristics of our solution.

2.2 Risk Management in High-Tech World: Past and Present

Risk management in the high-tech world is a fairly recent phenomenon. It's a fairly safe assumption that the high-tech industry lags behind the financial services and energy industry in terms of risk management sophistication. There are various reasons about this situation and a few are listed below.

- **Diminished Need**: The majority of current high-tech titans achieved their scope and size in last two and a half decades. During this time period, they enjoyed a double digit growth, most of which came from US domestic business growth in a relatively safe environment. With relatively few perceived risks to their business continuity, there was no urgent need to focus on risk management. In fact a few companies like DEC, in the early technological era focused so much on growth that they ignored and masked risk management to their peril.
- **Cost Center Outlook:** Risk management is considered a cost center by most firms. Therefore, firms tend to neglect it until they are hit by a catastrophe. Prior to 9/11, except for strategic and governance threats, firms did not perceive any other kinds of threats.
- **Start up Roots**: Most current high-tech titans have start-up roots. Although they all took huge bets on their product lines from time to time, their business nature was inherently less risky than financial and energy industries. An oil exploration company will need to bet billions of dollars to do deep sea oil exploration, in the face huge uncertainties.

Similarly, global trading, foreign exchange and sovereign risks would mean lot of risk for financial companies as well. Therefore, these two industries had incentives to focus on risk management and become sophisticated risk managers. Contrast that to high-tech industry, that was doing 90% of its business within the safe environments of US and whose titans grew up from a start up background. It will be wrong to say that the high-tech firms didn't play huge monetary bets, but compared to business environment of energy sector and large financial trading institutions, their risks pale in significance.

Therefore, in a nutshell, the high-tech world didn't have much incentive to focus on risk management in the past few decades. Nevertheless, in the past few years the high-tech industry is becoming increasingly sensitive to risk management. This change has been driven by many industry specific and external factors; and a few of these factors are listed below.

- **External Threats**: Post 9/11, companies feel vulnerable to external threats and therefore have started focusing their attention to external threats related risk mitigation.
- **Globalization:** Although globalization has been a potent force for many decades, the high-tech industry is becoming "truly global" only recently. With a US IT spending growth prediction of 4-8% for rest of the decade, aggressive growth in foreign markets is top agenda for most high-tech companies. Similarly, the increasing reliance on Asia as the major supply-chain partner with respect to procurement, manufacturing and distribution is making most high-tech companies feel nervous about possible supply-chain disruptions because of various risks. With an increased exposure to global markets and supply-chain, high-tech firms have awakened to a need for increased risk management.

- **Technology Strategy**: With most infrastructural standards in place, high-tech firms have to take bigger financial bets when taking major strategic technical bets. Ten years back major US wireless service providers would only deploy CDMA and TDMA networks, but because of a multitude of reasons, a few of them are changing to GSM. This means enormous financial bets, akin to deep sea exploration in increased uncertain situation of non-prevalence of one particular standard. Therefore, increased complexity and uncertainly related to technology strategy has forced high-tech firms to hedge their bets and think in terms of risk management.
- **Product Life Cycle Span**: In last 10 years the life cycle of most technical products has come down by almost 50%. This life cycle time decrease has put time demands on manufacturing, marketing and distribution of technology products. As an example – in view of Moore's law, the whole cycle of chip design, manufacturing, supply etc., has come down to a 9-12 month cycle, which poses increasing risks to technology business.
- **Obsolescence** – The obsolescence rate in the high-tech industry is growing fast thereby causing increased business risks to firms. As an example – the exponential increase in the density of transistors per chip forces Intel to invest billions of dollars in new fabrication machines, while the old machines become obsolete. Interestingly, the rise in the cost of these fabrication machines is exponential, while the marginal utility of increased transistor density decreases. This poses huge financial risks to companies like Intel and AMD, who have to place huge financial bets based on their strategic direction. This has caused the advancement of fields like real options that help achieve risk management by hedging options.

In summary, the high-tech industry had a diminished need for risk management until a few years back because it wasn't a source of competitive advantage. Nevertheless, in last 5-6 years, it has become a source of competitive advantage because in the age of diminishing margins and high volume, a small business disruption can adversely affect the competitive advantage of an industry leader. Although the high-tech industry has started focusing on risk management from past 5-6 years, but there remain substantial challenges in a holistic implementation of ERM. These challenges arise because of the gaps in the current risk management approaches, and we cover these risk management approaches and challenges in the next section.

2.3 Current Risk Management approaches and their gaps

No two firms face the same kind of risks therefore there using a standard risk solution would not help every firm. Different experts push specific risk management views, thereby making it harder for the firms to decide the right path in an evolving field. At the risk of generalization, there are four schools of thought on risk management, which are as follows, in terms of increasing scope of their outlook.

- **The Insurance Approach**: According to the insurance approach, risk management is about insuring all possible kinds of risks. In fact a few insurance firms also have dedicated consulting arms that help clients identify various insuring possibilities. According to this school of thought, holistic risk management is about identifying and thereafter insuring the risk against its assigned capital loss value.
- **The Financial Approach**: According to this approach, risk management is about managing capital & finance related risks using sound portfolio management techniques.

According to this school of thought, if there is a derivative instrument available to hedge a capital flow related risk – the risk could be categorized as mitigated.

- **The Strategic Approach**: The strategic approach looks at the risk-reward relationship at the CXO level. Nevertheless, tying strategy and execution together is a challenge and in the case of risk management, the challenge is in execution. The risk-reward relationship is well understood by the top management, but risk management is all about execution and that's where the firms find themselves at a loss. According to this school of thought, if the risk has been identified at the strategic level and the top management is aware about it, they would know how to mitigate it.
- **The Information Systems Approach**: According to this approach, risk is all about "not having the right information at the right place at the right time". If there is an ERP solution in place, that collects data from various sources and creates certain alerts based on the change in this data – the risk could be known by the firm and subsequently mitigated.

Each of the four approaches described above have a specific focus and a limited scope. On benchmarking these four approaches to ERM, we notice that these approaches have substantial "gaps". Some of these gaps are discussed below, with the help of examples.

A wireless service provider can not insure the risk of Chinese government's decision of going ahead with their own wireless standard. The financial risk management approach can not manage the risks with technology innovation, since the product, market and technology adoption related to the innovation might not be mature enough to use financial risk management instruments. Similarly, the strategic approach is great to understand the risk-reward relationship

at the corporate level, but it can not help manage the risk of an international supply chain, in absence of a quantitative and analytical approach. Finally, managing risk through information management is of not much use if the information system fails to capture the novelty of the market, firm and the economy. It's clear from the above discussion that each of the approach focuses on a particular aspect of risk mitigation, but they are far removed from ERM; and in fact, even their combination fails at realizing ERM, because of a lack of focus on operational risk management by any of these approaches. The following paragraphs discuss some more limitations of these approaches.

Out of the above four categories, the strategists have made good advances studying the relationship between risk, reward and corporate strategy at the top level; but the conversion of risk strategy into execution remains an issue for most high tech firms. According to Larry Bossidy, the CEO of Allied Signal – "Execution is everything!", and it's the execution phase where firms face challenges because of organizational, culture and language issues. Even on a strategic level there is little insight available on strategic risk management compared to relationship between corporate strategy and risk; a subject that's been thoroughly explored by strategic thinkers.

Another shortcoming in one of the above four approaches is the issue of *conflict of interest.* A few consulting companies consult on risk with an "insurance" focus because they are owned by parents, who have insurance business. As a result these consulting companies focus only on the risks that could be quantified, tied to an immediate capital loss and thereafter insured. This focus is largely a side-effect of their main job; lining up insurance business for parent companies. Nevertheless, this narrow focus isn't in the best interest of technology firms who need to look at qualitative as well as quantitative risks to get a broader risk management picture.

In summary, it's noteworthy, that each of the above four approaches do tackle an important piece of the ERM puzzle, but, individually or even their combination fails to take a holistic view of ERM. In fact, even if the above four "view points" are combined, there remain substantial gaps in the holistic treatment of risk management as discussed in the above paragraphs. In view of these gaps firms need to know where they stand with respect to risk management and how to become sophisticated risk management user. The following section addresses this issue.

2.4 Firms and Risk Management Maturity Curve

In section 2.3 we discussed the prevalent risk management approaches and the gaps within these approaches. It is clear that before a firm tries to increase its risk management sophistication, it has to understand the gaps within its risk management practice. Consider figure 1 that shows a risk management maturity curve. This curve is a simplified version of the Risk Management Maturity model that we will introduce in Chapter 4. This curve can be used by a firm to assess its current risk management capabilities and sophistication.

This curve compares the degree of risk management sophistication and integration of a firm with the firm's scope of risks. As the degree of risk management sophistication of a firm increases, the firm needs to be more integrated across business functions (boundaries). This means that as the sophistication increases, the firm should move from simple hazard management to financial risk management. Thereafter, it should move to operational risk management and finally integrate strategic risk management as well. The placement of a firm on this axis determines the risk management sophistication of a firm, and the degree of integration across the firm. For example at the lowest level of the risk management curve is a risk

management strategy that's focused on hazard mitigation only. At this point the risk management strategy is silos based and the firm has minimal integration across the boundaries.

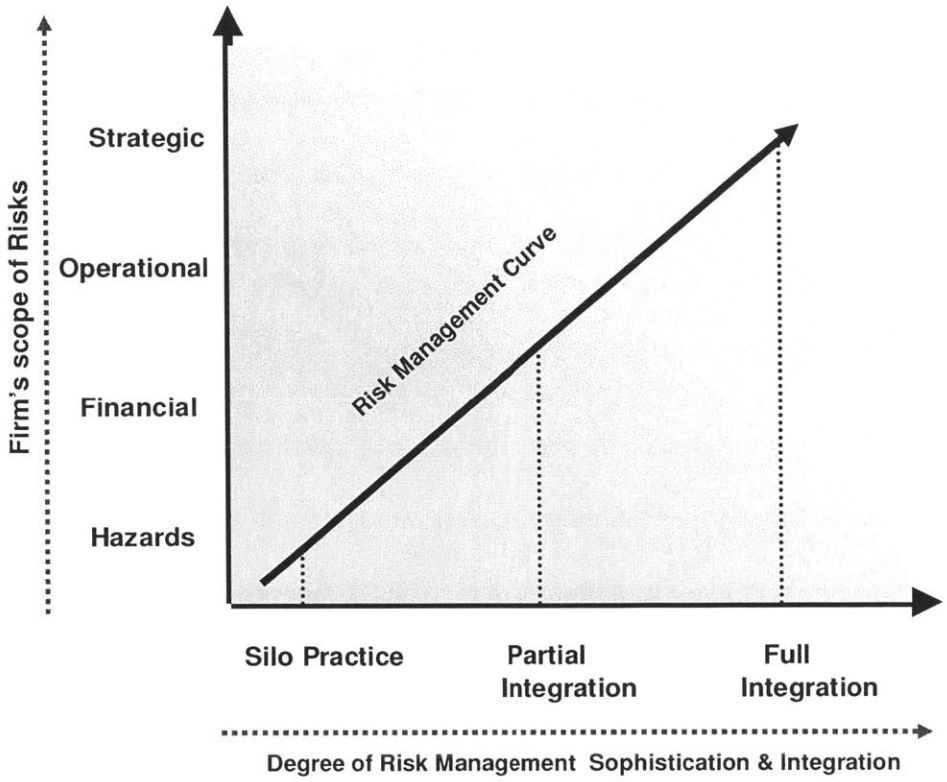


Figure 1: Risk Management Maturity Curve

At this lowest level of sophistication level the firm doesn't have a common risk language across the firm and uses inconsistent risk methodologies across the business units. Therefore, a risk that is severe according to one business unit could be medium risk to other because of inconsistency in risk language and methodologies. In such a scenario, the firm is using one or more of the four risk management approaches described in section 2.3. The hazard mitigation responsibility is usually handled at the business unit level and therefore it encourages a silos based culture, because of the localization of the mitigation effort. In an agile organization risk related knowledge should disseminate faster than any other

information. Adopting such silos based approach the risks get isolated and mitigated within business unit boundaries, which according to Paul Carlile (Carlile, 2004) creates short term benefits but generates much bigger risk in the long term.

The middle portion of the curve depicts a risk management approach that has moved beyond the silos based approach and has attained some level of partial integration across the firm. Apart from hazard mitigation, the firm at this stage is involved in financial risk management as well. At this level the company has some uniformity in risk analysis methods across business units and a common risk language. Finally, at this level the firm has made some advances in nailing down the operational risk management as well. In a nutshell, the middle domain is a cross between silos based risk management, financial risk management and some advances in operational risk management.

The top portion of the curve depicts the most sophisticated risk management approach within the firm. At this level of risk management the firm is fully integrated across various business units, has sophisticated operational risk management in place and uses consistent risk language, methodologies and risk processes across the firm. Also, at this level the firm has a strategic risk management in place; which means it has risk-reward relationship tied to its business strategy apart from having a risk adjusted returns based culture across the firm. In a nutshell the top level is a cross between financial, operational, informational and strategic risk management.

In summary to achieve sophisticated risk management, firms need to move up the risk management curve with time. Nevertheless, the current risk management approaches address only certain specific risk management issues and do not provide a generic approach that could be used by a firm to advance to the next level of risk management sophistication on the

risk management curve. This is where our work fills such a wide gap. It propounds a generic risk management approach through a combination of knowledge and risk management frameworks. The following section briefly touches upon our holistic approach and the solution we propose.

2.5 Our Approach and Solution – ICRM© and 3T- 4R Framework

In view of the shortcomings in the current risk management approaches and the challenges faced by the firms to traverse the risk management curve; our risk management approach, called Integrative Risk Management Approach (ICRM©) uses a generic framework to assist firms navigate the risk management curve.

The ICRM© approach looks at the firm as a systems architecture and advocates using 3T-4R framework to handle risk management at the macro or the micro level. The 3T framework is a knowledge management framework that was introduced by Paul Carlile and is explained in section 3.3 of Chapter 3. The 3-T framework takes at it main unit of analysis is the boundaries between different silos or domains—and so manage novelty or risk participates on either side of the boundary have to have the capability to represent that novelty to each other. The 4R framework is introduced in Chapter 4 and outlines a four step process of managing risk that has a direct overlap with the process steps developed in the 3-T framework.

Given the generic mechanisms outlined the 3T- 4R framework could be applied to any firm to examine what is present or lacking in effectively managing risk. The framework is powerful enough to unearth dormant risk trigger points for each business and does not advocate a silver bullet approach. Also, the risk mitigation aspect is tightly tied to business value impact thereby advocating lower mitigation related investment for low business value impact scenarios and vice-versa.

Finally, the 3T - 4R framework combines strategy & execution is applicable to operational scenarios based on solid financial analysis where possible. It combines qualitative and quantitative analysis.

In summary, our work proposes a generic systems level approach using a combination of knowledge and risk management framework (3T-4R) to help firms achieve risk management maturity across the risk management curve.

2.6 Chapter Summary

The chapter started with a historical view of theory of risk, and its development from 10th Century B.C to 21st century. Thereafter, we discussed risk management with respect to high-tech world. The reasons of risk management neglect within the high-tech industry were discussed before touching upon the reasons that have made high-tech industry change its attitude towards risk management in recent past. The four popular approaches towards risk management and their pitfalls were discussed thereafter.

We argued that firms face risk management implementation challenges not only because of these incomplete market approaches but also because of intra-company challenges owing to culture, communication and non-uniform risk approaches. This is why firms fall at different points of the risk management curve that was introduced in section 2.4. Finally, we introduced our systems level ICRM risk management approach and the 3T-4R framework that would help companies traverse the risk management curve irrespective of their level of risk management sophistication.

The next chapter intends to do literature review of firm-analysis, communication, knowledge management and risk analysis frameworks that will form the core of 3T- 4R solution.

3 LITERATURE REVIEW

In the academic and industrial circles there is abundant generic literature on risk, nevertheless there is almost limited or no work on efficient and workable risk management methodologies that could be used by high-tech organizations. The ICRM© framework introduced in Chapter 4 builds heavily on organizational analysis and learning capability of an organization. Paul Carlile has done path breaking work in this area and this chapter will touch upon these frameworks. Subsequently, a few popular risk analysis frameworks are analyzed as well.

3.1 Organizational Rigidities

The best firms that are able to thrive in a risky environment are the one that are adaptive to learning and are able to shed off organizational rigidities that impede this learning. It's been seen that established organizations have difficulty dealing with change. (Leonard-Barton, 1992) Leonard-Barton expands upon the idea of core competencies and introduces the concept of core rigidities. He notes that organizations are often unsuccessful when trying to adapt to new ideas, while innovating outside of their core competencies. Leonard-Barton describes the difficulty in modifying core competencies as core rigidities. There is a great inertia in the organization to resist change in the processes that have brought success in the past. At the same time, there is inertia in introducing new processes for new initiatives. In the context of this work, firms face challenges while introducing risk management processes in place, if they are not in place from past.

Getting an organization shed its organizational rigidities and adopt a holistic risk management approach requires a disruptive thinking approach. Utterback has argued about creating disruptive

technologies (Utterback, 1994), but Carlile makes the argument that it is more important to develop a disruptive organization (Carlile, 2004) rather than just disruptive technology. According to Carlile it is imperative to innovate within teams or an organization will not be able to effectively transfer the best ideas within organization. Carlile also argues that an organization that is capable of evolving its form and function will be better at generating and sustaining competitive advantage. It is in this context of organizational rigidities that Carlile's work on organizational lenses and knowledge management is a prerequisite before delving into the details of 3T-4R framework. Irrespective of the efficiency of the 3T-4R and ICRM framework, an organization will fail to take its advantage if it's not able to shed its rigidities and embrace change. Nevertheless, before initiating any positive changes it's pertinent to understand the organization as a strategic, political and cultural unit and thereafter follow an appropriate change management strategy. Paul Carlile's 3-Lenses help us understand the organization from these three viewpoints. The 3-Lenses are covered in the following section.

3.2 3 – Lenses

According to Paul Carlile, organizations could be seen in three lights, or through 3-Lenses. Looking at organizations in these lights helps in understanding the organization. This in depth understanding of the organization can be effectively used to implement change management. The three lenses are as follows.

3.2.1 Organization as Strategic Design

In viewing the organization as a strategic design, (Carlile, 2004) the organization is seen as an input, throughput and output system, and the role of the leader is seen as a strategist or organizational architect. In real world, the strategic lens could be used to understand the strategic

path of the organization. In the context of risk management studying an organization as a strategic organization helps understanding the relationship between risk and corporate strategy at the corporate level. If the organization is centered around a corporate strategy of high risk, high reward relationship; risk management goals are different compared to an organization that's centered around a corporate strategy of low risk, low reward relationship.

3.2.2 Organization as a Political System

The organization is viewed as an arena for conflict, while viewing organization as a political system. (Carlile, 2004) While viewing organization through this lens, it's important to understand the various stakeholders, their relative power and influence, their interests and the dominant coalitions in the organization. The leader in such a system is seen as an astute negotiator who forges right coalitions while identifying and leveraging interests of various stakeholders. In the context of risk management, the political lens is very important, especially if the firm has organizations rigidities in place. In the context of risk management, right coalitions can make the make or break difference. Risk management being a truly cross-functional exercise, an executive level commitment is required from all business units. In a large organization, this is only possible if a right coalition is formed at the top corporate level that would drive the enterprise level risk management exercise while facing minimal resistance.

3.2.3 Organization as a Cultural System

In viewing organization as a cultural system (Carlile, 2004), the organization is seen as a shared social construction. This social construction has shared identities, symbols, cultural products, values and assumptions. The role of leader in such a system is to articulate the vision, the symbol of the culture and leveraging the culture of the organization. In context of risk management,

cultural lens is very critical as it helps understand the dominant culture and established mindsets that could challenge the change required to implement risk management in place. Understanding the culture of the organization helps understand what works and doe not work in the organization. Also, the cultural lens provides insights into the top-down versus bottoms-up risk management approach.

3.3 3-T Framework

According to Paul Carlile, organizations are a collection of boundaries where knowledge/information must be shared for the stakeholders to be effective. Nevertheless, the challenges faced by organizations are often dynamic in nature. As a result, the nature of boundaries is also in flux, which presents different contexts for the movement of knowledge. The 3-T framework (Carlile, 2004), shown in Figure 2, provides a means of discussing the different types of boundaries.

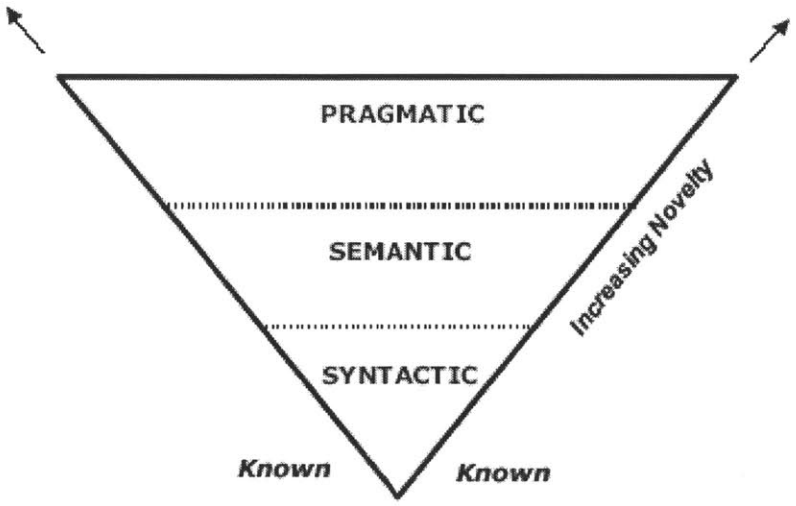


Figure 2: 3-T Framework

The transient nature of contextual knowledge is captured by novelty. According to Carlile novelty is a change in a complex system that is different or unique when compared to what is originally known. Note that novelty is deliberately used in place of uncertainty. Unlike uncertainty, something that is novel is not immediately recognized. It is something new and unknown for the person experiencing it and can easily be seen as irrelevant. (Carlile, 2004) As the level of novelty increases between two actors, the movement of knowledge changes across the boundary. The first boundary is Syntactic; at this level a common syntax exists between actors and the status of the boundary is stable. Therefore, it is sufficient to simply transfer information.

The next boundary is Semantic, and interpretation and relevancy of knowledge is different on each side of the boundary. In addition, all of the differences and dependences between the actors are not known. A shared meaning or common syntax must be created to communicate effectively. In other words, the knowledge on each side of the boundary must be translated for it to be relevant for the actors on each side.

The pragmatic boundary is at the highest level. At this level, novelty has risen to the point where each actor's knowledge impedes the other. Change will be required to create a common set of interests. Differences and dependencies across the boundaries have negative consequences. Knowledge must be transformed to represent the impact of novelty. In addition, the consequences for each side need to be understood before making tradeoffs. Carlile's 3-T framework directly relates novelty with increasing knowledge transfer complexity. With respect to risk management, the 3-T framework provides a language to deal with novelty as it arises in form of unknown risks or the new knowledge that comes across actors while sharing risk management solutions across business units.

In terms of the 3-T framework, the firm has to have the capacity plus the ability to have the capability to "see" the risk. Without such a capability the firm won't be able to recognize the novelty. The following section goes into details of increasing novelty and risk management capabilities.

3.3.1 Parallelism between 3-T and Risk Management

The 3-T framework provides a means of discussing the types of boundaries in an organization and the flow of knowledge between these boundaries. Risk management in a broad context is also about learning how to manage the knowledge related to "risk" between the boundaries of an organization; and thereafter taking actions to mitigate these risks. Therefore, there seems to be a fundamental relationship between knowledge management and risk management. This relationship could be captured by drawing parallelism between 3-T and the 4-R[2] framework.

The transient nature of contextual knowledge is captured by novelty in the 3-T framework. Novelty is something new, different and unique compared to what an organization is used to in terms of knowledge. Therefore, it could be argued that risk is about understanding and managing novelty. Note that novelty is not uncertainty, but novelty, whether external or internal causes uncertainty; which has strong relationship with risk. Figure 3 shows the parallelism between 3-T and 4-R framework. Note that the three boundaries in the 3-T framework; the syntactic, semantic, and pragmatic boundaries correspond to the first three stages from the 4-R framework i.e., risk identification, risk analysis and risk mitigation. The fourth step in the 3-T framework, the iterative loop corresponds to the risk monitoring phase of the 4-R framework.

Therefore it can be argued that the parallelism between 3-T and 4-R is based on a correspondence relationship.

---

[2] The 4-R framework is covered in details in Chapter 4

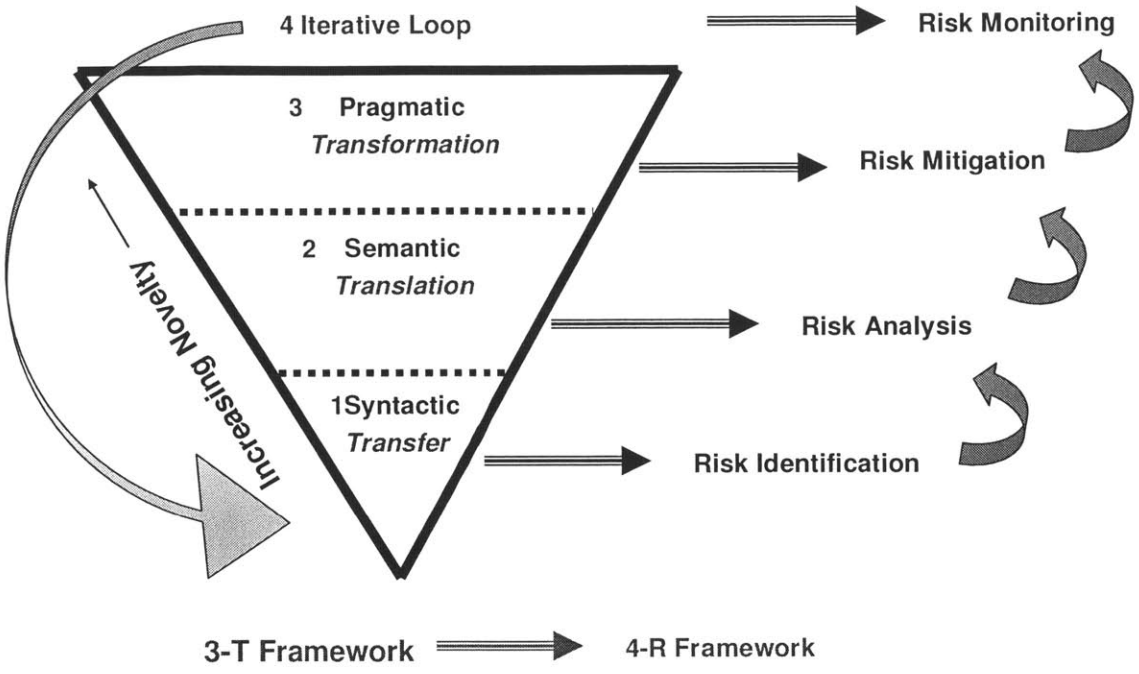


Figure 3: Parallelism between 3-T Framework and 4-R Framework

In the 3-T framework, the transfer of knowledge corresponds to the risk identification phase of the 4-R framework and at this level developing a common lexicon capacity, a common language to describe risk, is most important. The translation of knowledge corresponds to the risk analysis phase of 4-R; at this level having a common language and establishing common meaning is essential to address the novelty present. The transformation of knowledge corresponds to risk mitigation stage of 4-R and at this level apart from establishing common language and meaning, establishing common interests is also important. Finally, the iterative approach, where actors get better at developing an adequate common knowledge for sharing and assessing each other's knowledge – corresponds to the risk monitoring stage of 4-R. The

correspondence between the various types of boundaries and the 4-R framework is explored in more details in the following paragraphs.

The syntactic boundary has the least amount of novelty present within it. A syntactic capacity requires the development of a common lexicon for transferring domain specific knowledge. Figure 4 shows the correspondence between the syntactic boundary and the 4-R process.

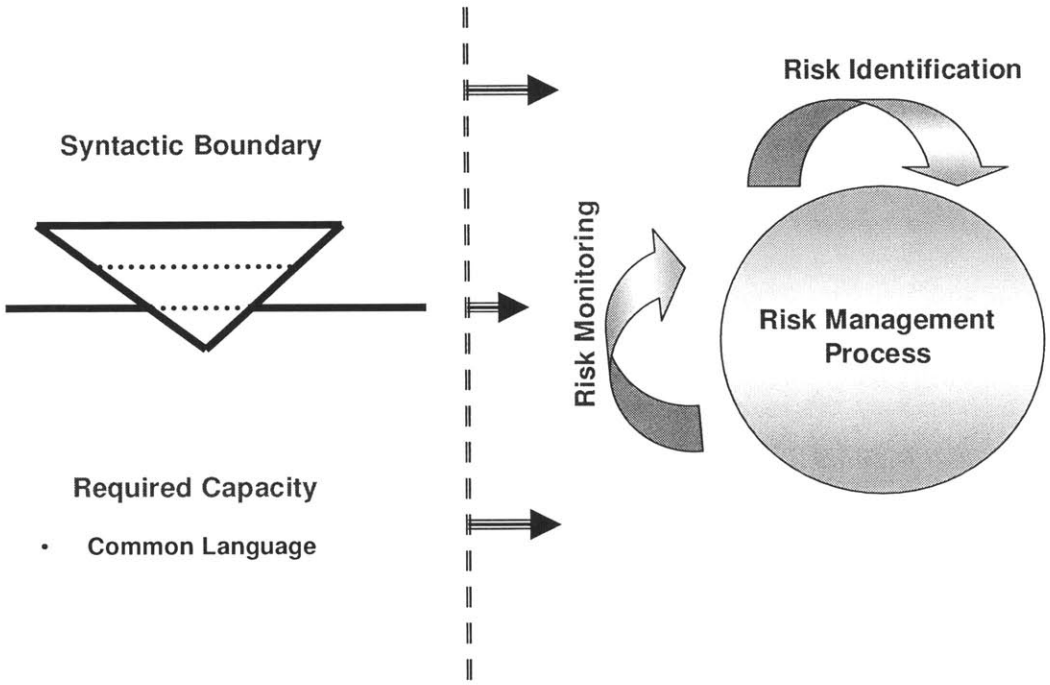


Figure 4: Syntactic Boundary: Correspondence with 4-R

In this case the status of the boundary is stable, and it is sufficient to simply transfer information. This corresponds to establishing generic risk identification methods and processes within a business unit or the firm. At the risk identification level, there is a need to develop a

common terminology for "risk". The meaning of risk as understood by a technology strategy group could be very different than the meaning understood by a supply chain group. The technology strategy group would probably focus more on the strategic side of risk, while the supply chain side could be more focused on the operational side. Therefore at the syntactic level, or the risk identification stage, it is important to have a common risk lexicon to transfer risk knowledge. This argument is parallel to the assertion that if the risk is stable then syntactic boundary is faced and a common language for identifying those known risks along with a process of iterating and monitoring the boundary will be sufficient to manage the relationship at the boundary. For example, consider the risk of China adopting a market determined Yuan. Although, this would be a huge risk in terms of its effects on business in Asia-Pacific, nevertheless, as long as the firm has a monitoring mechanism that warns it of the impending changes; the risk could be treated as a fairly stable risk. In such a case it is good enough to monitor the risk at the boundary, without immediately going into building a capacity for countering the risk.

The next boundary in the 3-T framework is the semantic boundary. At this boundary the novelty has risen above the syntactic level and more capability needs to be built into the system to counter the risk at hand. In terms of complexity, this boundary lies between the syntactic level and the pragmatic level, while in terms of novelty the inherent novelty in the system is in a mid-range between the syntactic and pragmatic level.

Figure 5 shows the relationship between semantic boundary and 4-R framework. Note that in this relationship, only three capabilities from the 4-R framework are shown, because these are three capabilities that the system need to develop as discussed in the following paragraphs.

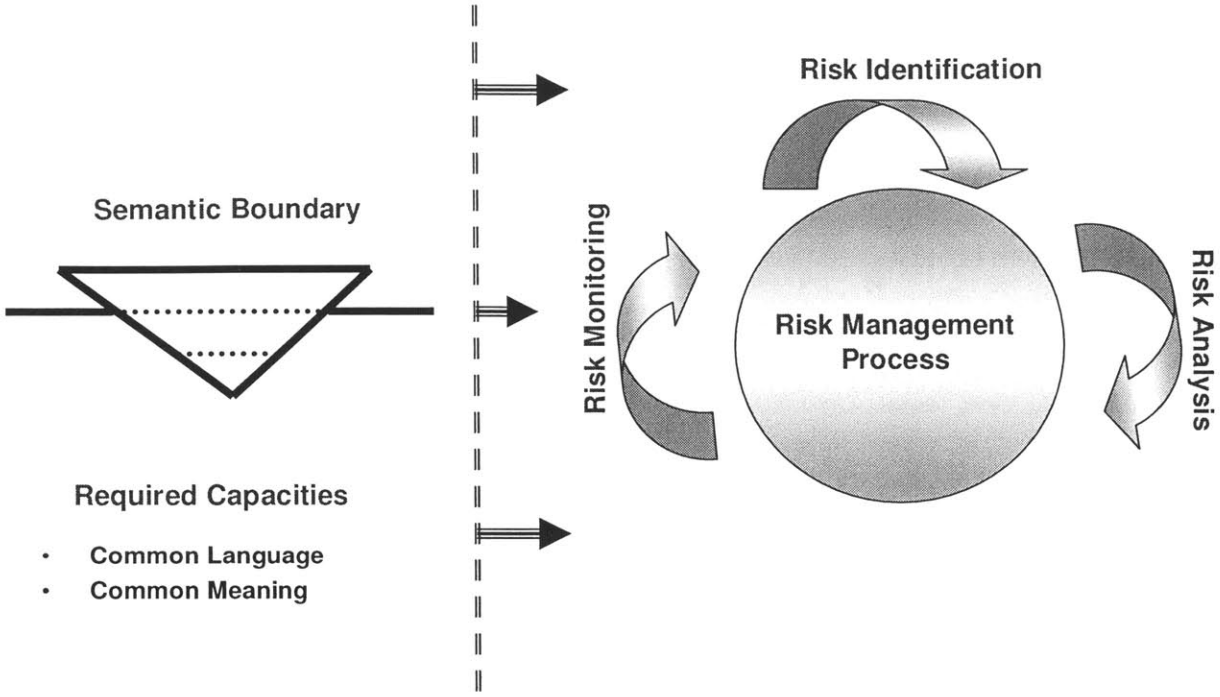


Figure 5: Semantic Boundary: Correspondence with 4-R

At this level the interpretation and relevancy of knowledge is different on each side of the boundary and all the differences and dependences between the actors are not known. A semantic capacity develops common meanings for identifying novel differences (Carlile, 2004), dependencies and translating domain-specific knowledge. Within the semantic boundary, the risk identification, risk analysis and risk monitoring capabilities from the 4-R framework need to be developed. In other words, the knowledge on each side of the boundary about risk must be analyzed translated for it to be relevant for the actors on each side. In other words when novelty arises and new risks are faced a semantic boundary is present. Here an iterative process of

developing common language and meaning must be developed. For example – if brand reputation risk is increasing because of quality issues than a new language and meaning must be developed between these two departments to understand and mitigate the risk. The required correlative risk processes are identifying, analyzing and monitoring risk. In some situations the new risks will be identified and small changes can be made to address them. In other situation the risks identified require substantial changes in order to mitigate risk- and so a pragmatic boundary is now faced.

The next boundary in the 3-T framework or the pragmatic boundary is at the highest level. At this level, novelty has risen to the point where each actor's knowledge impedes the other and change is required to create a common set of interests.

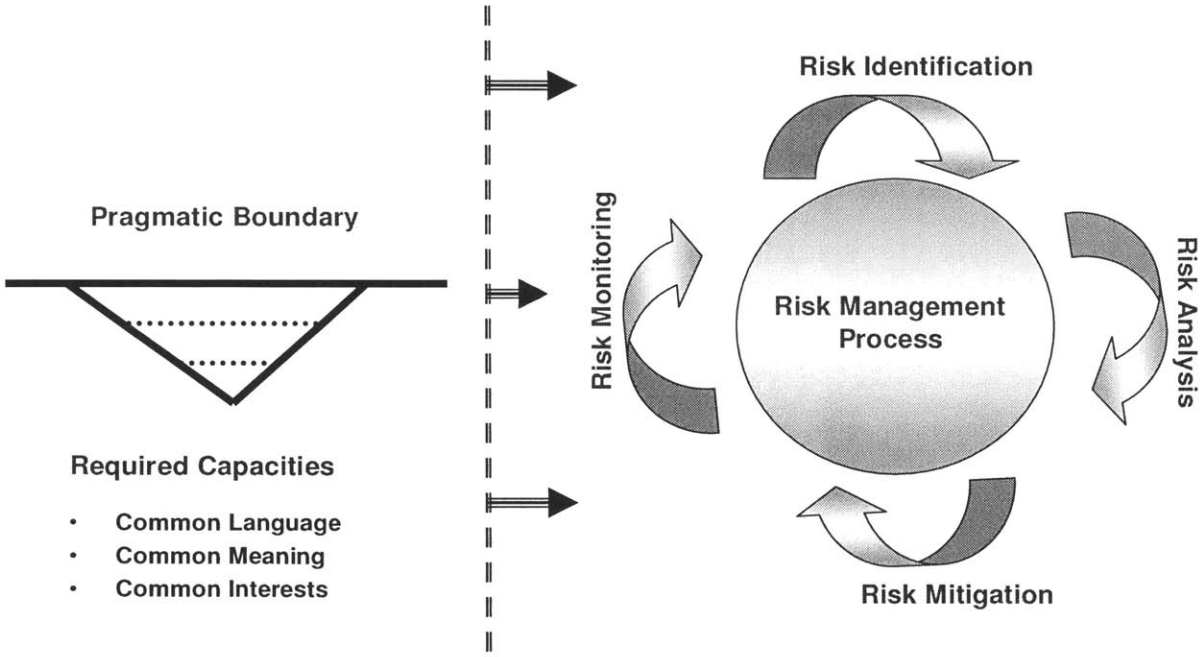


Figure 6: Pragmatic Boundary: Correspondence with 4-R

Figure 6 depicts the relationship between pragmatic boundary and 4-R. At this level there is a need to develop capacities to establish common language, common meaning and common interests for making trade-offs and transforming domain specific knowledge. At this level, all four stages i.e., risk identification, risk analysis, risk mitigation and risk monitoring from the 4-R framework are required. When significant risks are faced then major changes need to occur between the parties involved—so in other words to mitigate risk pragmatic change is required for those involved—how they operate in their own domain and how they now measure risk.

It is clear from the above discussion that there is a correspondence relationship between 3-T and the 4-R framework. Different boundaries, based on the level of knowledge management sophistication require different phases from the 4-R framework. The syntactic boundary, that has the least amount of novelty in the system requires only two phases from the 4-R (identification and monitoring), while the pragmatic boundary that has the maximum amount of novelty present requires all four stages from the 4-R framework. In summary, the combination of 3-T and 4-R can help a firm understand the risk capacities that need to be built at each boundary of the firm. By using such an approach the firm will have a common set of risk language, syntax and risk processes. By using this common set of language, syntax and processes the firm can advance on the risk management curve that was introduced in section 2.4.

3.4 Risk Analysis Frameworks

One of the biggest challenges with risk frameworks is their non-uniformity of application. Based on the current approaches that were introduced in Chapter 1, no single approach could be used to analyze risk in all situations. For example the strategic approach could be used to identify risk-reward relationship at the corporate level, but it could fail at the operational level in absence of

any analytical or actionable analysis. Similarly, the information management approach could be helpful if the risk indicators could be clearly identified and quantified. Nevertheless, information management approach could fail in the case of qualitative risk analysis scenarios. Firms have long struggled with identifying the right approaches and frameworks to analyze risk at the micro and macro level.

In the following sections we discuss two risk analysis frameworks. Section 3.4.1 discusses a few corporate level risk analysis frameworks, while section 3.4.2 discusses Value at risk (VaR), a micro level risk analysis framework, that's commonly used in the financial world. The value at risk framework is of particular interest to us, since it will sit at the core of a few risk analysis methodologies that we will introduce in Chapter 4.

3.4.1 Integrated Risk Measurement at Corporate level

The top leadership of a company is interested in risk-reward relationship at the macro level; the boundaries they consider or recognize as consequential. Examples of these are *"economic capital"* (EC) and *"Risk-adjusted return on capital"* (RAROC). (Marrison, 2004) These two frameworks measure risk at "macro" levels or the boundaries that the top management values.

Economic capital provides a common framework for quantifying the risk from many diverse sources and also allows us to calculate the amount of equity capital that a firm should hold. RAROC on the other hand allows us to compare the profitability of different transactions. RAROC is slowly becoming standard way of measuring risk-adjusted profitability. RAROC ranks transactions according to their expected return adjusted in some manner for their risk. Transactions that offer a risk-adjusted return on capital above some threshold are accepted. Those that do not are rejected. RAROC also has a slight variation called *Shareholder Value*

Added (SVA). The next section discusses value at risk, a framework that's used in the financial world.

3.4.2 Value at Risk (VaR)

Value at Risk is one of the most widely used measures of potential loss from an unlikely, adverse event in a normal, everyday business environment. VaR is denominated in currency units and therefore gives a risk-loss relationship that can be easily understood. In a typical situation VaR is an amount, say D dollars, where the chance of losing more than D dollars is $p\%$ over a future time interval of t days. The above statement being a probabilistic statement, VaR is a statistical measure of risk exposure and its calculation requires application of statistical theory. An exhaustive analysis of VaR is outside the scope of this work, although a decent in depth analysis is provided in Appendix 10.1.

Within the context of our work, calculating the VaR for a situation would include the following steps.

- Business impact value estimation
- Likelihood estimation of event
- Variability calculation of risk factors (if the risks are independent, the variability in the risk scenario is the product of individual probability distributions)
- Setting up the time horizon
- Setting up confidence level
- Calculate worst case loss for each scenario
- Construct probability distribution for the worst-case loss from the above scenario data.

3.5 Chapter Summary

This chapter did the literature review of popular organizational, knowledge management and risk measurement frameworks. Carlile's 3-T framework for novelty assessment and 3-Lenses framework for organizational analysis were introduced. Thereafter, the parallelism between 3T and 4R frameworks was addressed. It's critical to note that as the level of novelty increases in a system the level of risk management capabilities required also increase. It's this parallelism or the 3T-4R framework that will be the core of our risk management solution

Thereafter we discussed the limitations of the current risk management approaches, and discussed how a framework or methodology based on these current approaches would fall short; a challenge that our work, through the usage of 3T-4R framework solves.

Thereafter, RAROC and Economic Capital, two common frameworks used at the corporate level were discussed. Finally, Value at Risk, a popular risk measure used in the financial world was introduced. VaR is of special importance to this work, since it will be used as a core measurement technique for various risk analysis frameworks that will be introduced in the next Chapter. The next chapter introduces various risk management frameworks that this work has come up with.

4 RISK MANAGEMENT FRAMEWORKS

In this chapter we introduce our frameworks and methodologies that were briefly touched upon in Chapter 2 and 3. Before a firm decides to become a sophisticated risk management user, it needs to identify its current risk management capabilities, and establish a risk management path for itself. The Risk Management Maturity Model (RMM©) could be used to accomplish this task. This model is introduced in section 4.1; note that the risk management curve introduced in section 2.4 is based on this RMM model.

Thereafter, we introduce the 3T-4R© Framework. The 3T-4R framework is based on Paul Carlile's 3-T framework (section 3.3) and the 4-R methodology, that's being introduced in section 4.2. The 3T-4R framework is a generic and scalable framework that can help firms navigate the risk management curve described in section 2.4

Subsequently, we introduce a few risk analysis methodologies for specific business functions. As we have previously argued in Chapter 1, one of the big gaps in the current risk management approaches is the use of similar risk analysis approaches in all business situations. This being not true, we tackle a few business functions and come with analytical risk analysis methodologies for them. Note that these methodologies do not reduce the generic usability of 3T-4R framework; the 3T-4R framework provides a generic framework to tackle risk management, while the specific risk analysis methodologies are to be used once the 3T-4R framework has identified the risks and their business nature.

Since, it's outside the scope of this work to come up with customized risk analysis frameworks for all business functions; we tackle three important business functions only – M&A, supply chain management and Information Security.

Finally, we tie these frameworks and methodologies together in the Integrative Corporate Risk Management (ICRM©) framework together to get the enterprise wide risk management picture. It is at the ICRM© level that we see how 3T-4R and unique risk analysis methodologies gel together within the organization to provide an ERM solution.

4.1 Risk Management Maturity (RMM©) Model

Before starting the risk management goal within a firm it's important to find the firm's maturity on the risk management curve. Every firm has different needs and goals, therefore by finding out where a firm stands on the risk management curve, and where it desires to be - can help the firm adopt the right risk management strategy. The risk management model shown in Figure 7 can help firms identify the right risk management strategy. The vertical axis shows the firm's scope of risks, while the horizontal axis shows the present degree of risk management sophistication and integration of the firm. The alignment axis on the right hand side tells the degree of alignment that's required for a firm as it moves up the risk management curve. For hazard mitigation based on silos practice, the firm needs or has minimal integration. As the risk management sophistication increases or is required, the firm's scope of risks increases from hazard to strategic; while the level of integration increases from no alignment to full alignment.

To find out the position of a firm on the risk management curve, the firm needs to do a critical assessment of its current risk management practice in three dimensions; the firm's scope

of risks, the degree of risk management sophistication and the level of alignment in place across the firm.

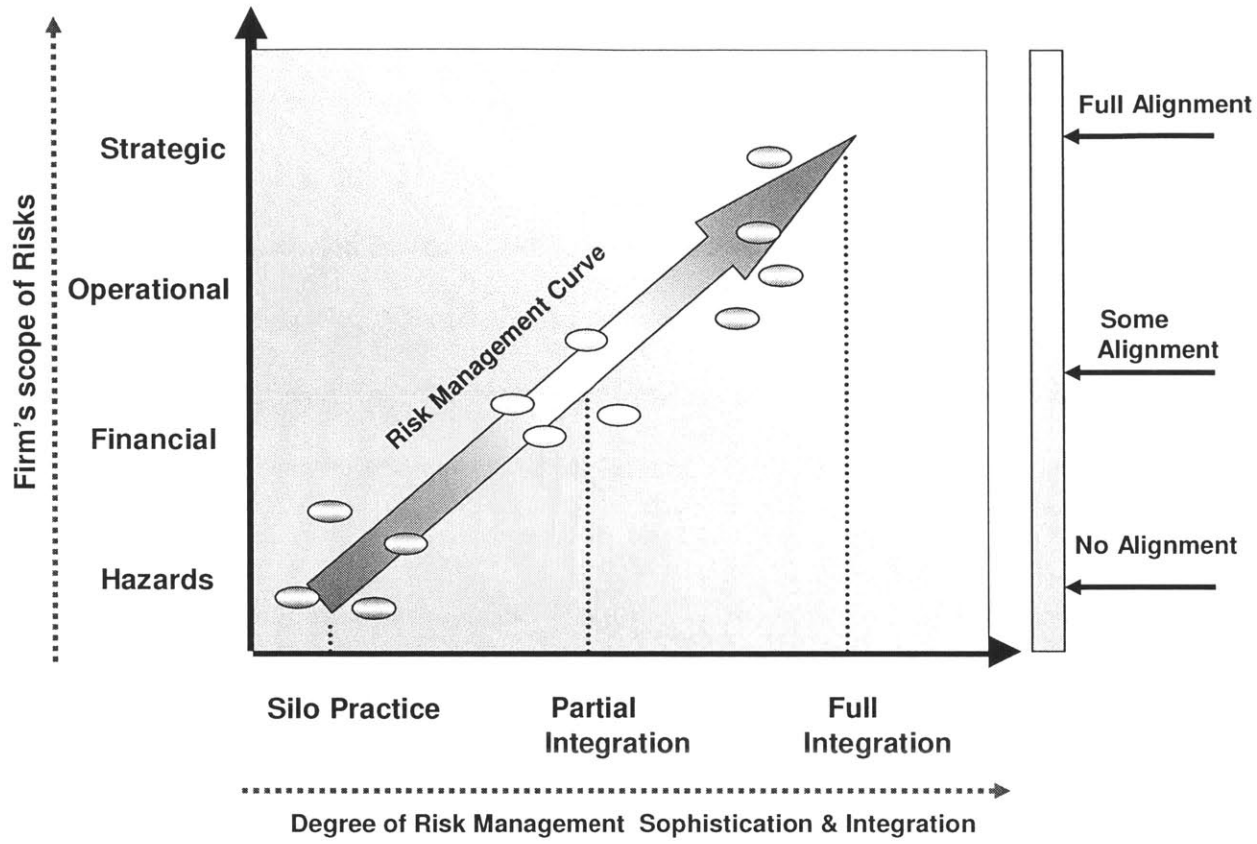


Figure 7: Risk Management Maturity Model

The red circles denote the firms that have silos based risk management practices and focus only on hazard management. These firms have the least advanced risk management practice and need to move up the curve, if their business conditions demand so. To move up the curve, these firms need to manage their financial risks and achieve partial integration.

The yellow circles denote the firms that have achieved partial risk management integration across business functions. Apart from hazard management, these firms also have

financial risk management in place and are looking forward to operational risk management. These firms have moderate to good risk management practices in place. To move further up the curve, these firms need to make advances in operational risk management, by using customized risk analysis methodologies for various business risks. Also, these firms need to integrate strategic risks in their scope of risks, and achieve full risk management alignment across various business functions.

The green circles denote the firms that have achieved success managing the operational and strategic risks. These firms are at the highest level of risk management curve and have achieved full risk management alignment and integration across various business units. These firms are the most agile risk managers and can achieve the optimal risk-reward ratio in their day to day business.

After a firm has identified its location on the risk management curve, and decided its target position - it can use the 3T-4R framework to build business function specific risk solutions, eventually integrating them through the ICRM framework. The 3T-4R framework is explained in the following section.

4.2 3T-4R© Framework

The scope of identifying, analyzing, mitigating and monitoring risks at the firm level is a humongous task; therefore a disciplined risk management approach is required. The 3T-4R framework provides such a disciplined approach at the macro or the micro level. On the macro level the analysis could start with the firm, taking a top-down approach. On a micro level, the analysis could start at the business function or division level, and then moving to a bottoms-up approach. Figure 8 shows the four steps involved in the process which are explained below.

These four steps describe the overall process that would have to be completed to adequately manage risk at a given boundary or set of boundaries.

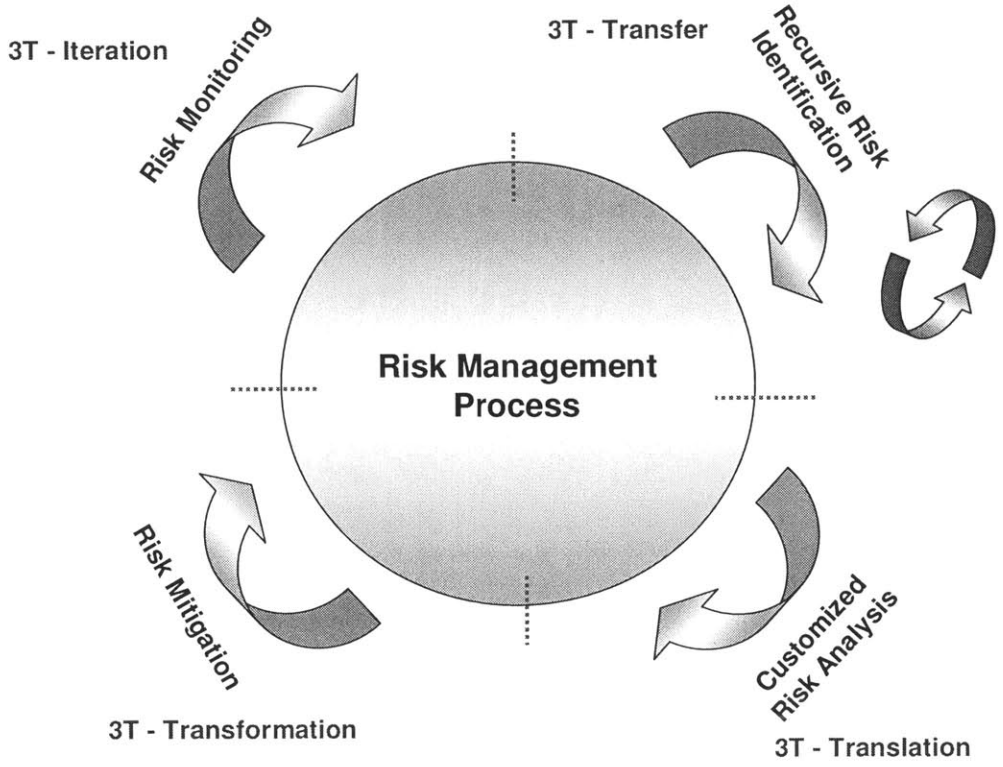


Figure 8: 4-R Framework

4.2.1 Recursive Risk Identification

Recursive risk identification is the first step in the risk management process. During this stage, the risks should be identified in a recursive top-down approach using MECE (Mutually Exclusive Collectively Exhaustive) methodology. This approach lays down all risk factors in a tree form, and then each risk factor is revisited to find out the risk trigger events that could generate these risks. A lot of firms use linear risk identification process instead of recursive method; the linear method although satisfactory doesn't unearth all the underlying risk trigger

points of the base risk. The basic difference between the linear risk identification and the recursive risk identification method is in the efficiency of finding dormant risk trigger points. For example, while analyzing the risks in introducing a new product, it might seem that slow rate of network diffusion could be a risk, but on recursively analyzing the rate of diffusion, the real reason could be the disparate standards, that will minimize diffusion. The linear method of risk identification does not go deep into risk trigger points and therefore the company might be mitigating the wrong risks.

4.2.2 Customized Risk Analysis

The risk identification stage is followed by the risk analysis phase. This phase is the most confusing and least understood part of the risk management process. The confusion stems from an attempt to analyze all risks using the same methodology or framework; which at best is faulty. No two risks are similar therefore their corresponding impacts can not be analyzed in the same fashion. Firms end up with faulty risk analysis because of imposing the same analysis method to different risk scenarios. It is this force-fitting of a common methodology that can eventually lead to an incoherent risk management strategy within the firm.

For example – the business impact analysis of brand collapse is very different than the business impact analysis caused by single-node disruption in the supply-chain of the company. While VaR could be a good methodology to analyze business impact of brand collapse; expected monetary value loss could be a better methodology to analyze the business impact analysis of single node disruption in the supply chain of the firm.

In terms of 3T-4R framework, this means that at different boundaries, different risks are there; and further they require different (customized) boundary objects in order to adequately measure the risks that are present there. In a nutshell, the risk analysis stage is about building a

common language and meaning to do risk mitigation. The risk mitigation stage is explained in the next section.

4.2.3 Risk Mitigation

After the risk identification and risk analysis phase comes the risk mitigation phase. Risk mitigation is about the actions and the changes we make to address the risk. In this phase right execution is everything. Like the risk analysis stage, the mitigation plans can not be uniform for all business functions. Each business function requires a customized mitigation plan and needs a different execution priority and focus. One of the challenges faced by the firms during this phase of risk management is the difference between having a risk mitigation plan and "implementing" the mitigation plan.

Firms that do business with Asian suppliers face this challenge frequently. In most cases, to get large supply orders from US firms, these firms need to have a business continuity plan in place. Nevertheless, the challenge is with the business continuity plan implementation. The US firm would not know if the plans exist only on paper or if they have been operationally implemented. Therefore it is important that the US firms focus not only on their internal risk mitigation plans, but also on the audit of risk mitigation plans of their suppliers and other partners.

In terms of the 3T-4R framework, risk mitigation is very much about the actions that we take to address the risks. This is very much like dealing at the pragmatic layer where change and transformation are required to address the novelty present. The final step in the 3T-4R framework is the risk monitoring phase, which is explained below.

4.2.4 Risk Monitoring

After the first three phases, the firms need to have a monitoring process in place to monitor the various mitigation plans and variance in the levels of various risks on a day-to-day, weekly or quarterly basis. In this phase uniformity of processes is probably the most important thing. Using a common language, meaning, interests and standard set of processes, the firm can monitor various kinds of risks and see if any one of them is showing huge variance and need close monitoring or analysis.

Note that the monitoring process has a feedback loop to the risk identification phase. Based on the results of this monitoring the risks that show variance beyond the acceptable level could be further analyzed using the risk identification and analysis stage to find out if all risk trigger points have been accounted or not. In terms of the 3T-4R framework, this is equivalent to a feedback loop helps recognize the situation of increasing novelty. The extent of this novelty will determine the steps from the 3T-4R process that need to be taken again to accomplish risk management.

4.3 Risk Analysis Methodologies

The 4-R framework could be thought of as a set of four principles that could help building adequate capability at pragmatic boundaries. The capabilities would focus on creating common language, common meaning, common interests/pragmatics and iteration at the boundary. Although all the four steps identified in the framework are integral to the success of enterprise risk management, the second step; risk analysis poses the most challenges. In terms of 3T-4R, this is akin to using the specific object for the boundary in question. The boundary could be macro or micro, and it might not have the capacity to identify novelty as circumstances change.

This task of finding the right risk analysis method or the right object is a huge challenge, because it comes under the purview of operational risk management; which at best is a nascent and evolving field. Most firms are still at a loss deciding about the right methodologies to use while analyzing their business function specific risks. Inventing methodologies for all possible business functions is outside the scope of current work, but in next few sections we propose three novel methodologies to address the risk analysis part pertaining to a few important business functions. The methodologies that we propose could be used as pilot innovative methodologies, and could motivate others to come up with methodologies for remaining business functions. In terms of 3T-4R framework, this is akin to analyzing three types of risks or boundaries and three examples of boundary objects (risk analysis tool) used at each boundary.

4.3.1 M&A - *m*ValueRisk© Methodology

Risk practitioners follow a standard methodology while doing risk analysis related to mergers and acquisitions. According to this approach, they quantify the risks at each stage of M&A process and thereafter try to insure that risk, in case the deal doesn't work. This methodology is a decent approach to do risk analysis in the pre-deal stage, but doesn't really give any insights about value creation or destruction by the deal over a period of time for the firm. Doing risk analysis of the deal only till the "deal" phase is probably not the best way for a firm to understand the complete impact of the deal.

In fact, a deal that poses no risks at the time of deal, but then destructs value for the company over a period of time is worse than a deal that poses limited risks while execution but provides long term value. Cisco's acquisition of Linksys is one example. The deal was risky from the point of view of adjacency of business goals, but it created a lot of value for Cisco over a period of time. Figure 9 shows the *m*ValueRisk© methodology that tries to capture the pre-deal

risks and post-deal value-creation/destruction metrics to fully analyze the risks involved with a deal.

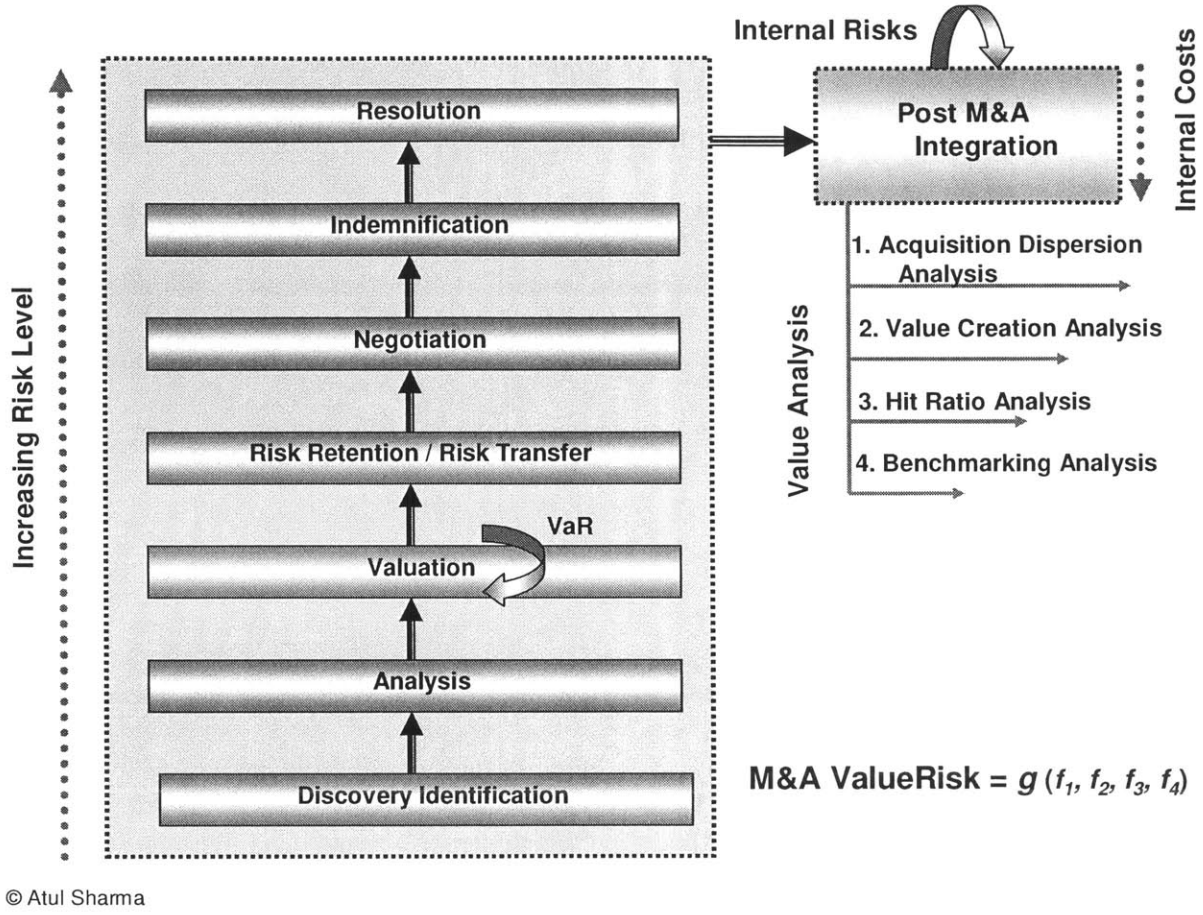


Figure 9: The *m*ValueRisk© Methodology

According to this methodology cost-benefit analysis is used to come out with a loss figure, if the deal fails at any stage of the process except for the valuation phase. The valuation phase uses Value at Risk (VaR) methodology. This phase uses VaR because valuation is highly subjective to future predictions of cash flows. This cash flow analysis could be tied to the parameters of the VaR methodology based on the likelihood of hitting these flows, subject to a likelihood function that depends on various parameters like industry state, possibility of the

business hitting its business goals etc. Based on this analysis, a comprehensive pre-deal risk analysis could be done.

To do the risk analysis of the deal, post integration and after a time period of ***n*** years, four more analyses are done; and the results of these analyses are combined through a relationship function.

- **Acquisition Dispersion Analysis**: In this analysis the deal is analyzed on a 1-10 scale of dispersion with the current business goals of the company. For example, if a software storage company buys an internet service provider there is no congruence in respective business goals. Therefore, there is a maximum dispersion (dispersion = 10) of goals in this case. Contrast that to Juniper Network's acquisition of NetScreen, a security company; an acquisition that has almost no dispersion (dispersion = 1).
- **Value Creation Analysis**: In the value creation analysis, a deal is analyzed based on the value it has created or destroyed based on the initial deal premises related to value creation. Note that this value doesn't need to translate to dollar amount, if perceived value by the company is more strategic than monetary. For example – a company could do an acquisition just to pre-empt the move by a competitor. In this case, the value creation analysis will be more subjective.
- **Hit Ratio Analysis**: The hit ratio analysis focuses on the "percentage success" of acquisitions based on the deal goals. A subjective hit/no-hit is assigned to the deal based on the perceived success of the deal by the firm.
- **Benchmarking Analysis**: In the benchmark analysis, the deal success is measured with respect to the prevalent venture capital analysis models. For example – as an industry standard, on an average, out of 10 deals, 5 should be failures, 3 should bring 5X returns, 1

deal should bring 10X returns and the another remaining deal should bring 100X returns. Although, this is a fairly rough benchmark, it's commonly used in the VC industry to measure the effectiveness of the firm in deal making.

Based on the above four analyses and the pre deal analysis done, the risk analysis for a deal could be done. Note that, this model is fairly subjective since the definition of "deal success" is highly dependent on the "deal objective". Nevertheless, if the above methodology is consistently used within a firm; a pattern could emerge based on the past deals. This analysis could help the firm perform the risk analysis of future M&A deals.

4.3.2 Information Systems Security – *i-sec*ValueRisk© Methodology

Information Systems Security is one of the most important operational risk management areas. In 1999 approximately $7.6 billion was lost in business productivity by Melissa, the worm and other viruses (Briney 1999). Although approximate business impact of information systems security is calculated based on lost productivity caused by denial of service, our methodology *i-sec*ValueRisk© provides a more exhaustive and analytical approach to do business risk analysis.

The *i-sec*ValueRisk methodology uses Value at Risk (VaR) to figure out the magnitude of potential losses that could occur because of information systems security issues. Although information systems security is an emerging field and accurate likelihood scenarios can not be forecasted based on past trends, our methodology does provide an elaborate roadmap to assess the risk and figure out the corresponding investments in mitigation plans to counter these risks. Figure 10 depicts *i-sec*ValueRisk methodology and is explained below.

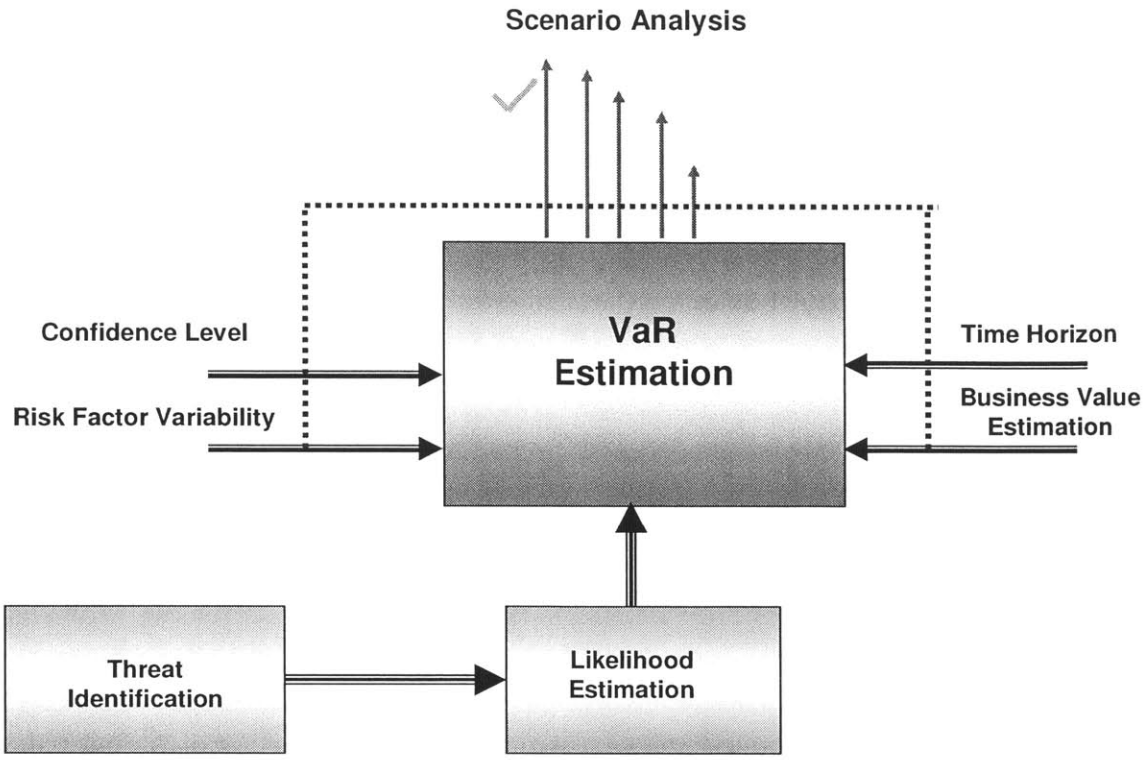


Figure 10: *i-sec*ValueRisk© methodology

Essentially the methodology involves the following steps.

- **Threat Identification**: According to a Microsoft Security (Microsoft Security, 2004) paper the various types of information security threats could include denial of service, information altering, information theft etc. Various methods that can be used to pose these threats could include using viruses, Trojan horses, worms, password cracking; e-mail hacking, packet replay and network spying. Once the threats have been identified, the next step is to perform likelihood estimation.
- **Likelihood Estimation**: Likelihood estimation could be done through a number of ways. Standard survey's viz., Ernst & Young IT security report could be used to find industry

averages for various types of IT security breaches. The other method that is popularly used is estimating frequencies from access logs. Based on industry survey, log data, historical data and some qualitative information from IT security personnel, it is possible to estimate the probability of a distribution of threats. Thereafter, possible risk scenarios can be developed based on the probability distributions of individual risks. A simple thumb rule for calculating scenarios is the 2^n rule; i.e., if there are n possible risks then there are 2^n possible scenarios.

- **VaR Estimation**: Once the different types of risks have been identified and their likelihood or the probability distribution estimated; the VaR can be calculated. The following steps help us calculate the VaR
    - Set business impact value for the situation
    - Calculate variability of risk factors from probability distribution of various risk scenarios. In case risks are independent, the variability in the risk scenario is the product of the individual probability distributions.
    - Set a time horizon for the possible loss
    - Set a confidence level
    - Pick the worst case loss for each case of risk scenario for the given time horizon.
    - Get the worst case loss probability distribution
    - From the distribution, calculate the worst case for a given confidence level- this is the Value at Risk (VaR)

This VaR estimate corresponds to the maximum dollar amount that the firm can lose over a period of time t at the $c\%$ confidence level. Note that the VaR computation can be further simplified if the worst-case loss distribution can be ascertained to belong to a parametric

distribution family viz., normal distribution. This VaR is taken as the risk analysis impact or the worst case business impact figure and the mitigation plan budget can be built around this figure

4.3.3 Supply Chain Management - *scm*ValueRisk© Methodology

Supply chain disruption is the biggest worry for operation managers. The disruption could happen because of a multitude of factors and nailing down the likelihood of these factors is a challenge. Most risk analysis methodologies currently used assign a dollar figure to a supply chain node and tie the likelihood of node disruption to catastrophic reasons. At best the firms have business continuity plan for these nodes in case of hazards. This risk management approach, at best could be categorized as a silos approach, where the focus is only on hazard mitigation. In most cases firms can not be faulted for this approach, since coming up with a risk analysis methodology for supply-chains is not an easy task. There are various complications in doing so and a few are listed below.

- **Non-uniform criticality**: If different nodes have different business values assigned to them, a uniform method can not be used across the chain. This situation becomes more complicated in case of global supply chains. For example, consider that node N_1 in Figure 11 is a distribution center for a company, while node N_2 is the final test & assembly center (FTA). In this case sub-assembled parts come to node N_2, where the product is assembled and moved to node N_1. Node N_1 in this case acts as the main distribution center and therefore is the most critical node followed thereafter by node N_2 in terms of criticality factor. Therefore the risk analysis of the supply chain has to take into account this variation amongst nodes in terms of business value loss that could be caused because of the particular node disruption.

- **Sovereign risk:** In case of global supply chains, quite a few nodes in the supply chain could fall in different countries. Each of these countries could have a different sovereign risk with respect to currency, political stability and general business environment. It is fairly tough to come up with reasonable sovereign risk estimates and incorporate them in supply chain risk analysis. The financial world uses a sovereign beta (β_{sv}) to account for the sovereign risk in a foreign country. The sovereign beta approach is good for making capital investment decisions, but it doesn't help much in accounting sovereign risk to supply chain nodes in case of global supply chains.

Our *scm*ValueRisk methodology takes into account the above challenges and espouses a method that takes into account the uniqueness of each node. The *scm*ValueRisk© methodology doesn't apply same risk analysis to all nodes in the network, and treats each node different with respect to risk analysis.

On a very broad level our methodology calculates the value at risk (VaR) for each node and thereafter finds the expected monetary value loss of the complete supply chain. Estimating the expected monetary value loss for the entire supply chain is a tricky issue because the supply chain could be fail because of one or more, simultaneous failures at critical points. We use the *"Network Analysis by Critical Paths"* method that is explained shortly, to analyze the supply chain. Figure 11 shows a typical global supply chain that we will use to explain the *scm*ValueRisk methodology.

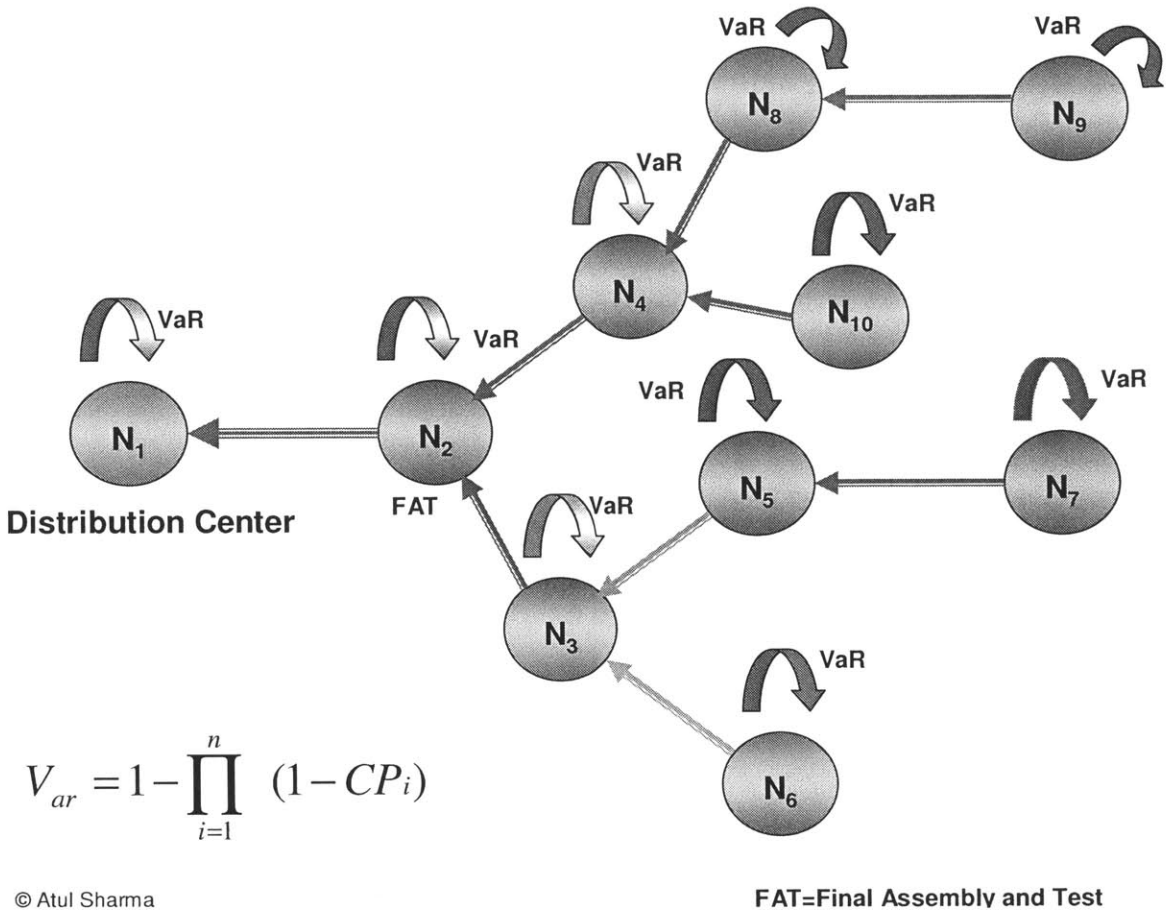


Figure 11: *scm*ValueRisk© Methodology

As a first step VaR is applied to each individual node of the supply chain. Note that we use an atypical definition of VaR in this case, compared to the traditional definition used in the financial world. The traditional definition and treatise of VaR is given in Appendix 10.1, but in our case we will modify VaR to include sovereign and other risks as well. To apply VaR to each node, that might be facing different sovereign risk and might have a different criticality index, we define a likelihood function that takes into account these varying factors into account. We define the likelihood function "L" as follows.

L = f (Criticality factor, sovereign risk, currency risk)

Or $L = f(C_f, S_r\ C_r)$

Now, if the business Impact value is denoted by "V", while "C_l" denotes the confidence level and "t" denotes the time interval of assessment, the VaR for a node N_i could be depicted as a function $N(V_{ar})$; where $N(V_{ar}) = G(L, V, C_l, t)$.

Once the $N(V_{ar})$ is applied to each node in the global supply chain, we get the value at risk of each node, but that's not sufficient enough to find the value at risk for the complete supply chain. The worst case loss of the whole chain is not the simple sum of worst case losses for each node. In fact to get the worst case loss scenarios we need to apply the cut-set theory of network analysis to the global supply chain. According to the cut set theory, the global supply chain will fail if one or more of the *"critical paths"* within the supply chain fail. The critical path is defined as the shortest path that if fails, brings down the whole supply chain down.

As an example, in the above supply chain if the connectivity between N_1 and N_2 fails, the supply chain fails. Therefore the $N_1 <> N_2$ connectivity is a critical path. To find out the value at risk of the whole supply chain, we find all possible cut sets, find their collective value at risks; and the collective value at risk of the whole chain would be an "OR" function applied to these cut sets. This relation could be mathematically shown as below.

$$V_{ar} = 1 - (1 - CP_1)(1 - CP_2)...(1 - CPz)$$

Where V_{ar} is the eventual value at risk of the global supply chain and C_{P1}, C_{P2},..., C_{Pz} are the possible cut sets that could fail the supply chain. Based on this V_{ar} the company could come up with a risk mitigation budget to mitigate the possible supply chain risk. The case study in Chapter 5 shows a detailed supply chain example, where this methodology is applied.

The above three examples of risk analysis methodologies for specific business functions show the application of 4-R (specifically the use of risk analysis) at four different types of boundaries. The boundary in this case is the specific business function in question. The increasingly complex business functions that we analyzed in the above sections could be used as models to come up with risk analysis methodologies for other business functions or the risks faced by the firm. In the next section, we see how the results of the 3T-4R framework analysis could be woven on a corporate level to come up with an ERM solution for the firm, using the Integrative Corporate Risk Management framework.

4.4 Integrative Corporate Risk Management Framework (ICRM©)

After covering the 3T-4R framework and a few business function specific risk analysis methodologies, that form the sub-systems of the ERM, it's pertinent to go into the details of ICRM. The ICRM is an integrative framework that combines together other ERM sub-systems and is shown in Figure 12.

ICRM combines the sub-system frameworks together in a disciplined manner to create the firm level risk management architecture or the ERM architecture. As discussed before, the 3T-4R framework provides enough flexibility to the firm to focus on the micro or the macro level of the risk. The usage of 3T-4R at the micro level i.e., at the business unit level could lead to risk management at different boundaries. The ICRM framework connects all these micro level risk management efforts together into a corporate level risk management framework; hence giving a corporate level risk management view to the top leadership.

The ICRM framework is based on uniform language, meaning & processes across the firm and provides the needed consistency across the board. As shown in Figure 12, ICRM has three main constituent blocks, which are explained below.

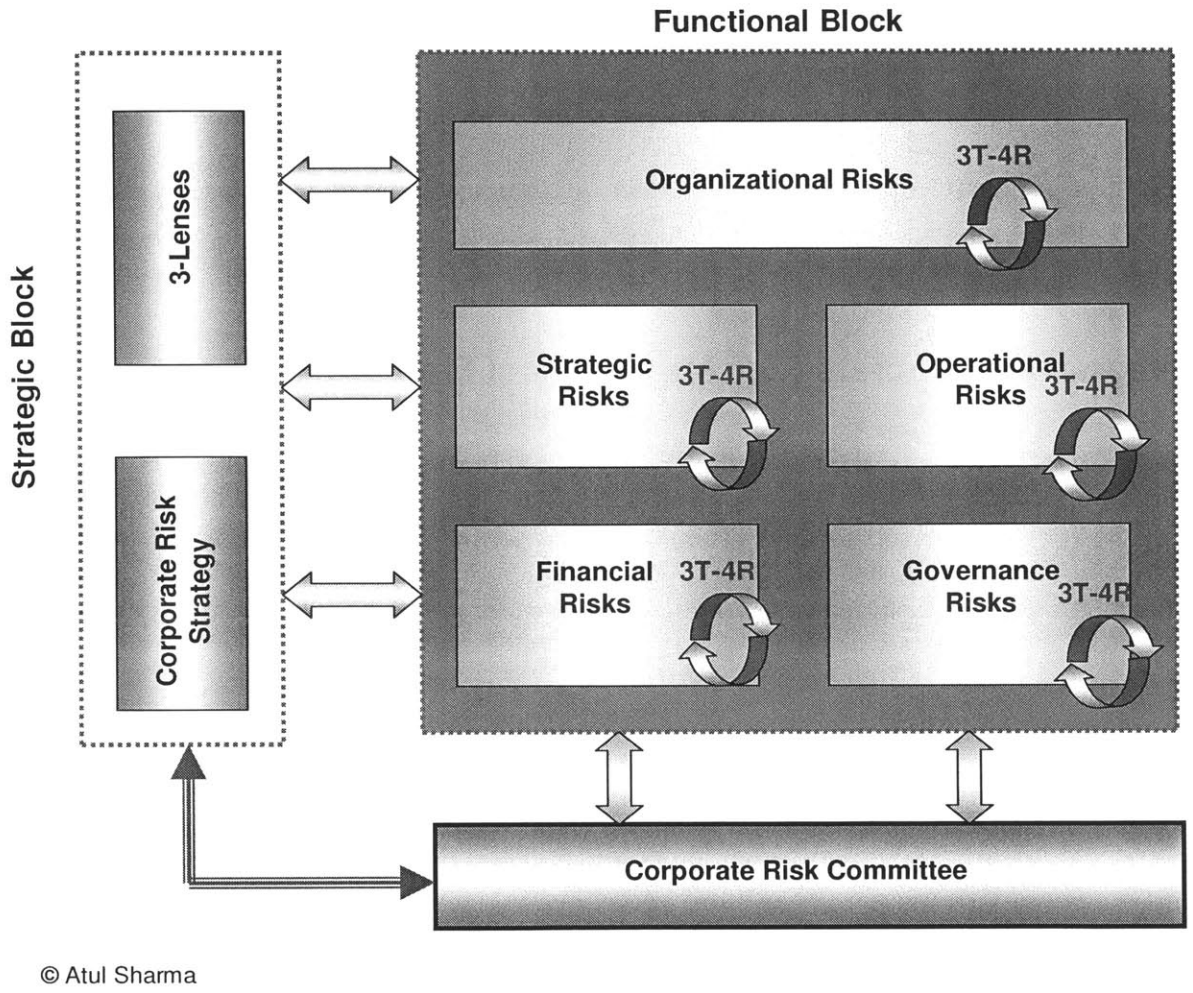


Figure 12: The ICRM Framework

Strategic Block: The strategic block signifies the process that is first and foremost required before delving into the functional and operational details of risk management. As has been discussed in Chapter 1; there is no one right approach towards risk management. Each firm has

to chart its own path based on its DNA and the way knowledge is shared amongst the stakeholders within the firm. Carlile's 3-Lenses can be used during this stage to do organizational analysis figure out the firm's DNA, culture and the right methodology to handle change management. The 3-Lenses framework helps figure out the kind of organization in place, and thereafter helps the firm chalk out the right approach towards undertaking risk management using the 3T-4R framework. Also, one of the phases in 3T-4R framework, risk monitoring requires firm wide processes to manage knowledge related to risk monitoring. It is in this context that Carlile's 3-T framework helps the firm find out the right way to handle novelties (or risks).

Corporate risk strategy is another important constituent of the strategic block. Without having a proper corporate risk strategy in place, the firm will not be able to pull together an enterprise level risk management practice. The key point here is the "strategy about risk" rather than relationship between "corporate strategy & risk". The key points to be considered at the corporate risk strategy stage are.

- Would the firm follow a top-down approach towards risk management or a bottoms-up approach?
- Whether to follow Risk Adjusted Return on Capital or Economic Capital as the way to look at risk at the corporate level?
- What are top risks at the firm level?

In a nut shell, the strategic block sets the direction of enterprise risk management and makes sure that the right strategy is followed based on organization culture and the way novelties would be treated within the firm.

Functional Block: Within the functional block "execution" is the key word. With a multitude of business functions, following the right risk analysis frameworks, finding the

right capital loss scenarios and putting together right risk mitigation and risk monitoring systems in place is crucial for the success of risk management within the firm. Within this block, the 3T-4R framework is recursively applied within each business function to unearth all possible risk trigger points and then put together corresponding risk mitigation and monitoring processes in place. Chapter 5 has a detailed case study where the 3T-4R framework is exhaustively used.

Corporate Risk Committee: The corporate risk committee is the corporate risk management watch dog. It interacts with the strategic block to make sure that the firm is identifying new threats and novelties, and their corresponding sources at the strategic level. Also, the committee has to make sure that business units are executing risk management in the most efficient manner by performing the following functions.

- Providing and ensuring an independent audit of the corporate risk strategy
- Ensuring that proper organization analysis and knowledge management mechanisms are in place at the corporate level
- Ensuring that each business unit is uncovering all risk trigger points corresponding to it's line of business
- Ensuring that proper risk analysis methodologies and frameworks are used by business units so that optimal capital risk exposure is calculated by the business functions. This avoids any games on part of business functions to show overly exposed or least exposed to risk.
- Ensuring that business functions have risk mitigation processes in place that correspond to their normal level of capital risk exposure

- Ensuring that uniform risk monitoring processes are in place across all business functions that could be seamlessly connected to the corporate risk processes or to the business performance management systems. This will make sure that the top management can get a consolidated view of aggregate risk to the firm.

4.5 Chapter Summary

This chapter introduced the frameworks and methodologies that form the core of our work, and that could be used to achieve true holistic risk management in the firm. The chapter started with the introduction of risk management maturity model' a model that could be used by a firm to assess its position on the risk management curve and devise an appropriate risk management strategy.

Subsequently, the 3T-4R framework was introduced, that could be used at the business function level or the firm level to do risk management. The biggest challenge faced by firms is doing the right risk exposure analysis; the second step in the 3T-4R framework. A few methodologies were introduced that could do the appropriate risk analysis for some of the most popular business functions viz., M&A, Supply chain management, Information security etc.

Finally, the ICRM framework was discussed, the parent framework, in which the other frameworks and methodologies introduced in the chapter get architected. The next chapter presents a detailed case study of a typical high-tech firm to achieve holistic risk management using 3T-4R and ICRM.

5 CASE STUDY

This chapter presents a case study on the risk management process for a typical large high-tech firm. Risk management being a highly sensitive topic for most firms, the intent of this chapter is not to dwell on the risks of any particular firm – but understand the application of our frameworks in a high-tech environment. The case study will take a top-down approach in risk management, starting with a firm level analysis using 3T-4R and then tackling a few business functions in detail.

5.1 Disclaimer

The risk management case study presented here does not focus on any particular company, but it could be applied to any large or small high-tech organization. Of course, a large organization will face very different risks than a small organization; but the 3T-4R framework is generic enough to unearth and manage the risks for both the organizations.

Note that out of the four risk management stages, the second stage – risk analysis stage is heavily dependent on the type of industry and the size of the firm. This is so because the size and type of industry defines the risk impact that could be faced by the firm. For example – the supply chain impact in case of Nortel is definitely higher than the impact in the case of a communication start up in Silicon Valley.

Therefore, to keep our discussion within bounds the frameworks will be applied to a typical large firm in the communications industry. Also, some discussion might not hold true for large software firms that have different supply-chain and emerging technology analysis requirements. Large software firms have diminished supply-chain and manufacturing costs

involved because of the nature of their products; therefore some of the risk analysis methodologies need to be tailored to their business practices, before being used as such.

5.2 Risk Management Maturity Identification

The first step before embarking on the risk management process is to find out where the firm belongs on the risk management maturity curve. The position of a company on the risk management curve provides a road map about the future risk management direction of the company.

Based on public information, it appears that companies like Nortel, Cisco, Juniper, Lucent etc., do have hazard mitigation and financial risk management in place. This would put most of these companies in the curve region inhabited by yellow dots; signifying that these companies have somewhat achieved the partial integration and alignment. Nevertheless, the annual reports and other public data don't provide any data to ascertain with confidence, if these companies have achieved full integration towards enterprise risk management. It is assumed that most of them must be working towards a full integration.

The following paragraphs discuss how the frameworks discussed in Chapter 4, could allow a company of similar size and scope to achieve full integration over a period of time.

5.3 Risk Identification

After a company has identified its position on the risk management curve and identified its goals, it needs to apply the first step of 3T-4R process; the risk identification stage. Although a company could adopt a top-down or bottoms-up approach based on what it seems fit for its needs, we follow a top-down approach, starting from the firm level, in the risk identification stage.

5.3.1 Firm Level Risks

At the firm level, the scope of the risks is all inclusive; i.e., the firm should focus on internal as well as external risks. An internal risk is the risk associated with the operations of the company, while and external risk is classified as a risk originating because of market and business conditions. The former risks could be classified as operational risks, while the latter ones as strategic risks.

To keep a disciplined approach, this stage should focus on identifying only top four or five risks that are mutually exclusive but collectively exhaustive in terms of covering all internal and external risks. Figure 13 in the tree form shows the top level risks that the firm could be facing. Since 3T-4R follows a recursive risk identification strategy; a tree form of risks is intuitive to understand the various risks.

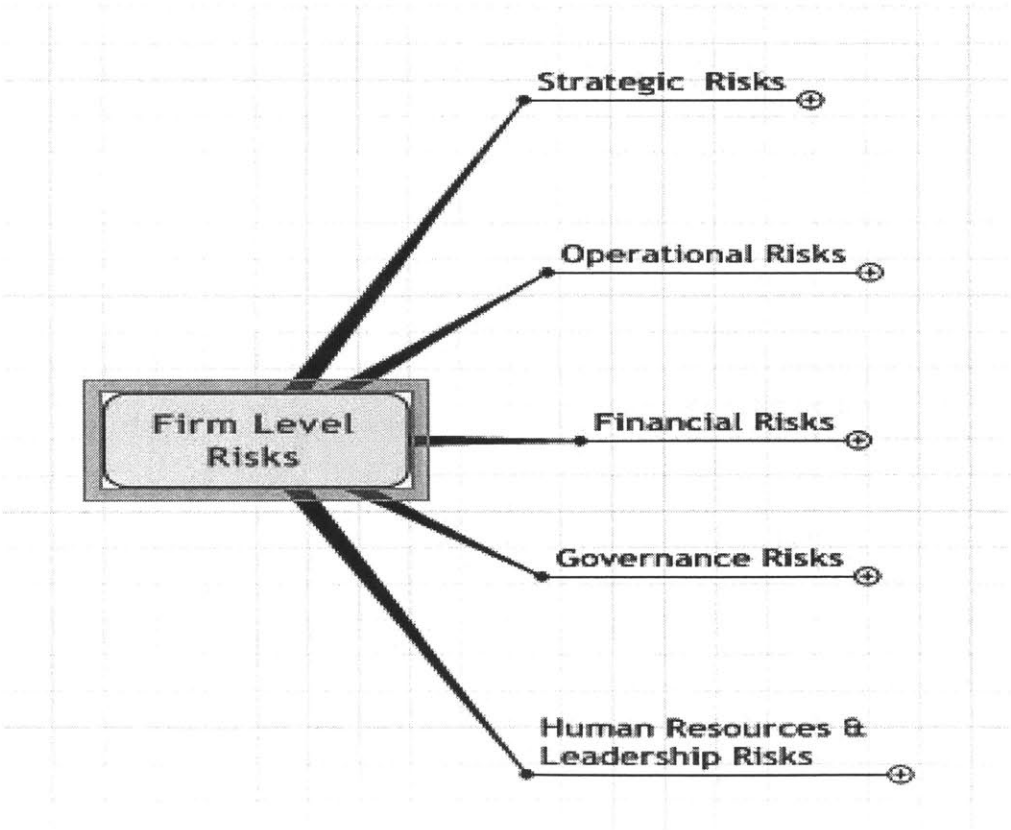


Figure 13: Level 1 risks of a firm

As evident from Figure 13; the major level one risks faced by the firm are strategic, operational, financial, governance and human resources & leadership risks. In the next step of the recursive risk-identification process, each branch of the tree is traversed and the level two risks are identified.

Figure 14 shows the level two view of the risks faced by a typical firm. For example, in the strategic risks category, the major risks that a firm faces are brand, reputation, competition, technology strategy, customer defection, emerging technologies and mergers & acquisitions. Similarly in the human resources & leadership risks category, the major risks that a firm could face are talent turnover, employee morale, post-M&A integration and succession planning risks etc.

It's been observed that the second level of risk identification gives detailed information to a firm in terms of micro and macro risks. The corporate risk committee, at this point could act as a think tank to coordinate with the risk owners of level one risks and help them in organizing their risk efforts for level two risk management process. The level two risks are thereafter assigned to operational managers within the business units.

At the level two risks there is a greater possibility of witnessing different boundaries and objects. This translates into having different risk analysis and mitigation methodologies. One of the biggest challenge that firms face is creating a common language, syntax and processes for managing these level two risks. Unless a common language and syntax is not created to handle the level two risks, the firm would face challenges integrating risk management plans in a bottoms-up fashion.

Note that the level two risks could be more exhaustive than the ones shown in Figure 14, but the risks shown below represent a typical firm scenario.

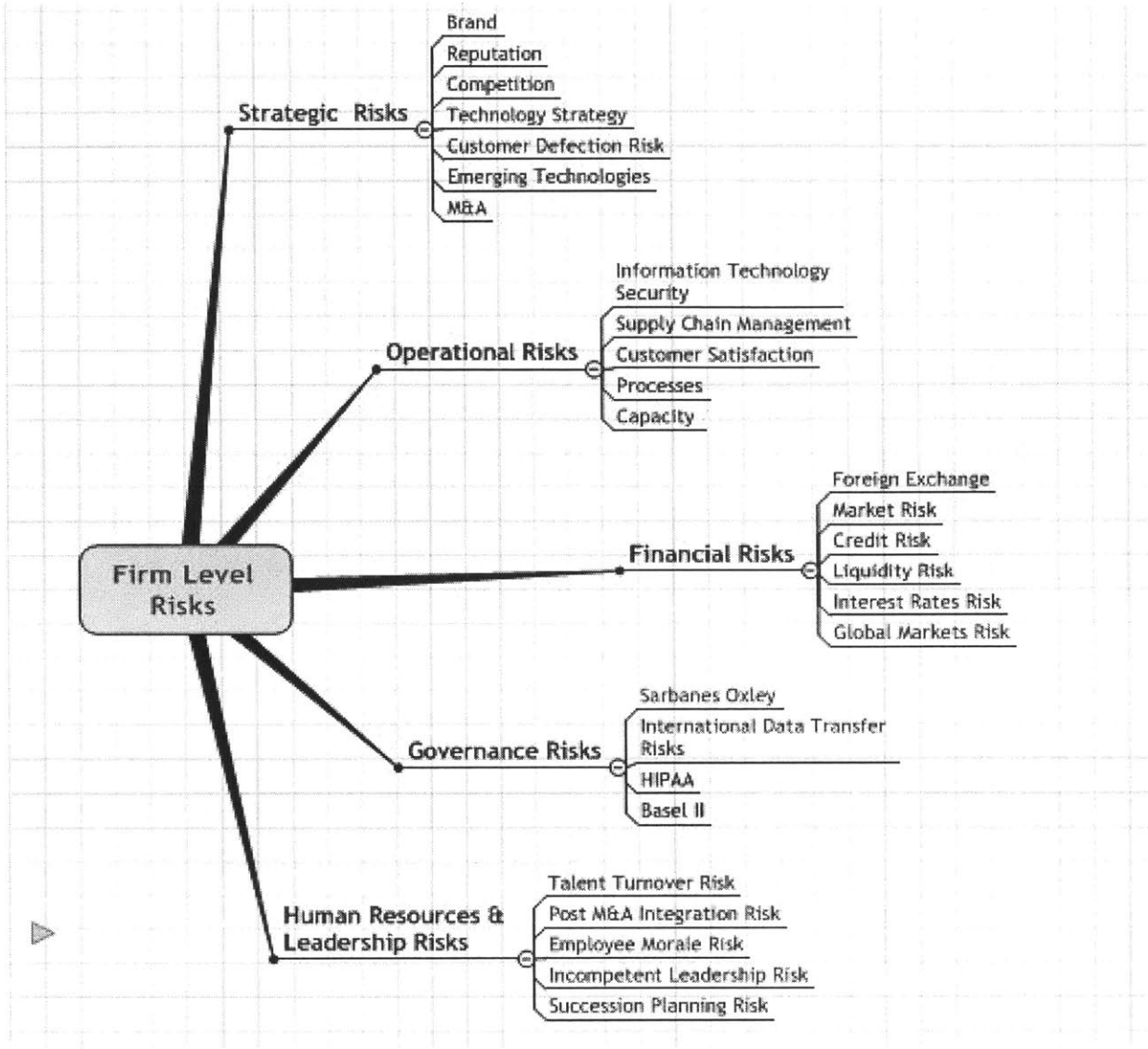


Figure 14: Level 2 Risk Identification for a typical firm

It is outside the scope of this work to apply recursive risk identification technique to all the sub-branches of the risk-tree, but the following paragraphs cover in detail the risks for a few business functions that are of critical importance. Later, we apply the complete 3T-4R framework to one particular business function; supply chain management.

5.3.2 Competition

The rate of competition is a primary driver of novelty or risk; in fact the amount of competition is correlated with the amount of novelty in the system. Being taken over by the competitors is perhaps one of the biggest risks faced by a firm. Figure 15 depicts the various risk indicators that could be tracked for the competitor, so as to analyze the business health of the competitor and assess the overall risk from the competitor. In other words these indicators could be considered as key boundaries to be monitored.

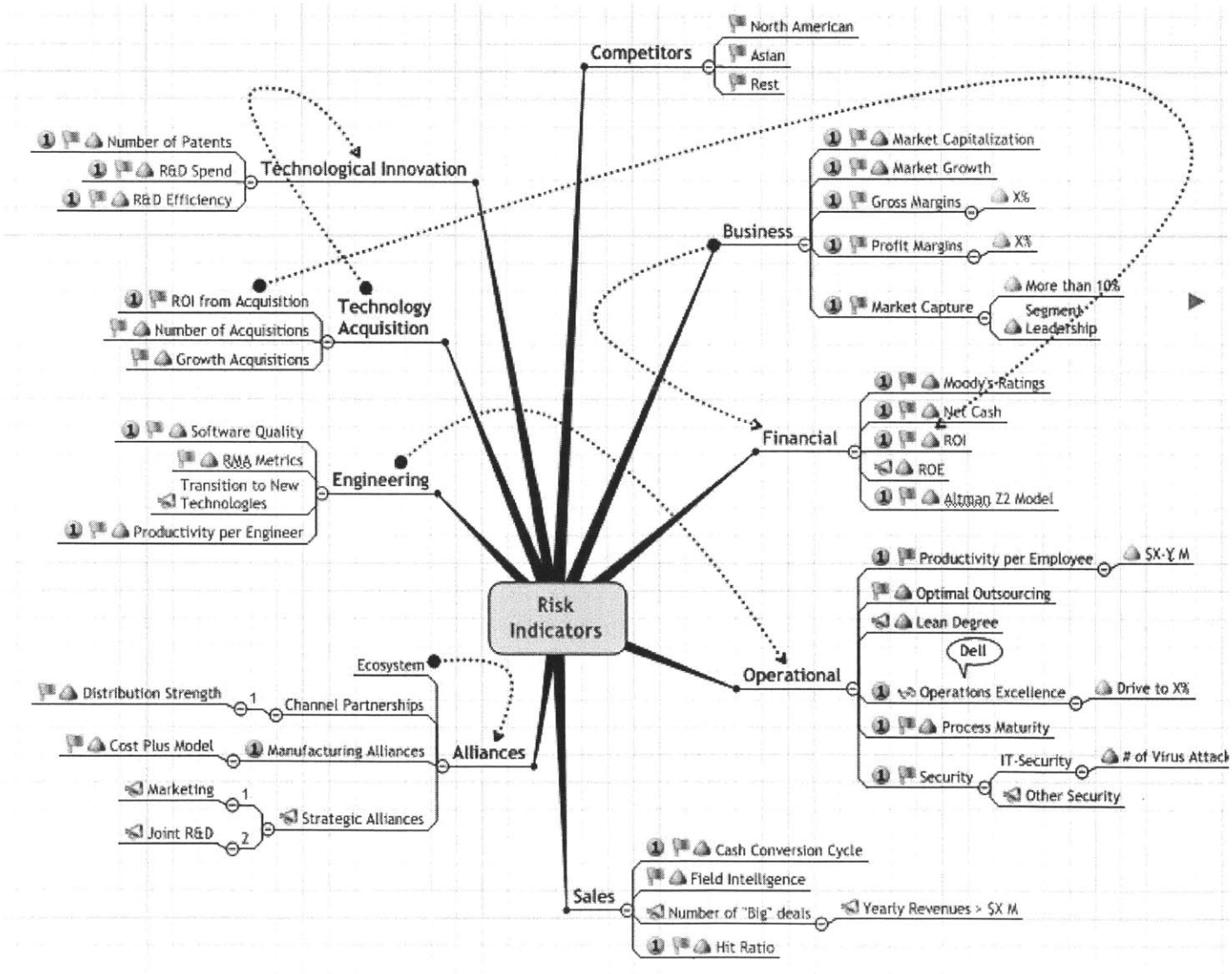


Figure 15: Risk Indicators for Competitors

As an example to assess the technology acquisition related indicators the firm could look at the respective ROI from each acquisition, the total number of acquisitions done by the competitor and the number of growth[3] acquisitions done by the competitor. These metrics could then be compared with the corresponding metrics of the firm to find out the relative risk of the firm vis-à-vis the competitor in the area of technology innovation.

Consider another example - the case of business alliances; an important metric to asses the growing power and importance of a competitor. In the area of alliances, the recursive risk identification technique would list channel partnerships, manufacturing alliances and strategic alliances. For each of them the recursive risk identification technique would yield relevant risk indicators. For example- in the area of strategic alliances there could be marketing alliances of joint R&D alliances. Once these metrics are identified and quantified, the firm could use a weighted indicator analysis to find out the degree of risk posed by the alliances of the competitor. Note that, the risk identification process only identifies the risk, but to unearth the business loss potential because of these alliances, a relevant risk analysis framework needs to be used through the risk analysis phase of 3T-4R framework.

5.3.3 Technology Strategy & Innovation

For a high-tech firm, apart from competition, technology strategy & innovation is another area which requires extensive risk management. The future leadership of a firm could be dependent on two facts; one – how efficiently is the firm managing its technology and innovation risks, and two – how the firm has been performing years over year in this area. Figure 16 shows a detailed tree of various risk indicators that could be tracked and later analyzed to gain more insight into the above two facts.

---

[3] Acquisitions targeted to increase the top line growth of a company

For example – the technological innovation branch shows indicators like number of patents, location of firm's technologies on the S-Curve, R&D spend, R&D efficiency etc. By tracking these indicators, and combing the related indicators into one group, the firm could gain insight about a major risk factor. A risk analysis of this risk group could tell the company about the potential capital loss risk, and finally by having risk mitigation and risk monitoring plans around these risks, the firm could mitigate and monitor these risks.

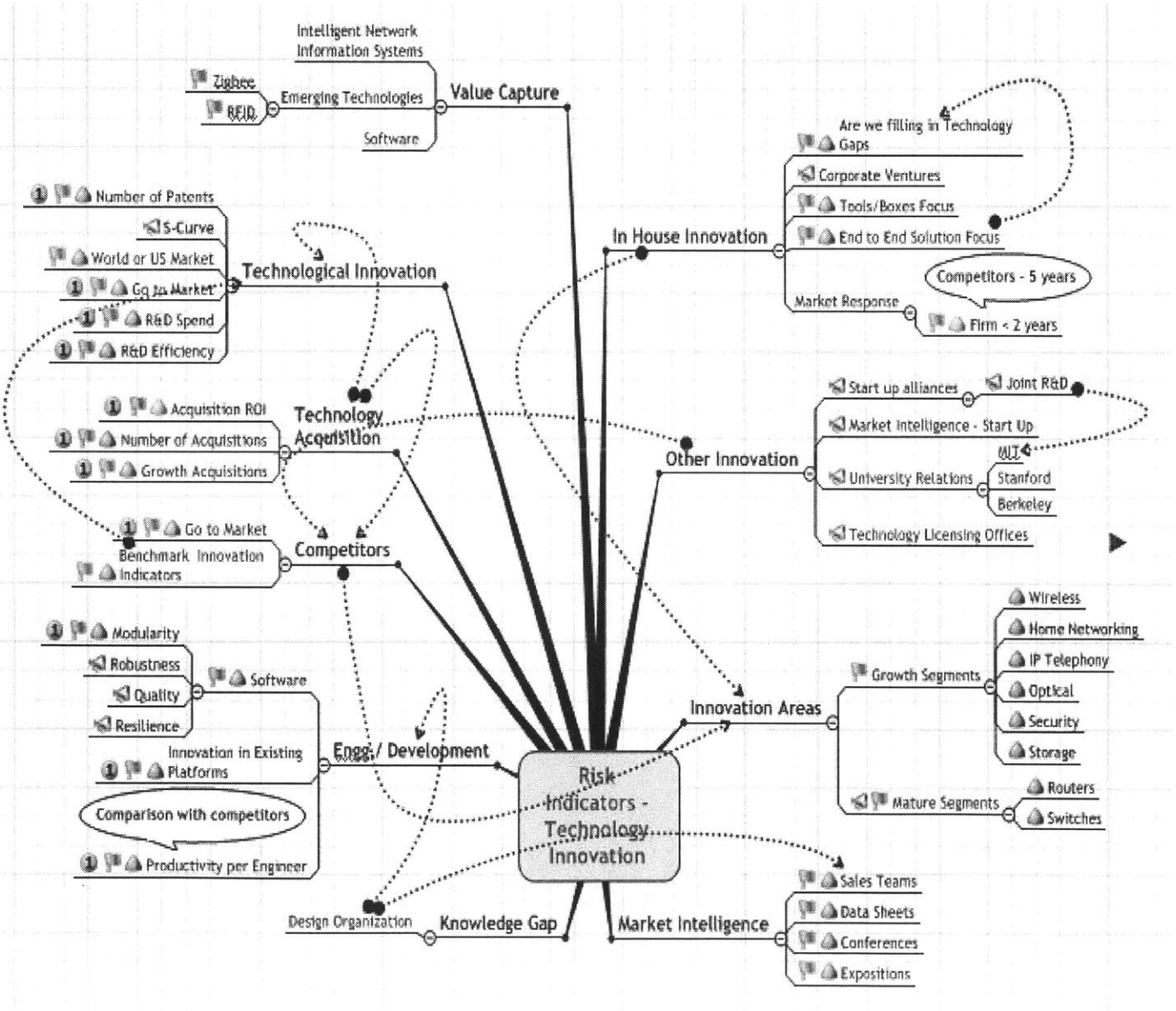


Figure 16: Risk Identification Indicators for Technology Strategy & Innovation

Also, a year over year analysis of these indicators and comparison of capital risk figures could tell if the firm is doing a good job at identifying, mitigating and monitoring its risks or not. The next section treats the risks in the Information Technology Catastrophe category.

5.3.4 Information Technology Catastrophe

During the 9/11 catastrophe, apart from valuable lives a lot of companies who had offices in the trade towers, lost their IT infrastructure and therefore were not able to conduct their businesses. Subsequently, companies started taking renewed interest in IT Catastrophe risk management. Figure 17 depicts the risk tree for IT Catastrophe.

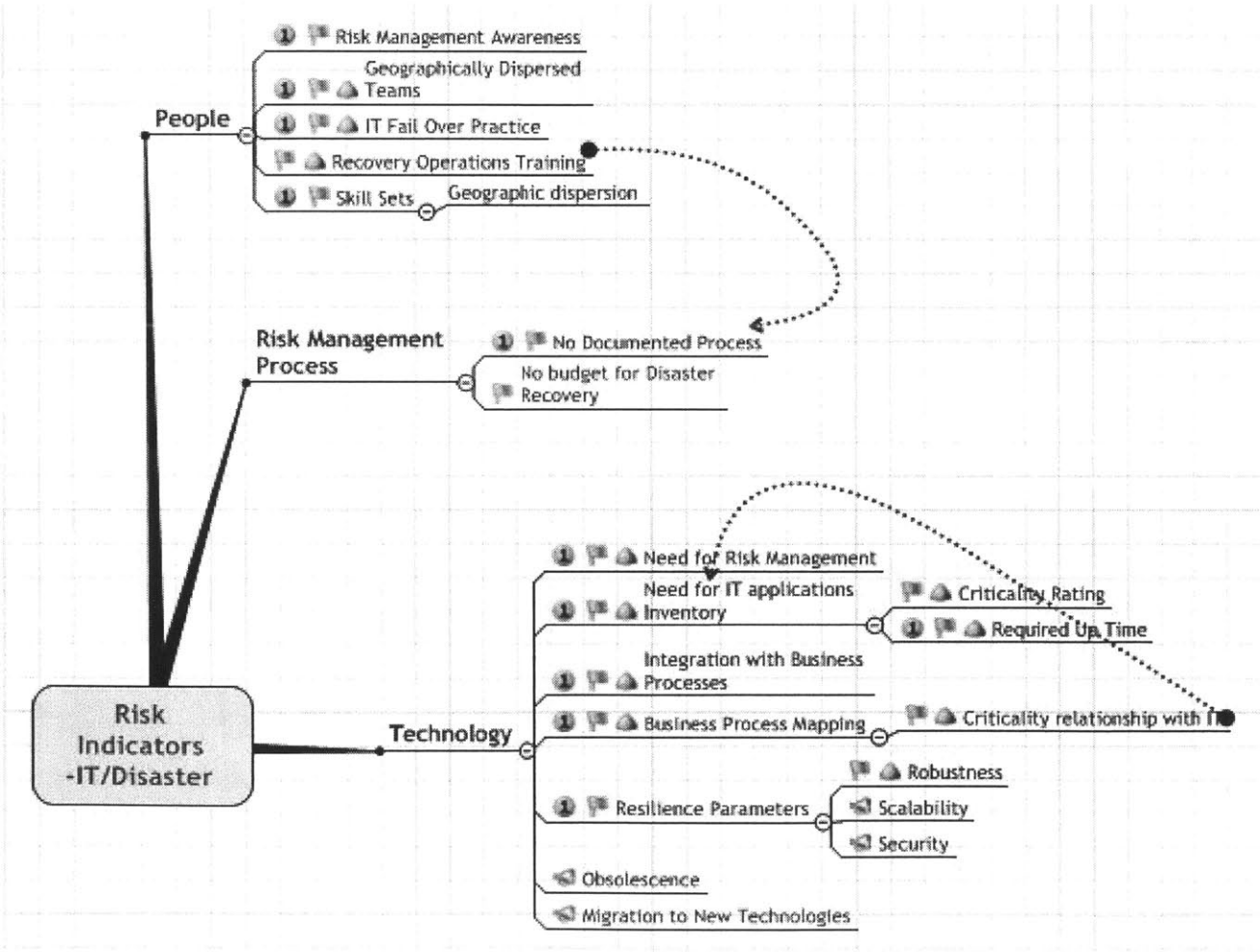


Figure 17: IT Catastrophe

According to the recursive risk identification stage of the 3T-4R framework, the overall risk associated with IT Catastrophe can be linked to risks related to people, processes and technology. Within the people category, the firm needs to track indicators like level of risk management awareness, recovery operations practice, geographical dispersion of teams etc.

On the technology front the firm needs to track indicators related to alignment with business processes, IT applications inventory etc. The application inventory needs to track the average up & down time of applications; apart from the time required to up these applications on an enterprise level in case of a disaster. In terms of processes the firm needs to track its risk processes that collect the risk metrics and perform the risk monitoring function. Also, the firm needs to track the alignment factor between the risk processes and the business processes.

Cumulative assessment of these indicators for people, process and technology will give a complete risk identification picture to the IT department of the firm, who can thereafter use risk analysis frameworks to assess capital loss relationships with the pertinent risks. The following section covers the risk metrics related to customer satisfaction and quality metrics.

5.3.5 Customer Satisfaction and Quality

Customer satisfaction and quality has increasingly become a major risk factor for most high-tech firms. This risk is more evident in commoditized hardware market, where price and support level are the major ingredients of the competitive advantage.

A decline in the customer satisfaction benchmarks because of quality issues are two risks that are heavily inter-connected. A risk in quality management can trigger a corresponding risk in customer satisfaction. Therefore these two risks are shown together in Figure 18 and try to do a collective risk identification process for both.

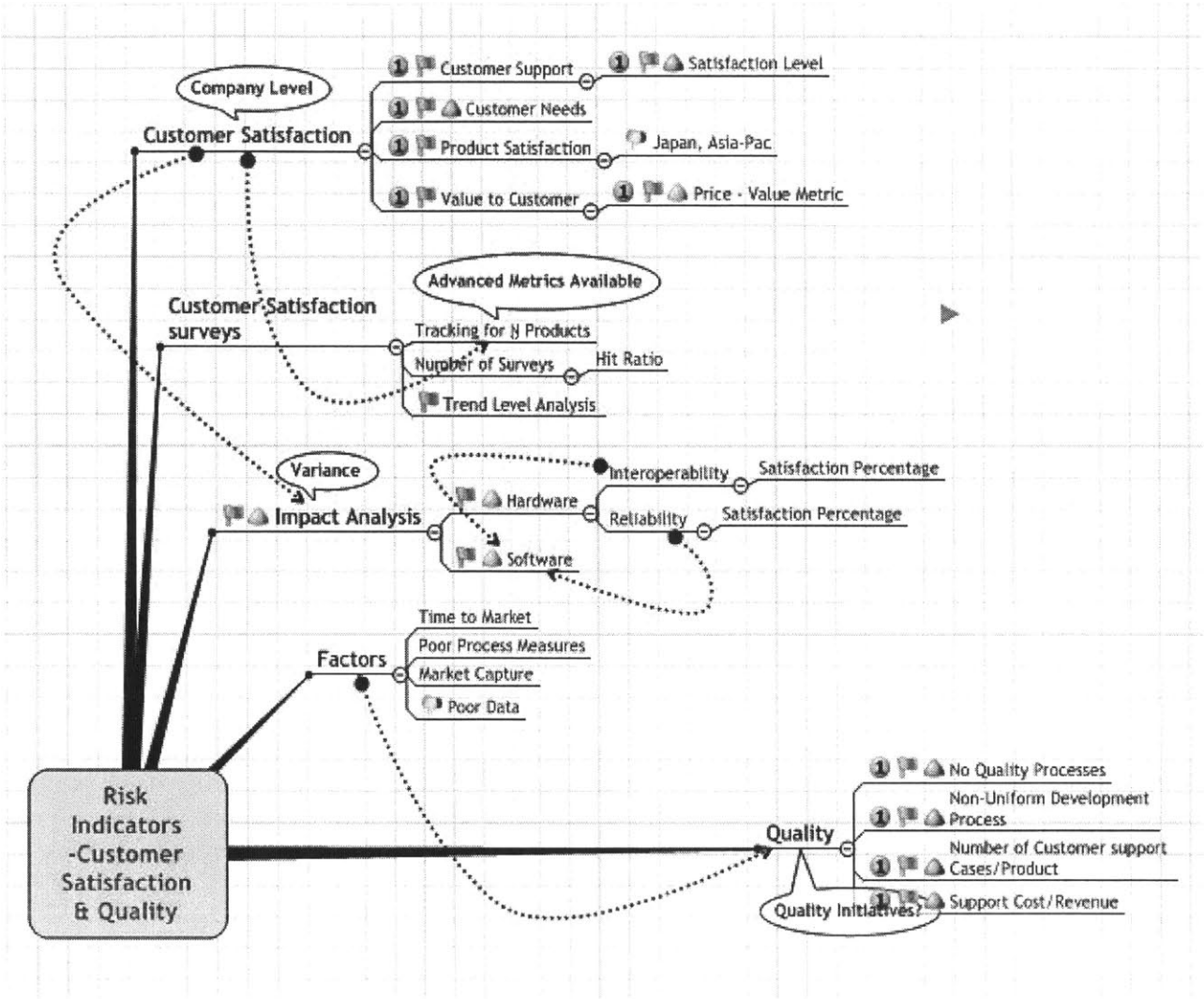


Figure 18: Customer Satisfaction and Quality

In the case of quality, some of the risk indicators worth tracking are degree of alignment of quality and business processes, number of customer support cases and the ratio of support cost to revenue generated by a product or a product line.

In the area of customer satisfaction some interesting indicators would be related to product satisfaction and value to customer metrics. In the case of hardware the indicators related to interoperability and reliability could be tied to customer satisfaction metrics. Bundling the

relevant indicators together, would form a risk group and subsequently the risk analysis, risk mitigation and risk monitoring phases could be applied to customer satisfaction and quality.

After applying the recursive risk identification for a few important business functions, we apply all the steps of the 3T-4R framework for supply chain management; one of the most critical operational element for firms.

5.4 Supply Chain Management: 4-R Application

In this section we do a complete 3T-4R analysis of supply chain management. This application of supply chain management will give readers a holistic idea about applying 3T-4R to a business function and then tying it to the corporate risk framework. Readers could use the same approach to apply 3T-4R to other business functions to perform risk management. Finally, these sub-system risk management solutions could be tied together using the ICRM framework to get ERM architecture at the corporate level.

5.4.1 Risk Identification

Figure 19 depicts the risk tree for supply chain management function within a typical high-tech firm. For the sake of simplicity, the first level risk analysis could be broken down into three categories; disruption, inventory level management and miscellaneous.

The disruption factor could be caused because of terrorism, sovereign risk, vendor's business health or force majeure. The business health of a vendor could be put in danger because of sudden bankruptcy. Similarly, force majeure could be caused because of natural disasters.

In inventory level management, the major indicators would be extremely high or low levels of inventory, poor forecasting etc. Similarly, the miscellaneous category reasons could

include single source procurement, vendors in politically risky countries, foreign exchange fluctuations and currency environment changes etc.

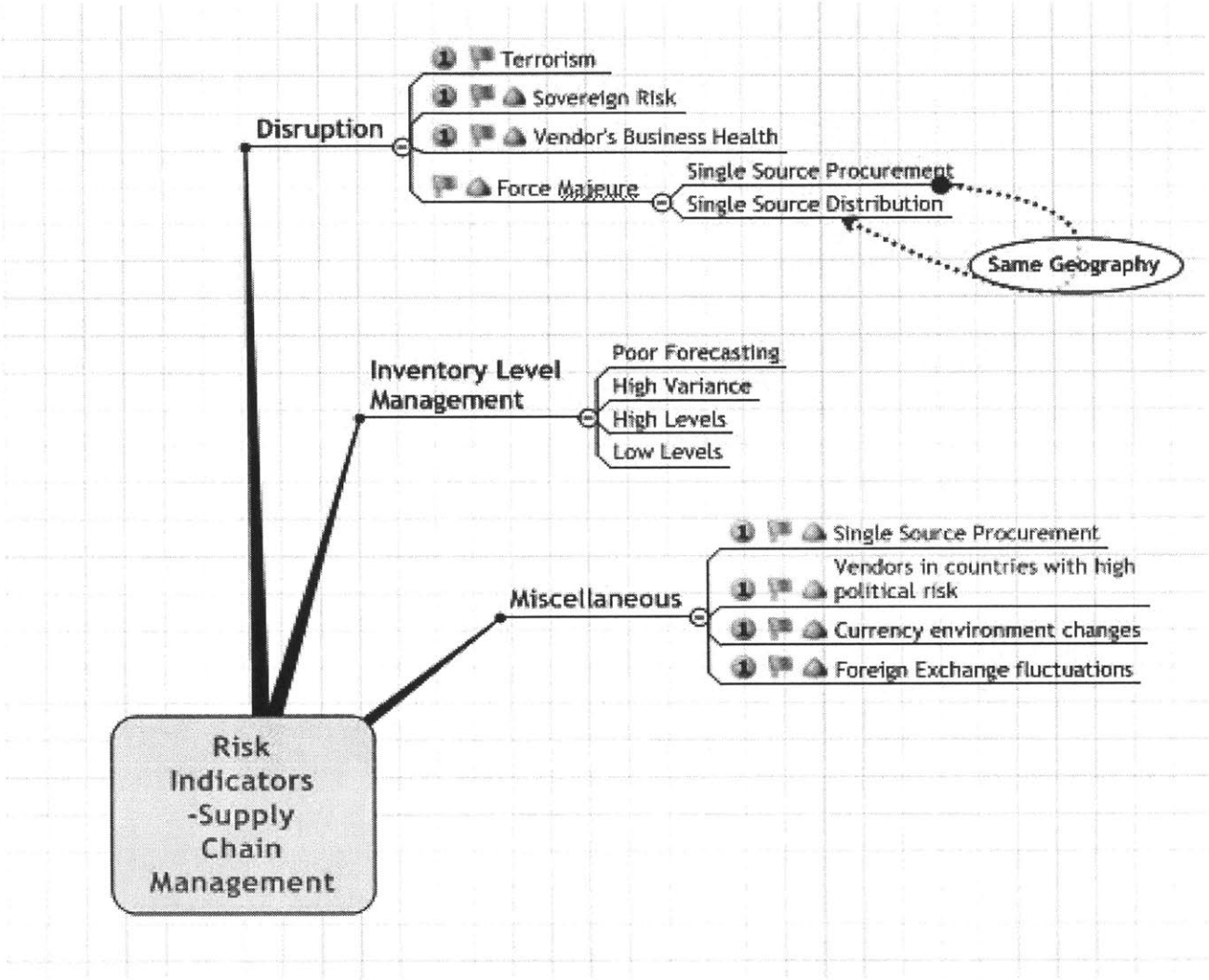


Figure 19: Supply Chain Management Risk Indicators

For the purpose of doing risk analysis, let's assume a force majeure situation, in which one or supply chain nodes could stop functioning, hence disrupting the total supply chain. In the risk analysis section we will allocate dollar value to each node based on the possible "business impact" value that the disruption of that particular node could cause. We will use value at risk (VaR) to determine the capital loss value for each node and use expected monetary value loss to

find out the loss because of the whole supply chain. The risk analysis part is covered in the next section.

5.4.2 Risk Analysis

Consider a simple global supply chain having five nodes in different countries. Node N_1 is a distribution center in Texas, while node N_2 is a final assembly and test site in Mexico. These two are the most critical nodes in the supply chain in terms of assembly and distribution. The other nodes are categorized as assembly phase I and single source procurement nodes, as shown below in figure 20.

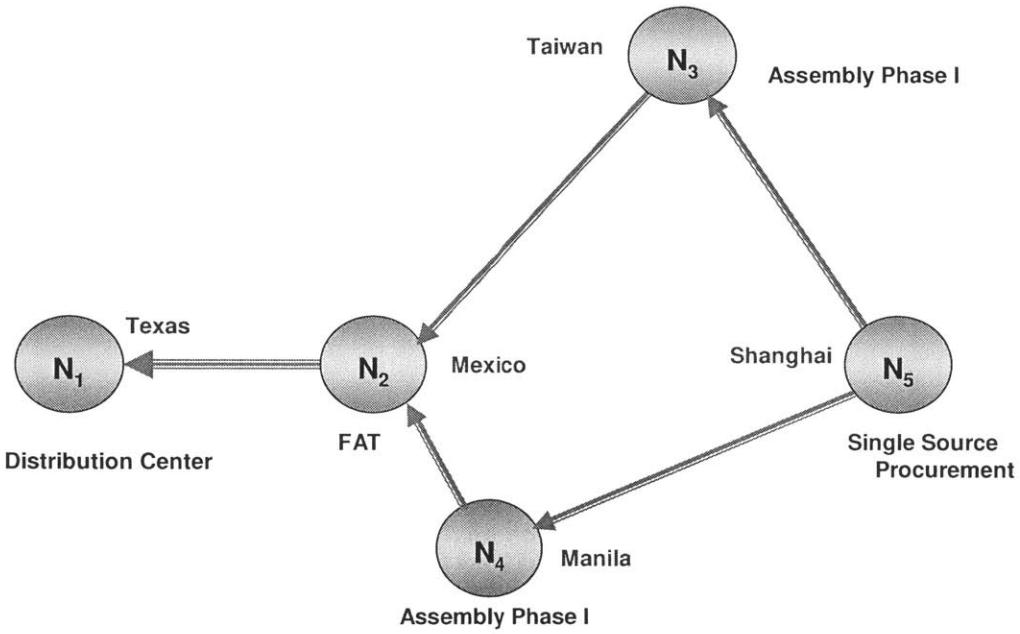


Figure 20: Supply Chain

The first step is to calculate the value at risk for each node. To calculate the value at risk associated with each node, we need to find out the approximate likelihood function that will mirror the likelihood of loss at a certain node. The likelihood function is heavily dependent on the criticality of a particular node. Considering that distribution, final assembly and single source procurement have the most criticality in the supply chain, we assign the following criticality factors to the various nodes of the supply chain.

Node	Type of Node	Criticality Factor
1	Distribution Center	High
2	FAT	High
3	Assembly Phase I	Low
4	Assembly Phase I	Low
5	Single Source Procurement	High

Table 1: Criticality factors of the nodes

Note that, node number one is a distribution center for the company, therefore if it goes down, the product distribution halts. Therefore this node is assigned a criticality factor of "high" in the supply chain. Similarly, there is only one final assembly and test site (node number two), therefore it's been assigned a "high" criticality factor as well, because if this node goes down the final assembly will stop. Node number three and number four have been assigned a "low" criticality factor because they are both same level nodes in terms of first phase assembly and even if one node goes down – the second can take over. Finally, node number five is assigned a "high" criticality factor, because it's a single source supplier and if it stops supplying for any reason, the supply chain is in problem.

After assigning the criticality factors to each node of the supply chain, the next step is to figure out the sovereign and currency risk for each node, based on the country in which it is located. The sovereign risk is defined as the general risk of doing business in a country. The Economist Intelligence Unit reports could be used to determine these risk factors and their relative scale. The currency risk is the high variance risk of the currency of a country with respect to the basket of major global currencies, as tracked by S&P or Moody's. Table 2 shows the relative sovereign and currency risks for the five nodes and the corresponding countries. Note that China has a low currency risk despite high sovereign risk because of its fixed peg to US dollar.

Node Number	Country	Sovereign Risk	Currency Risk
1	US	Low	Low
2	Mexico	Medium	High
3	Taiwan	Low	Medium
4	Philippines	Medium	High
5	China	High	Low

Table 2: Sovereign and Currency Risks

After finding the various constituents of the likelihood factor, the loss likelihood results are calculated. The following table shows the consolidated loss likelihood results for the five nodes. For simplicity of calculation, a high critically factor is diluted by a low factor and leads to a medium risk. A high multiplied by high gives a high critically factor and low multiplied by a low yields a low criticality factor.

Node Number	Country	Loss Likelihood Result
1	US	Medium
2	Mexico	High
3	Taiwan	Medium-Low
4	Philippines	Medium-Low
5	China	Medium

Table 3: Loss likelihood result

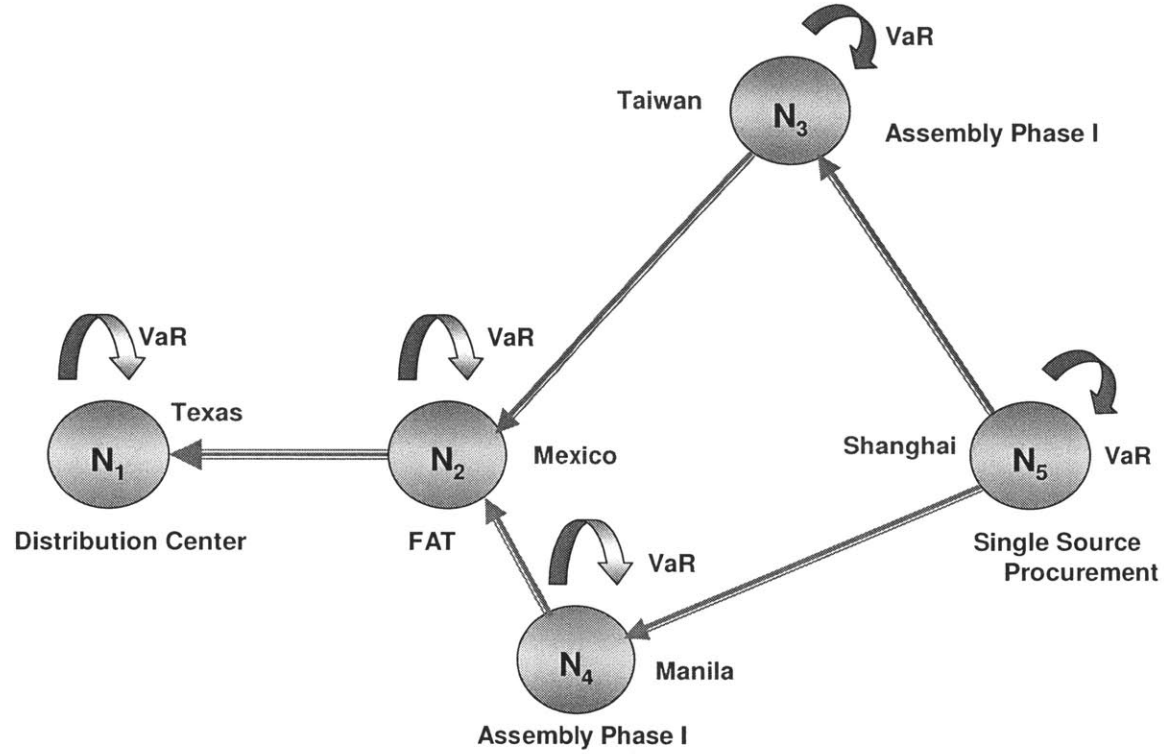
The next step is to calculate the worst possible loss per day per node in the chain. Assume that the following table depicts the loss to supply chain corresponding to each node. Note that the distribution center will have the highest loss and first phase assembly plants will have the lowest. The following table gives a fictitious loss scenario for various nodes.

Node Number	Country	Dollar Loss per day ($M) (corresponding to node disruption)
1	US	$100M
2	Mexico	$80M
3	Taiwan	$50M
4	Philippines	$50M
5	China	$30M

Table 4: Dollar loss per day per node

The next step would be to find the critical paths in the network shown in Figure 20. The critical paths methodology was touched upon in the supply chain methodology that was

explained in section 4.3.3. Figure 21 shows the equation for critical paths, along with VaR being applied to each node.



$$V_{ar} = 1 - \prod_{i=1}^{n} (1 - CP_i)$$

FAT=Final Assembly and Test

Figure 21: Supply Chain Risk Analysis

For the given supply chain network, the critical paths would be: $\{N_1\}$, $\{N_2\}$, $\{N_3 <> N_4\}$ and $\{N_5\}$. These four cut sets are the most sensitive sub-networks, which if disrupted could bring down the entire supply chain down. For each of these critical paths, the total dollar loss value would be a summation of dollar loss for each node that is a part of chain. Figure 21 shows that Value at Risk (VaR) is applied to each node and the value at risk for the whole chain could be denoted by the "OR" function that sums the various critical paths of the supply chain. Note that

in a typical critical path analysis, the focus is only to get the cut sets, but in our case we replace each critical path link by the value at risk dollar loss figure, to find out the total loss that could happen because of the disruption caused by one of these critical paths.

Finally, Table 5 gives a consolidated dollar loss calculation along with the loss likelihood factor for each. Note that the consolidated likelihood function in case of two nodes going down at the same time is the product of their likelihood functions. According to the following table the critical path that corresponds to the disruption of node N_1 has a final likelihood of "medium" based on the likelihood consolidation from criticality factor of the node, sovereign risk of the country in which the node is present and the currency risk of the country.

Critical Paths	Dollar Loss ($M)	Consolidated Likelihood	Final Likelihood
N_1	$100M	Medium	Medium
N_2	$80M	High	High
N_3<>N_4	$50+$50	(Medium-Low) * (Medium-Low)	Low
N_5	$30	Medium	Medium

Table 5: Critical paths, dollar losses & likelihood scenarios

From table 5, the following inferences could be drawn.

- The firm faces a best case risk scenario of medium risk amounting $30M
- The firm faces a worst case risk scenario of $310M, with a very low risk. This is if all likelihoods are multiplied and all critical path losses happen at the same time.
- The firm faces $80M of high risk loss because of node N_2

The analysis done in the above section is a fairly rudimentary analysis, but after doing detailed scenario analysis and fine tuning the likelihood function and the value at risk losses, the firm would know the amount of losses it can face and their likelihoods over a period of time. The goal of this section was to provide a road map to firms to tie rigorous analytical methodology in their risk analysis calculations.

5.4.3 Risk Mitigation

In the risk mitigation phase, the firm would put in place processes and solutions that would mitigate the above risks while investing a reasonable amount of capital. The mitigation plan is shown in figure 22.

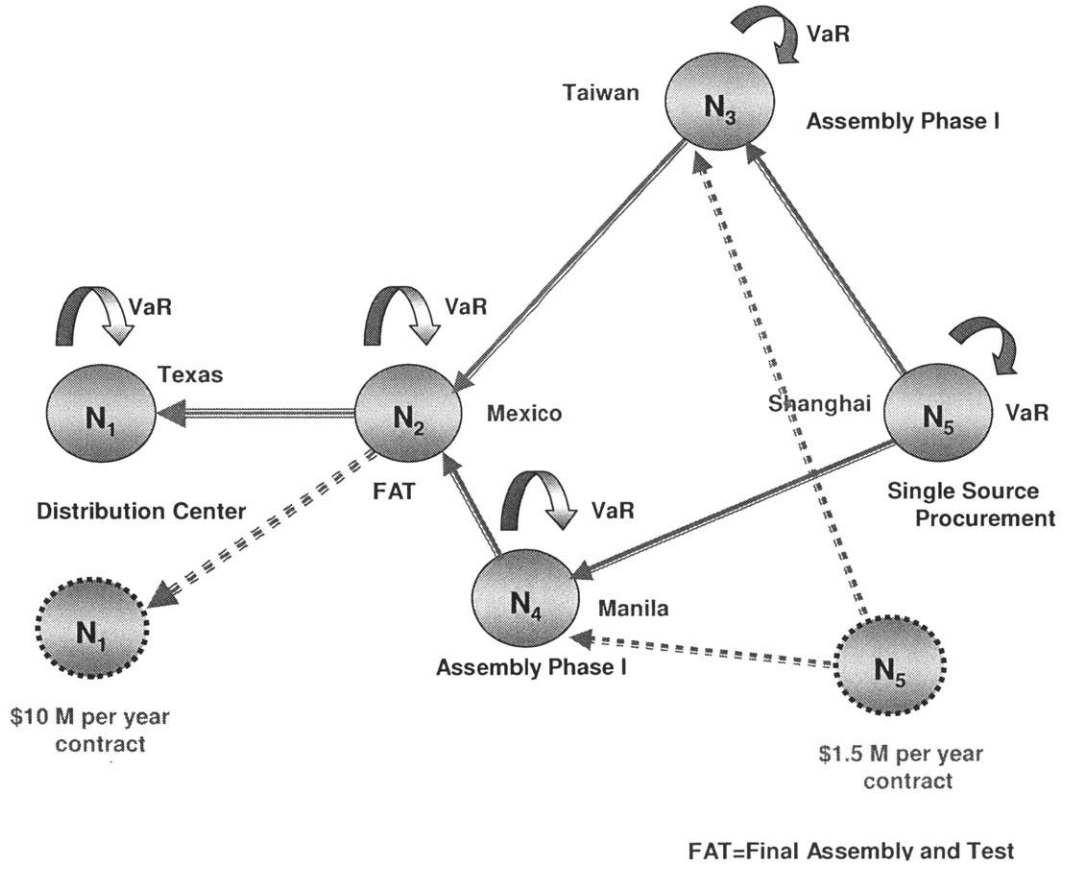


Figure 22: Risk Mitigation plan

Assume that the company is willing to invest 10% of the worst case loss scenario per day for mitigation[4] for high risk nodes and up to 5% for medium risk nodes. This would mean that the company will be willing to spend $10M for node N_1 and $1.5M for node N_5. Figure 22 shows that the mitigation could be achieved by having emergency contracts nodes in place for node N_1 and N_5.

The nodes N_1 and N_5 in the dotted circles represent mitigation contracts with other vendors and the corresponding costs of $10M and $1.5M per year are the mitigation costs that the firm could reasonably spend to mitigate these costs. Note that the above risk analysis and risk mitigation approach ascertains the importance of 3T-4R process. Risk management at the micro or macro level requires a thorough understanding of the dormant risk trigger points. Once these risk trigger points are completely understood and if the risks are deemed consequential then changes and transformation is required. Also, the pragmatic capacity requires running different scenarios about the changes that could be most beneficial to mitigate the risk, with a certain upper limit assigned to mitigation budget. In a nutshell, the key is making changes to mitigate the risk.

5.4.4 Risk Monitoring

In the risk monitoring process, the firm needs to put in place monitoring processes that would collect data about likelihood function factors and update the likelihood and loss calculations per quarter or year, based on firm's decision.

Based on these calculations and data from these processes, the risk pertaining to each node and the supply chain as a whole would be tracked. Also, these processes could feed into a

[4] Mitigation investment per year, assuming that worst case likelihood happens once per year

corporate risk process network, where they will feed information into the bigger risk picture that the corporate office could see.

5.4.5 Integration with ICRM

After the 3T-4R process is applied to the supply chain management function, the risk analysis, mitigation and monitoring processes are integrated into the ICRM framework. From a systems architecting point, this is akin to architecting a module, making it work and then integrating it into the super-system.

The corporate level risk processes are the super processes into which the risk monitoring processes from the various business functions integrate eventually. Finally, the corporate risk committee monitors and audits these four risk processes for each business unit to ensure that the risk management efforts of the business units are in synchronization with the corporate risk strategy and the corporate culture.

5.8 Chapter Summary

This chapter introduced a detailed risk management case study for a typical high-tech firm. Considering the sensitivity around risk management the case study did not focus on a particular company, but rather emphasized on the steps that a firm could take to accomplish risk management within its firm.

The chapter started with assessment of a firm's risks at the top level and then used recursive risk identification technique to unearth risk trigger points for a few business functions. Thereafter, the supply chain management function was treated exhaustively with respect to all four stages of 3T-4R framework. It is important to note that a pragmatic capacity would require

establishing different scenarios about the changes that would be most beneficial to mitigate the risks.

The chapter finished with a discussion around the assimilation of the result of these stages into the ICRM framework and the role of corporate risk committee. The next chapter discusses the method and approach that was followed in our work.

6 METHODS & APPROACH

This chapter discusses the methods and approach towards the problem analysis and the resulting solution. Our overall philosophy during this work has been that of *"Correct Analysis, Right & workable Solution"*. Risk management within the high-tech world is a relatively new field and there is a lot of confusion in the industry about the right approach in identifying the problem and proposing a workable solution. The following sections detail our approach towards the problem and its solution.

6.1 Problem Analysis Approach

There are various schools of thought regarding risk management. We briefly touched four of these in Chapter 2; these four approaches were the strategic, insurance, financial and IT approach. Rather than pick one of these and discard the others we took a "Mutually Exclusive Collectively Exhaustive" approach - a methodology that's frequently used in the management consulting world to analyze tough problems that have a lot of uncertainty inherent in them.

According to this methodology, a problem should be broken down into possible constituents in such a manner that no two constituents replicate themselves, while at the same time the sum of constituents should define the problem in its entirety. In particular, apart from using the above approach, we followed the following steps to analyze the problem.

Systems Approach: Rather than look at the risk management problem in isolation, we took a systems approach to analyze the problem. Therefore, we analyzed the risk management problem with respect to the following parameters.

- **Firm Analysis**: Different firms have different degrees of risk management sophistication when it comes to risk practice. Therefore, all firms don't face the same degree of problem. The firm analysis was done to understand if firms have different needs towards risk management and it was clear that risk management meant different things to different firms based on size, industry position and importance of risk to the firm's business strategy. The firm analysis helped us look at the risk management problem objectively, and helped us refrain from a generic risk management prescription fitting everybody's need.
- **Goal Analysis**: Different firms have different goals and for some of these firms risk might not be a big part of their business strategy. Consider for example, the companies in the high-tech support business. The goals of firms in this business are very different than the goals of companies who are in the business of marketing innovations. Therefore, risk could mean different things to a high-tech commodity company compared to a high-tech innovation company. The goal analysis helped us understand that rather than prescribe a solution, it was important for us to prescribe a "risk management approach" that could be used by different companies in the high-tech industry.

  After the firm analysis and goal analysis, we plugged in various pieces in our systems approach by continuing with gap analysis and then getting feedback about the approach from industry and academia.

Gap Analysis: In this stage, the four risk management approaches described in Chapter two were analyzed closely to find out the gaps in their hypotheses. Furthermore, these gaps were thereafter discussed with industry risk leaders and academic experts.

Industry Feedback: The risk management problem, as understood by us in the new light, was put across a few risk management leaders in the high-tech and financial services to ascertain if they saw the same gaps in the current risk management practices, that we saw.

Academic Thought: Finally, the problem hypothesis was put across a few academic experts to assert, if we are tackling the right problem. These academics were pooled from different areas; while Paul Carlile helped in brainstorming the systems view and the complete risk picture, other academics from MIT, during informal conversations stressed the need for a systems approach rather than being focused on a singleton risk approach.

6.2 Solution Approach

Risk management industry is abundant with solutions befitting specific situations. Nevertheless, as discussed in Chapter 2, these solutions take a tunnel view of the problem. Some solutions focus on insuring the risk, while others focus on hedging the risk financially. While devising a solution, our approach was guided by *"systems view"* and *"wide applicability"*. This dual focus was the first important aspect of our solutions approach.

Therefore based on our approach to focus on systems view and wide applicability; our goal was to come up with a generic framework that could be applied to any situation. Although our work has focused on high-tech industry and the case study in Chapter 5 focused on a large high-tech firm; the 3T-4R framework is generic enough to tackle risk management problem in any industry, irrespective of the size of the company. Similarly, the risk management maturity model introduced in Chapter 4 is also generic in terms of its applicability to firms. Therefore it was important that our solution be a *"generic"* solution that could be applied to any risk management solution.

The second important aspect of our solutions approach was help firms devise their own risk management strategy, rather than follow a cookie-cutter approach. This required a solutions focus that would help firms develop capabilities at their pragmatic layer to handle any kind of novelty. This focus to help firms develop a common language, syntax and processes related to risk was the second most salient aspect of our risk management solution strategy.

The 3T framework by Paul Carlile has the capability to address the issue of novelty at any boundary within a firm. The 4-R framework on the other hand had the capability to come up with a disciplined risk management approach for a micro or business function level. We combined 3T and 4R to form the 3T-4R framework, so that the generic nature of 3T could be married with the micro focus of 4R to come up with a *"generic", "scalable"* and *"robust"* risk management framework that could be used at any level (boundary) of the firm to handle any level of risk (novelty).

After coming up with the risk management maturity model and the 3T-4R framework, we focused on the risk analysis aspect for a few important business functions and came up with methodologies pertaining to these business functions. We covered methodologies related to M&A, Information Security and Supply Chain Management in Chapter 4. The approach while devising these methodologies was one of analytical rigor based on a fundamental risk analysis concept. We used network analysis method to analyze supply chain management and all our analyses had the value at risk (VaR) concept at their core. There is a wide debate in the risk management world about the right methodology that could be used in all situations.

We believe that the immediate goals of various business functions are too dispersed to be analyzed by a single methodology. Nevertheless, a fundamental risk analysis concept like value at risk could definitely be used at the core to come with advanced risk analysis methodologies

corresponding to different business functions. Therefore, our approach was to devise business specific risk analysis methodologies based on a fundamental risk analysis concept – value at risk.

Finally, while designing the ICRM (Integrative Corporate Risk Management) architecture or framework, our goal was to come up with a systems level framework that could work in tandem with the corporate risk strategy. Our solutions approach in this case was to have a common language and syntax at the firm level. In other words, in this case we treated the whole firm as a pragmatic boundary that required common language, meaning, interest and syntax capabilities to function as one cohesive group. Finally, the approach for suggesting the corporate risk committee was guided by the fact that the ERM capability of a firm requires constant audit and guidance by a corporate watch dog.

In a nutshell our solutions approach was guided by a systems view, a generic solution focus, customized risk analysis methodologies, workable solution and a consistency of ERM purpose across the firm.

6.3 Chapter Summary

The chapter started with a discussion of our approach and methods used to analyze the risk management problem and our proposed solution. The importance of firm, goal and gap analysis was discussed thereafter.

Finally, our solutions approach was discussed. It was stressed that our solutions approach was guided by a systems view and a generic solution focus. Also, our solution stressed on customized risk analysis methodologies, workable solution and a consistency of ERM purpose across the firm.

The next chapter will discuss the results drawn from this work. We will also discuss these results and finally we will draw the conclusions based on the results and discussion.

7 RESULTS, DISCUSSION & CONCLUSION

The case study in Chapter 5 elucidated the use of our novel 3T-4R framework and the unique risk analysis methodologies. While formulating these frameworks, methodologies and during their application to a large high-tech firm we found interesting results that are listed below and discussed thereafter.

7.1 Results & Discussion

The single most important result that we got during the process was the appreciation of the fact that ERM poses a unique challenge in creating a *"generic"* solution based on *"uniqueness"*. This is a true systems challenge.

A state of the art ERM requires that an organization have common language, common syntax and common processes related to novelties or risks; nevertheless there might be silos based risk management practices in place within various business functions of the firm. In such a case, the challenge is integrating these silos based practices into an organizational DNA that is based on common language and syntax.

To create such a common DNA across the firm requires following a "generic" risk management approach, while at the same time, integrating the silos based risk management practices would require taking the uniqueness of these silos based practice into account as well. In a nutshell, the firms that already have silos based risk management practices in place face the challenge of doing this big integrating exercise that is a mix of bottom-up as well as top-down approach.

Our "*generic*" and "*scalable*" 3T-4R framework that helps firm navigate the risk management maturity curve through the use of "*unique*" risk analysis methodologies is well placed to serve this risk management challenge that firms face.

The above discussion stresses the scope of our solution. Apart from this major insight, during the process of this work we came across other insights as well. The following paragraphs discuss our major results.

Firm Size versus Current Approaches: As discussed in Chapter 1, the current risk management approaches at best help the silos based risk management practices but do not help firms solve the enterprise wide risk management issues. Nevertheless, for a small firm one of these four approaches could be good enough to handle their business function specific needs. But as the size and scope of the firm increases the firm should desist from propagating the silos approach and should make efforts in achieving partial integration through our 3T-4R framework.

Qualitative versus Quantitative: Various risk management experts assign different weights to qualitative and quantitative data with respect to data. According to the quantitative school of thought, if the risk or the impact can't be quantified, the risk analysis or the impact can not be rigorously tested using traditional risk management models. According to the qualitative school of thought the biggest risks are often qualitative in nature and they can't be measured with certainty. Case in example is recent loss of CEO at McDonalds because of an accident.

Therefore it's a difference of opinion between the quantitative and the qualitative experts about the relative importance of data. We believe that there should be a healthy mix of qualitative and quantitative data. Some of the risks can never be quantified, but a generic scale that maps the impacts from the qualitative as well as quantitative data could be used to achieve some consistency of application. Nevertheless, firms should relentlessly try to map qualitative

data to quantitative metrics as and when possible so that the risk impact could be tested based on traditional risk management capital loss models.

Need Analysis & Risk Management: It is important that a firm start the risk management exercise only after analyzing its needs and the place of risk management in its corporate strategy. If risk is not a vital element of the firm's corporate strategy, then ERM could be a big exercise with low returns. Implementing risk management without analyzing a firm's location on the risk management curve could lead to misdirected efforts and resources.

Linear versus Recursive Risk Identification: Linear risk identification method can fail in identifying the real risk trigger points. One of the biggest challenges with risk management is that the perceived threat might not be the real threat. For example - in the current high-tech environment, a company might think that lack of growth opportunities is a major threat. Nevertheless, the real threat could lie in being the victim of the looming consolidation. Therefore recursive identification is important to unearth the dormant risk trigger points of seemingly obvious risk. Uniform risk analysis methodology can not be applied to all business functions.

Value at Risk: We believe that value at risk is a good "core" risk analysis methodology, on which business specific risk analysis methodologies could be constructed. Nevertheless, Value at Risk is not suited for risk analysis situations that require heavy qualitative judgments.

Integrative Risk Management at Corporate Level: Despite the uniqueness inherent in risk management process for various business functions, the Integrative Corporate Risk Management (ICRM) framework that was introduced in Chapter 4 provides a consistency of enterprise risk management purpose. The ERM process needs to be watched and audited by a corporate risk committee on a continuous basis. In a nutshell there needs to be an integrative risk management methodology at the corporate level to watch and audit the consistency of ERM purpose.

7.2 Conclusion

There are quite a few important conclusions that could be drawn from this work. Our first major conclusion is that the right risk management approach varies from firm to firm, based on the importance of risk in the corporate strategy of the firm and the size of the firm. As argued before, if risk is not a pivotal element of the corporate risk strategy and if the size of the firm is not large –silos based risk management might be good enough for the firm. In a nutshell, risk management needs to be customized based on a firm's needs and goals.

Secondly, an efficient enterprise risk management process is a slow process that has to create common language, syntax and processes to build capabilities at the pragmatic layer. In most cases most large firms would have some silos based risk management practice in place, while at the same time to build a firm wide pragmatic capability the mandate has to be started from the top. Therefore, risk management at large firms has to be a combination of top-down, as well as bottoms-up approach. This means that at the 3T-4R needs to be applied in an inside-out fashion starting from various business units; but slowly this capability has to combine various boundaries together through common language, syntax, meanings, culture and processes. This bottoms-up effort has to be supported by a top-down strategic risk management approach, whereby the corporate risk committee ensures that the bottoms-up integration is happening in accordance with the needs, requirements and corporate risk strategy of the firm.

We also conclude that although risk management should be treated in a generic way across the firm, but the risk analysis part for various business functions or boundaries need to be customized.

Finally, we believe that our work has laid an innovative foundation in the world of high-tech risk management. This is a new area and a lot of ground needs to be covered before the field reaches a decent stage of maturity. We hope that our work will help people get interested in this new area which is heavily dominated by operational risk management; and enable firms achieve superior enterprise risk management in coming years.

7.3 Chapter Summary

This chapter discussed the results drawn from this work. The utility of risk management maturity model, the 3T-4R framework and the ICRM methodology were discussed. It was noted that ICRM is an integrative approach that puts together the best of current risk management approaches and fills in the gaps by using 3T-4R.

Thereafter we drew our conclusions about the right approach of following risk management. We noted that every firm has unique needs therefore firms should not look at a particular risk management approach with a silver bullet outlook. Finally, we discussed the innovative ground that this work has covered in the area of enterprise risk management and expected that our work would lead to more interesting work in this growing field.

The next chapter covers some recommendations based on our work and we also discuss future work that could be carried on, based on this work. We lay out some ideas that could prove to be interesting to future enterprise risk management practitioners.

8 RECOMMENDATIONS & FUTURE WORK

Our work has come with a generic framework to address the issue of risk management for high-tech firms. The section on recommendations discusses some lessons that firms could employ to tackle the complex issues related to risk management. Also, while working on this project, it became clear to us that tackling risk management in its entirety is a huge exercise.

We believe that this work has laid out an innovative approach towards enterprise risk management, but a lot of ground needs to be covered to complete the work. The section on future work discusses some future work directions that could complement the current effort and help make advances towards the practice of *"systems based enterprise risk management"*.

8.1 Recommendations

The following are our recommendations to high-tech firms based on our work. Some of these recommendations are equally applicable to non high-tech firms as well.

Right Approach: Silos based risk management approach seems to be reasonable in the initial stages of risk management, or for small companies, but over the long period of time this approach hurts more than it helps. Therefore, firms should adopt an enterprise risk management approach from the very beginning, even if it seems more time consuming and costly.

To contain the costs, the firm could address risk management in a few business functions only. But adopting a top-down, enterprise risk management strategy saves huge re-integration pains that a firm has to go through while combining the silos approach and that too after a firm has gone through a massive growth phase.

Need Analysis: Fully integrated risk management is an advanced stage of risk management and all companies might not need it. If risk is not a dominant part of a company's business strategy, the firm need not allocate resources to move to the most advanced stage on the risk management curve.

A firm needs to manage the amount of risk, that is required – no more, no less. Therefore, a thorough risk management need analysis is required before a firm decides to reach to the highest bracket of risk management curve, in the shortest amount of time.

Right Analysis: Doing the right risk analysis is half the battle won in most cases, therefore adopting a cookie-cutter approach in risk analysis is detrimental to risk management. Supply chain risk analysis can not be analyzed in the same fashion as risk analysis in emerging technologies. Therefore, customized risk analysis based on the particular business situation is a key to right risk management.

Although, these risk analysis approaches could be different, they could be based on generic risk analysis fundamentals. In our work, we have relied on value at risk as our fundamental risk analysis component, but firms can chose any risk analysis component based on their needs.

Based on our work and the recommendations of other industry experts, we believe that value at risk is a robust risk analysis component based on which advanced and customized risk analysis methodologies for various business functions could be constructed.

Self Belief: Adopting the right risk management approach in a lot of cases could mean going against the wisdom of current practitioners. But companies should understand and appreciate the fact that operational risk management is an emerging field and they need to depend on themselves to adopt the "right approach" based on their situation and goals.

A system integrator or a management consultant can not be expected to know more about "customized" risk analysis compared to the firm itself. Therefore taking responsibility about its own risks and their right analysis is a job that can not be outsourced or bought as a service by a firm.

8.2 Future Work

We hope that our work will lay the foundation for a "systems" approach towards risk management and will spawn a lot of interest in various areas related to risk management. There a quite a few directions for future work and a few of them are discussed below.

Risk Analysis Frameworks: It was out of the scope of our work to come up with detailed risk analysis frameworks for all business functions that a firm has. Nevertheless, we developed a few risk analysis methodologies that could be applied to some of the most important business functions. More in depth quantitative treatment of the frameworks covered in this work and coming out with frameworks for other business functions could be an interesting future work direction.

Risk Processes: Another area of work could be an in depth study of risk processes and the right approach to have them in place along with the business measurement processes. What should be the relationship between these two types of processes could be another direction of future work.

Qualitative versus Quantitative: A lot of business analysis frameworks rely on qualitative information. Case in example is "brand reputation" risk. How should these qualitative assessments be backed by analytical rigor could be interesting work.

Top-Down versus Bottoms-up approach: Finally, taking a few companies as case studies and finding out relative merits and demerits of top-down versus bottoms-up risk management

approaches could be a worthwhile study. This study could help shed more light on the risk maturity model that we proposed in chapter 4.

8.3 Chapter Summary

This chapter discussed the recommendations to high-tech firms based on our work. Considering that this work was an initiation in the practice of "systems based risk management" a lot of ground needs to be covered in coming years; the section on future work talks about the future work that could be carried on based on this work.

9 REFERENCES

Leonard-Barton, D. (1992), "*Core Capabilities and Core Rigidities: A Paradox in Managing New Product Development*," Strategic Management Journal, 13 (Summer Special Issue): 111-125.

Bernstein, P. (1998), *"Against the gods: The remarkable Story of Risk"*, Wiley New Edition, August 31, 1998

Harmon, P. (2003), *"Business Process Change"*, Morgan Kaufman Publishers, 2003

Baron, T., Shenkir. W., Walker. P. (2002), *"Making Enterprise Risk Management payoff"*, FEI research foundation, 2002

Blanchard, B. and W. Fabrycky (1998), *"Systems Engineering and Analysis"*, 3rd Edition, New York: Prentice Hall

Carlile, P. (2004), *"Transferring, Translating, and Transforming: An Integrative Framework for Managing Knowledge Across Boundaries"*, Forthcoming in *Organization Science.*

Carlile, P. (2003), *"Dynamics of Firm Knowledge and Competitive Advantage"*, MIT Working Paper

Carlile, P. (2004), *"The Dynamics of Firm Knowledge and Competitive Advantage: A Theory and Case Example"*, Currently under review at Strategic Management Journal

Carlile, P and E. Rebetisch, (2003), *"Into the Black Box: The Knowledge Transformation Cycle"*, Management Science, 49, 1180-1195.

Christensen, C. (2000), *"The Innovator's Dilemma"*, New York: Harper Business

Lam., J. (2003), *"Enterprise Risk Management – from incentives to controls"*, Wiley Finance 2003

McCarthy., M. and Flynn., T. (2004), *" Risk from the CEO and Board perspective"*, McGraw Hill Business (2004)

Van Den Brink., G. (2002), "Operational risk – The new challenge for banks", Palgrave

Eppinger, S. (2001), *"Innovation at the Speed of Information"*, Harvard Business Review, 79, 1: 149-158.

Grove, A. (1999), *"Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company"*, New York: Double Day

Leonard-Barton, D. (1991), "*Wellsprings of Knowledge: Building and Sustaining the Sources of Innovation*", Boston: Harvard Business School Press.

Maier, M. and E. Rechtin. (2000), "*The Art of Systems Architecting 2nd Edition*", Boca Raton, FL: CRC Press.

Moore, G. (1999), "*Inside the Tornado*", New York: Harper Business

Schrage, M. 1999. *Serious Play*, Boston: Harvard Business School Press.

Utterback, J. (1994), "*Mastering the Dynamics of Innovation*", Boston: Harvard Business School Press

The Economist Intelligence Unit (1995), "*Managing Business Risks: An Integrated Approach*"

Ohmae, K. (1982), "*The Mind of the Strategist*", McGraw Hill

Sohnke, M. (2001), "*Corporate Risk Management as a Lever for Shareholder Value Creation,*" Economics Working Paper Archive at WUSTL

Björnsson, P. (2004), "*How to handle risk and uncertainty in supply chains - a real option approach*"

Lindroth, R., (2003) "*Managing Strategic Supply Chain Risks in the Telecom Industry*"

Mullai, A., "*Transport of Dangerous Goods - an analysis of risks from dangerous goods carried in packaged form by sea*"

Norrman, A., "*Supply Chain Risks and Risk Sharing Instruments*"

Paulsson, U., "*Risk Management of the Supply Chain Product Flow - a conceptual approach*"

Borge, D. (2001), "*The Book of Risks*", John Wiley & Sons Inc., New York

Deloach, J. (2000), "*Enterprise-wide Risk Management*", Arthur Andersen. Financial Times, Prentice Hall, London,

Doherty, N. (2000),"*Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*", McGraw-Hill Professional Publishing

Rasmussen & Svedung, I (2000), "*Proactive Risk Management in a Dynamic Society*"

Markowitz, H. (1952)," *Portfolio selection*", Journal of Finance, 7 (1), 77-91

Morgan Guaranty (1994), *"RiskMetrics Technical Document"*, 2nd Edition, New York: Morgan Guaranty

Finne, T. (1998), *"Information Security Implemented in: the Theory on Stock Market Efficiency"*

Markowitz Portfolio Theory and Porter's Value Chain, *"Computers and Security"*, 17 (4), pp. 303-307

Finne, T. (1997), *"A Conceptual Framework for Information Security Management"*, Computers and Security, 16 (6), pp. 469-479.

GAO Report (1999)," *Information Security Risk Assessment – Practices of Leading Organizations"*, Report No. AIMD-99-139

GAO Report (1998), *"Information Security Management – Learning from Leading Organizations"*, Report No. AIMD-98-68

Microsoft Whitepaper on Security (2002)," *http://www.microsoft.com"*

Simons, K. (1996), *"Value at risk – New approaches to risk management"*, New England Economic Review, September-October, pp. 3-14

Turban, E. and McLean, E. (1996), "Information Technology for Management: Improving Quality and Productivity", John Wiley and Sons

10 APPENDICES

The appendices include a treatise on value at risk, a risk measurement technique that's used at the core of our methodologies in Chapter 4. We also present a copy of the survey that was used to collect risk management data from a few business functions in selected firms.

10.1 Value at Risk (VaR)

Value at Risk is a measure of potential loss from an unlikely, adverse event in a routine environment; and it is denominated in units of a currency e.g., US dollars. In a nutshell value at risk is an amount $V where the chance of losing more than $V is, say, 1 in 100 over some future time interval, say 1 day. This being a probabilistic statement it is obvious that VaR is a statistical measure of risk exposure.

Traditionally in the financial industry VaR describes the probabilistic risk measure of the market risk of a trading portfolio. In the financial industry VaR is considered to be the single risk-measurement technique available. Nevertheless, usage of VaR in the operational situations is still in a nascent phase, and this work has used VaR in a few operational situations.

For institutions to manage risk, they must know about the risks while they are being taken. For example, in the financial world, if a trader does not rightly hedge his portfolio – the firm needs to know that before the loss is incurred. VaR gives firms the ability to do so. Unlike retrospective risk metrics such as historical volatility, VaR is prospective. It quantifies market risk while it is being taken and the time is measured in business days.

Assume that t_0 is the current time. Also, assume that the current market value of the portfolio is denoted by ${}^0p$ and its market value by the end of one trading day is denoted by ${}^1p$. Note that the market value of the portfolio at the end of one trading day is unknown, since it's a random variable. Being a random variable, it could be assigned a probability distribution. Using VaR the market risk of the portfolio can be reported using some parameter of this distribution. For example, we might report the 90%-quantile of the portfolio's single-period US dollars loss. This is called one-day 90% USD VaR. If a portfolio has a one-day 90% USD VaR of, say, USD $5M, it can be expected to lose more than USD 5MM on one trading day our of ten. This is illustrated in the figure below

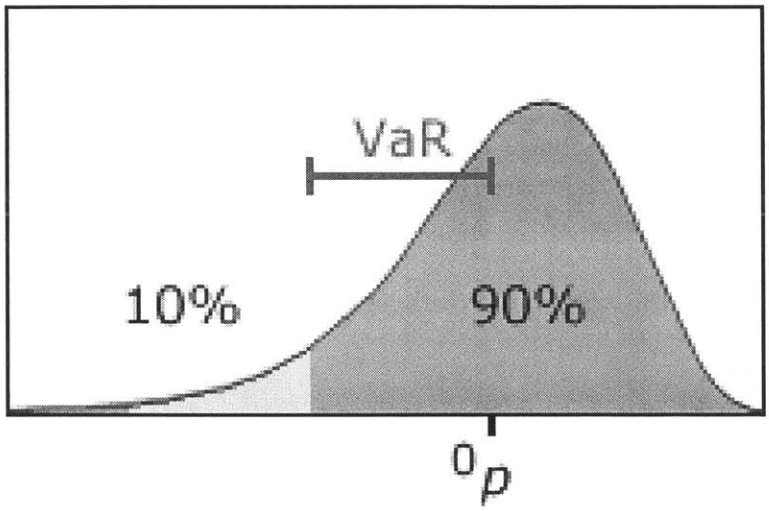


Figure 23: One day 90% USD value at risk

The figure shows one-day 90% USD VaR for a hypothetical portfolio and it shows the probability density function for the portfolio's value after ${}^1p$ day of trading. Since the current value of the portfolio ${}^0p$ is known, VaR equals the amount of money such that there is a 90% probability of the portfolio losing less than that amount over the next trading day.

10.2 Risk Management – Assessment Questionnaire

The following survey questionnaires could be used to collect information about the current risk management process of a firm. The surveys are divided into four portions and each portion collects information on one of the four stages of risk management. Note that the questions are based on the DMAIC (Define Measure Analyze Improve Control) methodology.

10.2.1 Risk Identification

1. What is business disruption according to your scope?

2. What "kind" of factors can cause this disruption? Example – Economic, Natural, Business, Terrorism etc.

3. Does your BU[5]/BF[6] have a Decision Analysis or Scenario Analysis mechanism in place to assess the root-causes of these disruptions?

4. Please list events in each of the categories outlined in Q.2 that could disrupt your business.

5. Apart from the factors and events outlined in Q.2 and Q.3 are there any other special factors that could cause disruption to your business?

10.2.2. Risk Analysis

1. What is Risk for your Business? How do you define it?

2. Define Organizational Risk and business unit risk? Could these be two different things based on the primary responsibilities of your Business Units?

3. What's the potential severity impact of this Risk to customers? What do the customers stand to lose because of this impact?

4. Please name the Business Units or Business Functions within the firm that your team works with in day to day operations?

5. For these cross-function operations - is there a possibility that the definition of Risk understood by these Business Units?

6. How mission critical is the disruption? (Scale 1-5, with 1 being least critical and 5 being most critical)

Measure - M

7. How do you measure Risk?

8. What Frameworks/Metrics/Tools do you use to measure it?

9. Do you use any Statistical Tools to do Risk Measurement/Analysis?

10. Do you use any in house tools to do Risk Measurement?

Analyze - A

11. Do you have data to measure Risk?

12. Do you have any historical data to do Risk Assessment? If yes, what's the distribution[7] that you have witnessed? Do you use any industry benchmarks?

13. What's the variance you have witnessed in the quantification of Risk?

14. What are the key factors that cause variation?

15. Do you use any probabilistic, statistical tools to study the variations etc?

16 Could any of these tools be used on a corporate level to do similar analysis for various Business Units ?

Improve - I

17. How do you think the Risk Assessment could be improved

18. What metrics should be in place to measure the Risk Assessment?

19. Are you aware of any tools available in market that could be used to study the Risk Assessment in your line of business?

20. Any other thoughts as to how Risk Assessment analysis could be improved in your line of business?

---

[7] Normal Distribution, Lognormal Distribution etc

Control - C

21. Is there any documentation in place to analyze Risk Assessment?

22. Do you intend to create new metrics to track, predict, asses Risk Assessment?

23. Would you create a process to do so? If so, who is the most likely person to own it?

10.2.3 Risk Management

Define – D

1. How do you define Risk Management within your Business Unit or Business Function?

2. Could Risk Management for your Business Unit be different than the Risk Management for the corporation?

Measure - M

3. How do you manage/mitigate the Risk?

4. What tools do you use to mitigate it?

5. Explain any practices, exercises that you do with clients/customers to mitigate the risk?

6. Do you work closely with your Clients to identify and mitigate the Risk? Are their any joint cross-functional teams working with client to manage common risk?

7. What's the frequency of interaction with your clients to identify and mitigate the risk?

8. Are their any metrics in place to measure Risk Management?

Analyze - A

9. Does your Risk Management strategy/plan immediately address customer needs?

10. Do you have data to analyze the Risk Management, as defined and measured above?

11. Do you have any historical benchmark data to do this analysis? Are their any past Risk Management performance pattern studies within your BU/BF?

12. What are the key factors that cause variation in Risk Management?

13. Do you use any probabilistic, statistical tools to study the variation in Risk Management[8]?

[8] This might not hold true if your Risk Management strategy is a collection of tools, processes

14. Could any of these tools be used on a corporate level to do similar analysis for various Business Units or Business Functions – especially the BU's/BF's with whom you have a operating relationship.

Improve - I

15. How do you think Risk Management could be improved

16. What metrics should be in place to measure the Risk Management?

17. Are you aware of any tools that could be used to do Risk Management in your line of business?

Control - C

18. Is there any documentation in place to analyze Risk Management?

19. Do you intend to create new metrics to track, predict, asses Risk Assessment?

20. Would you create a process to do so? If so, who would be the most likely person to own that process?

10.2.4 Risk Monitoring

1. How do you define Risk Monitoring within your Business Unit or Business Function?

2. Could Risk Monitoring for your Business Unit be different than the Risk Monitoring

for the corporation?

3. Where and how is the customer involved in the Risk Monitoring process?

Measure - M

1. How do you monitor the Risk?

2. What tools do you use to monitor it?

3. Explain any practices, exercises that you do with clients to monitor the risk?

4. Do you work closely with your Clients to monitor the Risk?

5. What's the frequency of interaction with your clients to identify and monitor the risk?

6. Are their any metrics in place to measure Risk Monitoring?

Analyze - A

7. Do you have data to analyze the Risk Monitoring, as defined and measured above?

8. Do you have any historical benchmark data to do this analysis?

9. What's the variance you have witnessed in monitoring Risk?

10. What are the key factors that cause variation?

11. Do you use any probabilistic, statistical tools to study the variation in Risk Monitoring?

12. Could any of these tools be used on a corporate level to do similar analysis for various Business Units?

Improve - I

13. How could Risk Monitoring be improved

14. What metrics should be in place to measure the Risk Monitoring?

15. Are you aware of any tools that could be used to do Risk Monitoring in your line of business?

16. Do you have any in house tools that could be useful for other departments etc.?

17. Any other thoughts as to how Risk Monitoring could be improved in your BU/BF?

Control - C

18. Is there any documentation in place to analyze Risk Monitoring?

19. Do you intend to create new metrics to track, predict, asses Risk Monitoring?

20. Would you create a process to do so? If so, who would own that process?

21. Any final thoughts on Risk Monitoring and overall BCP?