



Good Management in an Uncertain World

Risk and its Interpolation with Management



Preface to Treatise

We are living in an uncertain world. Whereas traditional risks are now mastered, real danger lurks within the so called untamed risks which are mostly strategic and operational in nature. Good people and leaders with strong moral coordinates were never so needed, and challenged, as they are today. Traditional supports have given way to secularism and market forces so great that the average citizen is greatly stressed.

Much is spoken about Enterprise Risk Management (ERM) and many electronic solutions provided. Risk management is now a main board agenda item and no longer just AOB. We have the first signs of the emergence of one universal nomenclature and framework for the management of organisation wide risks. This is all very good, but not good enough without the recognition of some fundamental principals without which organisations will fail in the 21st century. These include:

1. **Risk management is just good management:** People think of the management of risks as a specialist activity. This is untrue. Successful companies in the 21st century are those which will have acquired a resistance to traditional risks and developed a new strain of DNA rendering them more capable than others of surviving shocks and surprises. Without realising it they will have developed of way of thinking and doing and getting the right balance between doing the right thing, and doing things the right way,
2. **Risk owners own risks, risk advocates do not.** Embedding ERM is a change management process where risk ownership at the divisional and business unit line manager levels is the core objective. The management of risk should not be driven by IT solutions or external consultants on one off technical assignments.
3. **Good management of obstacles to goals and objectives is an iterative process:** Good management requires a blend of quantitative fact and subjective judgement. Once people ask certain questions and process information correctly they effectively inoculate the organisation to most common hazards and threats to opportunities. Thereafter corporate killers are most likely to be those associated with leadership issues and discontinuities.

There are some worrying fault lines in conventional risk management practice. These include:

4. **Risk Appetite:** Many organisations fail to pay sufficient attention to stakeholder expectations and capabilities and reaching a determination as to risk appetite and risk management criteria,
5. **Estimating probabilities and impacts:** This is rarely conducted in a credible and consistent manner. Recommended methods are frequently used incorrectly. A new methodology is proposed which is astounding in its simplicity and credible with regard to the soundness of its input and output conditions,
6. **Measurement and value for money:** Demonstrating return on risk management effort is fraught with difficulty. It is not unusual for risk management expenditures to be driven by either compliance or IT or a combination of both. Similarly it is not uncommon for organisations to claim dissatisfaction with value for money. A new methodology is recommended which when applied correctly postulates a return on risk management effort using measurement criteria which are demonstrably credible and auditable.



V0.4

Introduction

This treatise presents a methodology which adheres to the proposed ISO 31000 (risk management: draft) due for publication in June 2009. This standard is largely influenced by the Australia New Zealand risk management standard ANZ 4360. The methodology also adheres to ISO Guide 73 (Risk Management Vocabulary-Guidelines for use in Standards).

The methodology includes a patent pending element for estimating probabilities and impacts. When used in conjunction with project management methods it is possible to project a return on risk management effort in a demonstrable and auditable way.

The methodology is rendered very simple and straightforward through the use of a simple excel based data collection format. This format synthesises obstacles to objectives, risk assessment, risk evaluation and risk treatment. Risk communications and risk monitoring are achieved through the use of project management methods.

A detailed process flow which diagrammatically presents the methodology is included at the end of this paper.

The paper is organised in four sections as follows:

Section 1: Context: Natural observations and unheralded new rules

Section 2: Problem Definition: People, Perception, Language, Speed of Change, and Silos

Section 3: The Solution:

- Clarity
- Demonstration of return on risk management effort,
- Methodology for estimating probability and impact,
- Standard ERM framework, principals and risk management process,
- Standard language, terms and definitions,

Section 4: ERM Methodology Detailed Process Flow



V0.4

Contents

Preface	2
Introduction	3
Section 1: Context:	5
Section 2: Problem Definition:	7
Section 3: The Solution:	11
Section 4: ERM Methodology Detailed Process Flow	25

**Section I****Context****Natural Observations and Unheralded New Rules**

Uncertainty requires good management, not risk management. However good management in modern, internationally focused companies now requires the conscious adoption of particular business management skills hitherto regarded as specialist and not for the senior echelons. New required skills include a blend of certain aspects of risk assessment and project management. More often than not senior managers just need to know what questions to ask to ensure that the prerequisite requirements to good management of uncertain things are in place. This is the overarching requirement. Thereafter recognition of the unheralded arrival of new rules for good management is also required. These new rules will be listed shortly. First some observations:

Observation Number 1:

Risk strategy is owned by the Board, not by management. This is so because the Board is charged with long term sustained growth towards clearly stated goals. Management is charged with near term achievement of objectives required to secure goals. Time horizons for both are different, but they are aligned.

Observation Number 2:

Both directors and management need the same things. They require:

1. Knowledge of obstacles and risks to goals and objectives,
2. Understanding of those variables directly influencing probability and impacts of obstacles and risks,
3. Certainty that the entity is in full compliance with regulations and obligations,
4. Clarity.

Knowledge, understanding and certainty are not achieved through internal audit. Internal audit is a checking and compliance function. It is a compliance and administrative support to good and effective management. On the other side of the same coin there is risk management.

Risk management is a proactive function. It involves searches for threats, obstacles and tell tale characteristics of variables which influence the occurrence of both desired and adverse events.

Observation Number 3:

Theory and practice are somewhat different. Risk management expenditures tend to be largely directed at:

- Compliance which whilst important does not increase value. Compliance with regulations and obligations is an operational requirement and a sunken cost,
- Hazard and financial risks which whilst constantly requiring attention tend only to destroy value in exceptional cases¹. They're management have today become part and parcel of the mainstream professional management organisation.

¹ Two studies have pointed out the significant loss of shareholder share that resulted from the mismanagement of strategic risks. A study by Mercer Management Consulting analyzed the value collapses in the *Fortune* 1000 during the period 1993-1998. The analysis found that 10% of the *Fortune* 1000 lost 25% of shareholder value within a one-month period. Mercer traced the collapses back to their root causes and found that 58% of the losses were triggered by strategic risk, 31% by operational risk, 6% by financial risk, and hazard risk did not cause any of the decrease in shareholder value. (*Enterprise Risk Management – Implementing New Solutions*, 2001; 8.) A more recent study by Booz Allen Hamilton analyzed 1200 firms during the period of 1999 through 2003 with market capitalizations greater than \$1 Billion. The poorest performers were identified as companies that trailed the lowest-performing index for that period, which was the S&P 500. The primary events triggering the loss of shareholder value were strategic and operational failures. Of the 360 worst performers in the study, 87% of value destruction suffered by these companies related to strategic and operational mismanagement. (Kocourek, 2004: 1.)



V0.4

Risk management effort in these (financial and hazard risks) limited terms is confined to the downside and the historic. It largely ignores opportunity and fails to assist in the safe passage through strategic and operational risks.

Observation Number 4:

Whither clarity! Risk for most people is an abstract and difficult concept to grasp. The problem is compounded by models depicting risk quantification, the assumptions and algorithms of which are understood only by the few.

The rather incredible fact remains that global surveys repeat the message that many CEOs claim poor understanding and lack of preparedness for risks in the uncertain world in which they are required to operate. Discontinuities, irregularities and volatilities are increasing in a world where sustained earnings are demanded and any drop in performance severely punished.

Observation Number 5:

In a world where new innovations are appearing and boundaries collapsing at an exponential rate no one risk management solutions provider has broken through with a solution announcing greater assurance in our uncertain world. Technology providers have reengineered risk management processes such that things can be done electronically. But computers do not ask questions and make decisions, people do. Similarly decision support systems are not sufficiently advanced to keep up with the speed of change and multiple interdependencies embedded within the top risks facing decision makers of the 21st century.

Observation Number 6:

The unheralded arrival of new rules for good management should be widely acknowledged. New rules include:

1. **Rule 1:** Risk strategy is owned by the Board, not by management. Management owns execution.
2. **Rule 2:** Knowledge of obstacles, understanding of variables, certainty of compliance and clarity are mission critical to good management where uncertainty prevails,
3. **Rule 3:** Financial and hazard risks are now mastered. Danger remains within however they are now part of the mainstream professional management organisation. We need to apply the same rigor to the management of strategic and operational risks.
4. **Rule 4:** In the presence of growing uncertainty, strategic and operational risks require a clearly defined, well understood, people engaging and rigorously applied process management approach characterised by:
 - a. Clarity.
 - b. Standard convention for assessing return on risk management effort,
 - c. Standard methodology for estimating probabilities and impacts which releases us from the limitations, and excesses, of perception,
 - d. Standard ERM framework, principals and risk management process,
 - e. Standard language, terms and definitions,



Section 2

Problem Definition

People, Perception, Language, Speed of Change, and Silos,

Before we progress to the proposed solution it is instructive to reflect on some natural observations which help us to more sharply define obstacles to successful implementation of ERM programs.

Context: The management of risk is growing in importance as is the understanding that managing risks for compliance with regulations is not the same as managing risks to maximize desired outcomes, avoid catastrophe, and minimise shocks and surprises².

Problem Definition: For many organisations, risk management is a grudge purchase delivering questionable value beyond pure regulatory compliance.

Beyond Compliance: Problem Analysis:

- Insurable risks³ are predictable. Because something can be done about them they rarely destroy value. Uninsurable risks are foreseeable, but because not enough reliable data exists as to frequency they are unquantifiable. For this reason uninsurable risks have potential to destroy value, for example:
 - BP,
 - Enron,
 - AIG, Marsh etc and
 - Strategic mistakes, e.g. many mergers and acquisitions etc.

In addition to uninsurable risks strategic mis-steps, poor execution and incorrect alignment of vision to core capability(s) in the pursuit of business opportunities also destroy value.

- Human factors drive the perception of risk. Even where people see events occurring around them they very often perceive that those same, or similar, events will not occur to them,
- Typical risk registers frequently disguise the fact that there are critical dimensions to probability and impact which are frequently not understood. For example:
 - Possible events, be they single occurrences or a series of occurrences' need to be identified and understood if probability is to be correctly described⁴,
 - Consequence of an event(s)...not just financial,
 - Time; effect on probability and on impact,
 - Experience, particularly for events for which there is an inadequate supply of credible frequency data,
 - New discoveries,
 - Control efficacy,
- Paradox:
 - Most good companies employ predominantly good managers. Good managers are problem solvers. They tend to keep 'solutions' simple. Where they perceive credible risks they will do something about them,

² For example: IMA Letter to US SEC 'Seizing the Opportunity Afforded by Draft SEC/PCAOB SOX Proposal'.

³ Property, engineering, process, hazard etc. risks are transferable through insurance.

⁴ Likelihood (high, medium, low) is a general description of probability or frequency. Probability on the other hand is a measure of the chance of occurrence expressed as a number between 0 and 1. Typically, insurable risks are measured in terms of probability, whereas uninsurable risks are described in terms of likelihood.



V0.4

- Risk management processes are designed to provide assurance that controls are effectively applied on an ongoing basis,
 - Most risk solutions are heavy in process and process administration,
 - Most risk solutions are controls rather than risk focused. What this means is that people look at controls in isolation of potential events and consequences. This makes the management of risk an abstract and for many an unrewarding experience. This is particularly the case for line managers closest to risks in the field.

In practice there is a dichotomy between risk control and risk focus, they have become divergent activities.

Conclusion: Who ever is first to simplify risk control, risk focus and risk treatment for risks which destroy value will have created a solution for which there is great need.

Perspectives:

1. The risk services sector is growing rapidly. There are a number of drivers including:
 - a. Regulatory: Basle, Sarbanes Oxley, UK Super Code etc.
 - b. Board Level Concerns about shocks and surprises:
 - i. Concerns about risks to business performance and reputation,
 - ii. Concerns about discontinuities, labour movements and regulatory changes,
 - iii. Concerns about risks to continuity of operations,
 - iv. Concerns about risks to supply chain,
 - v. Concerns about risks to directors and officers personal wealth and reputation,
2. Of these, regulatory drivers have precipitated huge demand for risk management compliance services from the global accounting practices,
3. Costs are huge and continue to rise. In addition customers are pushing back and are seeking greater value for money from services provided by risk management solutions providers,
4. Enterprise risk management (ERM) solutions tend not to work as well in manufacturing, commercial etc. organisations as they do in financial institutions.

One reason for this is that Financial Institutions have one universal language for funds and credit risk management largely influenced by international standards, statistical instruments and models. This advantage is overarched by the intrinsically quantifiable nature of money as a basic unit of measure.

5. Barriers to effective ERM include:
 - a. Lack of engagement of risk owners⁵, as opposed to risk 'managers' and administrators in the proactive management of risk.

The management of risk is not embedded in day to day business practice.

The reasons for this are two fold:

- i. Managers find it difficult to perceive risk events, and consequences which they have not experienced before...*events will not occur if they have not occurred before!*

⁵ Risk owners are those 'managers' closest to risks in the field as distinct to risk managers, risk advocates, risk facilitators, risk administrators etc.



- ii. Where managers do perceive risk events and consequences they have limited ways in which to effectively communicate their concerns in a simple and straightforward manner to the right decision makers,
 - b. Lack of a universal language for the gathering of basic information. For example there is as yet no universally accepted risk nomenclature,
 - c. Speed of change. Risk planners find it very difficult to keep up with speed of internal and external change,
 - d. Complexity of customer organisation which has the effect of creating silos which separate people with critical information and knowledge pertaining to vertical and horizontal risk issues,
 - e. Administrative burden and complexity of many ERM solutions.
6. Strategic risk management at board levels tends to centre on barriers to growth, for example:
- a. New competitor innovation,
 - b. Macro economic conditions,
 - c. Access to markets and capital,
 - d. New regulatory requirements,
 - e. Currency exposures,
 - f. Energy, raw material etc. security of supply and costs
 - g. Political risk, major discontinuities etc.
7. Strategic risk management solutions delivered close to board levels tend to centre on those risks at chief officer levels which are represented on the corporate risk register. It can frequently happen that the treatment of such risks is not devolved to managers in a manner which assures effective treatment. For example effective and successful risk treatments are not always captured within HR programs for performance appraisal purposes etc.
8. At meetings with separate senior directors of two Major Irish Banks the following perspectives were received:
- a. Organisations in survival mode are not really interested in the management of risk,
 - b. Beyond regulatory compliance, organisations who cross the threshold into levels of business success perceive two primary areas of risk:
 - i. Risk(s) to reputation,
 - ii. Risks to continuity of operations,
 - c. The main suppliers of risk management services and solutions are the global accounting firms although no one firm stands out from the others,
 - d. Risk management is proactive. Compliance driven risk management is more of a checking exercise.
 - e. At the level of senior people value is difficult to quantify but when pressed stated that value delivered in the form of ...
 - i. Asking the right / pertinent questions ...
 - ii. Provision of a 'living conscience'
 - iii. Testing / finding gaps in risk assumptions and contingency plans
 Would be very valuable,



V0.4

9. At meetings with separate senior partners of two top 3 accounting firms (risk management services) the following perspectives were received:
 - a. Customers are primarily compliance driven and do not always pay as well for broader risk management services as they do for compliance services,
 - b. Compliance revenue streams support weaker risk management revenue streams,
 - c. Risk management services beyond compliance driven services are not always easy to get (sell) and are not always easy to do as customers do not always know what they want. They do:
 - i. Not expect that risk compliance spending will be an endless revenue stream
 - ii. Experience /anticipate customer push back and greater demand for value for money etc.
 - d. They often struggle to deliver / prove value beyond pure compliance,
 - e. Quite often even the smallest discovery of a risk management related issue is enough to sufficiently energise / satisfy customer relationships in terms of holding onto / growing accounts,



Section 3

The Solution

- 1. Clarity**
- 2. Demonstration of return on risk management effort**
- 3. Methodology for estimating probability and impact**
- 4. Standard ERM framework, principals, and risk management process,**
- 5. Standard Language, terms and definitions**

In our world of growing uncertainty risk management requires a clearly defined, well understood, people engaging and rigorously applied process management approach characterised by:

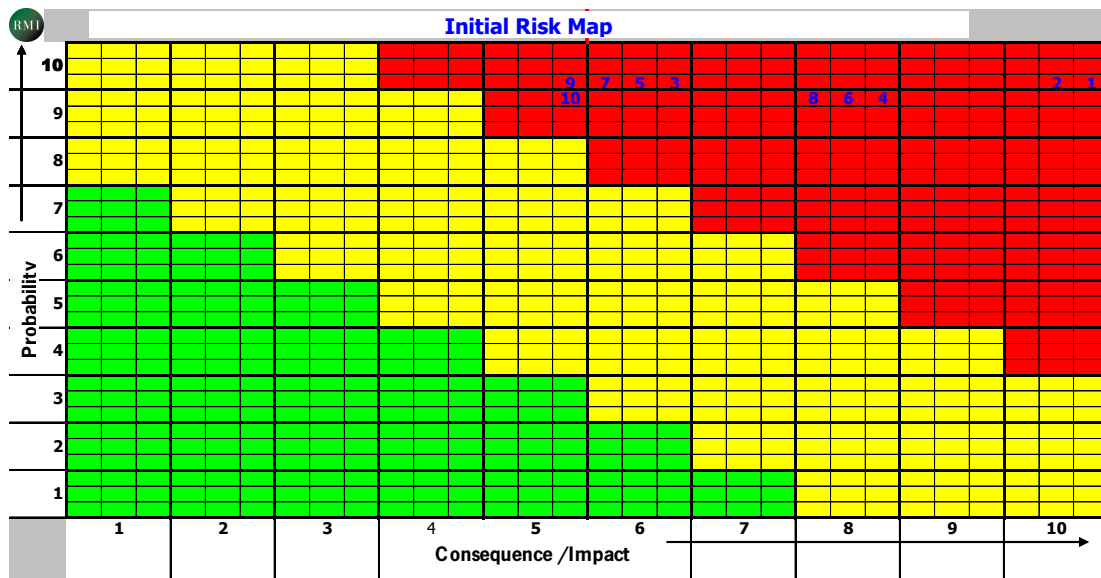
1. Clarity.
2. Demonstration of return on risk management effort,
3. Methodology for estimating probability and impact,
4. Standard ERM framework, principals and risk management process,
5. Standard language, terms and definitions,

RMI has developed a comprehensive process driven ERM methodology which adheres strictly to the requirements listed above. The methodology has three lifecycle phases, 3 milestones, 2 Gateways, 12 deliverables, and over 80 discrete tasks and sub tasks.

1. Clarity

The concluding step in the RMI ERM methodology is the review of automatically generated initial and residual risk maps.

The Initial Risk Map presents risks as they currently stand, using standard methodologies. For example:

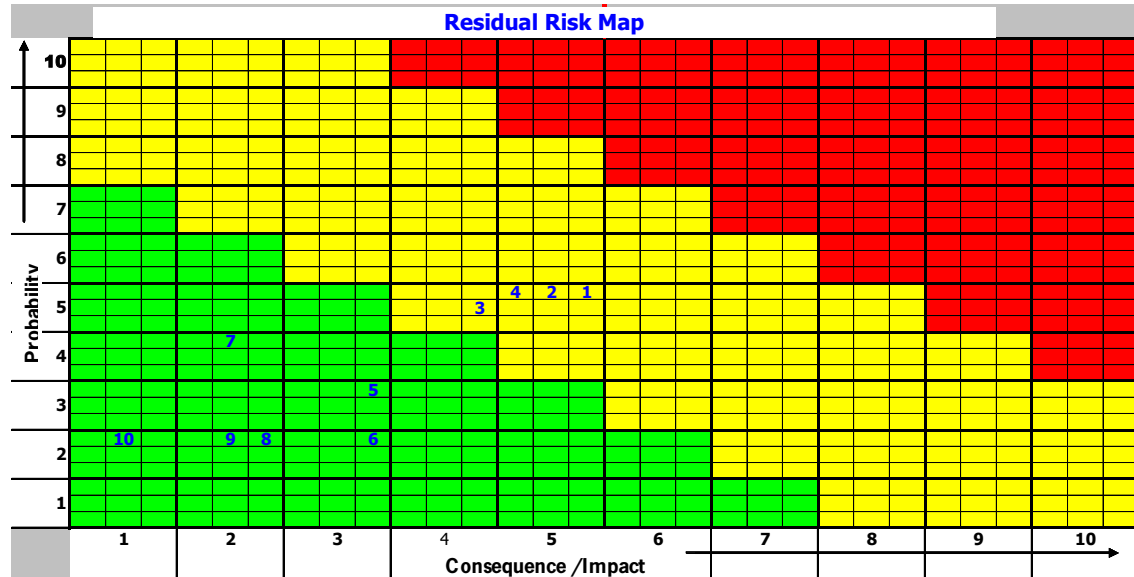




V0.4

The **Residual Risk Map** illustrates those same risks which having been treated in a defined way are projected to **improve measurably**.

A comparison of both the initial and the residual risk maps demonstrates projected return on risk management effort:



Clarity is achieved.

However the question then arises: *'how credible is the measurement of initial and residual risks and also the associated projected improvement in risk management performance'*.

If the initial and residual risk maps are believed then it is clear that the case for the projected return on risk management effort will have been proven.

What is required therefore is a method for introducing consistency in measurement which makes return on risk management effort demonstrably credible.



V0.4

2. Demonstration of Return on Risk Management Effort:

Measurement requires:

1. A start point,
2. An end point, and
3. Units of measure between both points.

This is achieved as follows:

The RMI ERM Methodology is comprised of three lifecycle phases:

Phase I: Establishing Mandate, Sponsorship and Establishing the Context, which is undertaken by the board and management supported by risk management specialists,

Phase II: Risk assessment and risk evaluation against established criteria which form the basis for the selection of risk treatment options,

Phase III: Implementation of risk treatments using internationally accepted project management methods to monitor performance, and ensure communication of critical information.

Phase III is lead by experienced project managers, and not by risk specialists or line managers who have different roles to perform.

Project managers support management in bringing into sharp focus:

1. Scoping risk treatments required to bring about improvements in planning, controls, infrastructure, supply chain, communications, training, preparedness, resilience etc.
2. Identification of required actions and expected outcomes,
3. Project planning and costing,
4. Performance of people who are assigned measurable tasks,
5. Project performance monitoring (deliverables, milestones, gateways),
6. Project communications,
7. Measurement based return on effort which either confirms or disproves that the desired improvement in risk performance as illustrated in the projected variances between the initial and residual risk maps has been achieved.

Consistency in measurement throughout all three phases, particularly phase II and phase III is achieved through the use of:

1. Proxies which put a structure and a discipline to hitherto loose and sometimes haphazard methods of estimating probability and impact when:
 - a. First assessing risk, and then
 - b. Projecting changes in probability and impact assuming risk treatments are applied as scoped and as planned,
2. Internationally accepted project management methods when applying approved risk treatments across the enterprise.

Companies which consistently operate project management methods already know their value. It is worth noting that confidence in project management methods is also underpinned by the existence of both internationally accepted standards and methodologies and associated post-graduate courses which are available through respected institutes and colleges around the world.



V0.4

Companies which do not formally operate project management methods are unlikely to deny that process in day to day business and operations management is an essential hallmark of a good company. Any resistance to the introduction of project management methods will almost certainly be associated with cultural and change management issues. Whilst material these issues are manageable when clear objectives and a strong leadership approach are applied.

What remains now is the requirement for a standardised method of estimating probability and impact.



3. Methodology for estimating probability and impact:

There is as yet no one established and universally accepted method for calculating probability. This is a profound and fundamental problem which is sometimes compounded by the wildly subjective applications of some of the best known qualitative and semi-quantitative methods for calculating probability.

The RMI ERM Methodology provides a solution. We have adopted a basic method which assures structured thinking when attempting to predict the future.

Background:

1. The laws of probability require:
 - a. Identified events, which occur
 - b. In large numbers, are
 - c. Spread, are
 - d. Independent in their occurrences, and are
 - e. Directly comparable
2. Events which obey these requirements provide frequency data with which probability⁶ can be determined as a number between 0 and 1.
3. Without frequency data, probability can not be determined. The reason that hazard risks are insurable is because frequency data is available. On this basis people who wish to transfer risk can do so as there are others (insurers) who are prepared to accept those same risks for a price (the premium paid) at which they believe they can make a profit.
4. Insurers however will not offer conventional insurance products for those risks for which there is insufficient reliable data. It is generally accepted that the majority of risks (i.e. the totality of that which can occur) greatly exceeds the minority that fall within the proscribed terms and conditions of typical insurance policies.
5. Financial risks on the other hand are managed in the main through controls which have over time become generally adequately proven and are subject to ongoing audit, internal audit and organisational checks and balances.

In addition, certain high level financial risks are treated through the use of financial instruments (hedges, options, futures, derivatives etc) which over time are becoming some sophisticated and reliable.

6. Strategic and operational risks however neither fit the instruments created for financial risk management nor the laws of probability for the hazard risk management.

These risks, together with residual financial and hazard risks require good management and a professional approach.

7. Clearly a substitute for unqualified frequency data needs to be found.

⁶ Probability: the extent to which an **event** (ISO Guide 73 line 3.1.4) is likely to occur. NOTE 1 ISO 3534-1:1993, definition 1.1, gives the mathematical definition of probability as “a real number in the scale 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1.”



Estimating Probability

8. There are some credible clues as to where the solution rests. These include the use of proxies for probability and for impact which when correctly applied with descriptors and associated values have the effect of putting a discipline and extracting a greater value from hitherto very subjective, and often very loosely applied methods of measuring the unknown. For example:

- a. The American Petroleum Institute (API) has developed a security vulnerability assessment (SVA) methodology for which they have come to the view that whereas you can credibly apply the laws of probability⁷ to the estimation of probability of hazard risks you can not apply anything equally credible for estimating probability (API uses the term likelihood) of terrorist attack. They have come to the conclusion that there are three surrogates for probability. It works as follows:
 - i. The surrogates are Threat Characteristics, Vulnerability and Target Attractiveness,
 - ii. The criteria for selection of surrogates is the 'soundness of the logical relationships inherent in the SVA method used to evaluate the input and output conditions'

The use of these surrogates requires knowledge of counter terrorist intelligence and operations. This knowledge allows the user to apply agreed descriptors for each surrogate to which specific values can be applied.

- b. It is interesting to note the consistent inclusion of control efficacy, and time, as factors for consideration when estimating probability in various reports emanating from Top 3 (accountancy) risk management departments,
- c. A simple natural observation which articulates abundant empirical evidence *'If I go out tonight to burgle a house then, all things being equal, I will avoid the house that has both an alarm system and a Rottweiler and pick the house that has neither. On this basis vulnerability (read control efficacy) has a direct influence, either explicit or implicit, on the probability of a particular house being burgled'*

These three examples confirm that control efficacy is a proxy which can be used in the estimation of probability.

Other proxies however do exist. For example the introduction of time and prior experience when using qualitative and semi-quantitative methods tell us that subject matter experts the world over use these two characteristics of probability on a reasonably consistent basis.

The RMI ERM Methodology uses the term Qualitative Probability Estimates (QPE) (patent pending) when describing these other proxies of probability.

The Qualitative Probability Estimates which have been developed by RMI are described as follows:

⁷ Whereas API uses the term likelihood, the RMI ERM Methodology only uses the term probability. This is done as the term likelihood does not exist as a technical term in ISO Guide 73. For this reason we recommend adoption of the ANZ 4360 definition of likelihood as it clearly illustrates the technical difference between the terms likelihood and probability. The requirement to do this becomes evident later in this section where we introduce the term 'Qualitative Probability Estimates'.



V0.4

Probability

We cannot predict the future yet we continue to try and measure that which we cannot see, feel or touch. We do this knowing full well that as human beings we are inherently superstitious and not always rational. These fundamental limitations notwithstanding we do still need to articulate sound and logical assumptions on which to build our plans for the future.

The challenge therefore is to remove the estimation of probability from the influence of ignorance and the human tendency towards lemming type behaviours when asked to comprehend the unknown.

A solution lays with a synthesis of proxies for probability which on the basis of natural observation seem sound and logical in their overall relationships; one with another, and all within the overarching premise of uncertainty.

The RMI methodology applies descriptors and associated values to those descriptors as follows:

$$(P) \text{ Probability} = (E_I \times T \times E_x \times P \times D) \times C / 6$$

This section has been removed from this published version because of its proprietary value to the author and to RMI.

The full version of this paper will be made available to international professional bodies, leading thought leaders and authors.

The criteria for release are moral courage⁸ and comfort when contemplating leaps of thought away from obfuscation and complexity...towards simplicity.

⁸ Napoleon once said *...moral courage is the only true courage...* it is a pity, though not surprising that the quote most attributed to him is *...don't give me a good general, give me a lucky general.* Many (but not all!) lucky generals in the experience of this author have accumulated great fame and great fortune at the expense of humanity and of nature. Some should be in jail, witness the destruction visited since Monday 15th Sept 2008.



Impact

Most events are of themselves non-financial; however most do have direct financial consequences of one kind or another.

Great difficulty arises in estimating impact in terms of direct financial cost. Estimates tend to be made using criteria and methods which are not as rigorous in application as that which goes into sound financial planning. For this reason it is important to establish some standard method with which financial and non financial people alike can make estimates which in the first instance at least are sufficiently sound for the purposes of establishing level of risk.

The RMI ERM Methodology uses the term Qualitative Impact Estimates (QIE) when describing proxies of probability.

The Qualitative Impact Estimates which have been developed by RMI are described as follows
(I) Impact⁹ = Consequences (S x SP x C x O x R x T) / 6

This section has been removed from this published version because of its proprietary value to the author and to RMI.

The full version of this paper will be made available to international professional bodies, leading thought leaders and authors.

The criteria for release are moral courage¹⁰ and comfort when contemplating leaps of thought away from obfuscation and complexity...towards simplicity.

The Formula

The formula P x I is applied where the average of the QPEs generates the value for Probability and the average of the QIEs generates value for Impact

The sum of the two sets of values determines the location of each risk plot on the risk map.

Thus Probability (average score of E_I x T x E_x x P x D x C) X Impact¹¹ (average score of S x SP x C x O x R x T) automatically generates the initial and residual risk map illustrated above.

We now need to turn our attention to the requirement for:

1. Standard language, terms and definitions,
2. Standard ERM framework, principals and risk management process,

⁹ Impacts are both positive and negative

¹⁰ Napoleon once said *...moral courage is the only true courage...*it is a pity, though not surprising that the quote most attributed to him is *...don't give me a good general, give me a lucky general.* Many (but not all!) lucky generals in the experience of this author have accumulated great fame and great fortune at the expense of humanity and of nature. Some should be in jail, witness the destruction visited since Monday 15th Sept 2008.

¹¹ Impacts are both positive and negative



4. Universal language, terms and definitions:

There is as yet no established and universal language which can be applied across all classifications of risk. This is a profound and fundamental problem.

The RMI Methodology provides a solution as we use only those terms and definitions which have been determined by predominant international standards and professional bodies. Consequently:

Term(s) and Definitions(0)	International Body	Comment
Risk Management	ISO ¹²	ISO Guide 73: Risk management —Vocabulary — Guidelines for use in standards, In addition ISO Guide 51 (Safety) is similarly adopted,
Enterprise Risk Management	COSO ¹³	ERM is defined in the publication <i>Enterprise Risk Management—Integrated Framework: Executive Summary Framework</i> , the Committee of Sponsoring Organizations of the Threadway Commission (COSO) as: 1. “A process, ongoing and flowing through an entity 1. Effected by people at every level of an organization 2. Applied in strategy setting 3. Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk 4. Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite 5. Able to provide reasonable assurance to an entity’s management and board of directors 6. Geared to achievement of objectives in one or more separate but overlapping categories.”
Risk Classifications ¹⁴	Institute of Management Accountants	<p>“Strategic Risks – examples include risks related to strategy, political, economic, regulatory and global market conditions; also could include reputation risk, leadership risk, brand risk, and changing customer needs.</p> <p>Operational Risks – risks related to the organization’s systems, processes, technology, and people.</p> <p>Financial Risks – includes risks from volatility in foreign currencies, interest rates, and commodities; also could include credit risk, liquidity risk, and market risk.</p> <p>Hazard Risks –risks that are insurable such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism.”</p>

¹² The International Organization for Standardization

¹³ Committee of Sponsoring Organizations of the Threadway Commission

¹⁴ Enterprise Risk Management, IMA SMA on Frameworks, Elements and Integration submitted to the US SEC on Jan 25th 2007



V0.4

Operational Risk ¹⁵	Institute of Management Accountants	Risks related to the organization's human resources, business processes, technologies, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration,
Operational Risk Program	Bank International Settlements, Basel	A program, which includes qualitative and quantitative steps which not only enhance resilience from attack, but also which support critical assurance goals
Likelihood ¹⁶	ANZ ¹⁷ 4360	Likelihood: used as a general description of probability or frequency NOTE: Can be expressed qualitatively or quantitatively.

¹⁵ Enterprise Risk Management, IMA SMA on Frameworks, Elements and Integration submitted to the US SEC on Jan 25th 2007

¹⁶ As likelihood is not included in ISO Guide 73 we recommend the adoption of the term as provided in ANZ 4360

¹⁷ Australia and New Zealand Standard

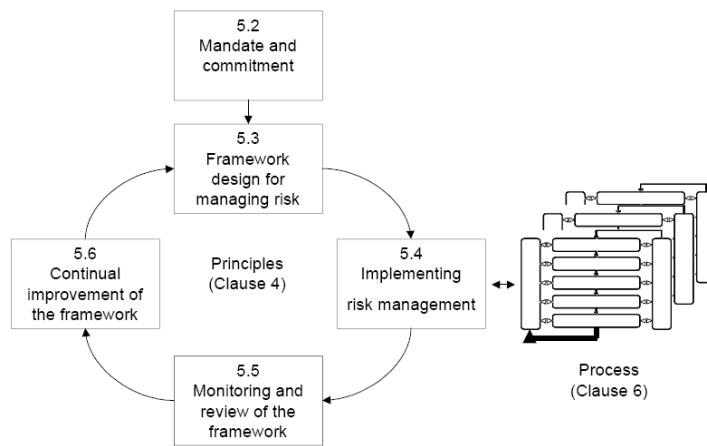
5. Standard ERM framework, principals and risk management process:

There is as yet no one established and universally established best practice or international standard which can be applied across all classifications of risk. This is a profound and fundamental problem.

The RMI ERM Methodology provides a solution as we have adopted the anticipated ISO 31000 (risk management)¹⁸ as the universal best practice ERM framework when finally published.

This standard (draft) recommends a:

- a. Framework approach,
- b. Eleven (11) principals, and
- c. A risk management process.



146

©ISO

The risk management process (process clause 6 above) which is already known and proven is the AS / NZS 4360 Risk Management Process.

ISO 31000 (Risk Management) Draft recommends ISO Guide 73 and ISO Guide 51 mentioned earlier in this section.

The RMI ERM Methodology provides a solution through:

1. A life cycle approach (described below) which includes 3 phases, 3 milestones, 2 Gateways, 12 deliverables, and over 80 discrete tasks and sub tasks. When correctly applied the RMI ERM Methodology ensures effective enterprise risk management using the anticipated¹⁹ international best practice standard ISO 31000.
2. The recommendation that HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004 is used by managers when assessing, evaluating and treating risks,

¹⁸ Due for release June 2009

¹⁹ In the meantime ANZ 4360 provides the basis for an internationally accepted risk management standard which in any event is the platform on which ISO 31000 is being developed.



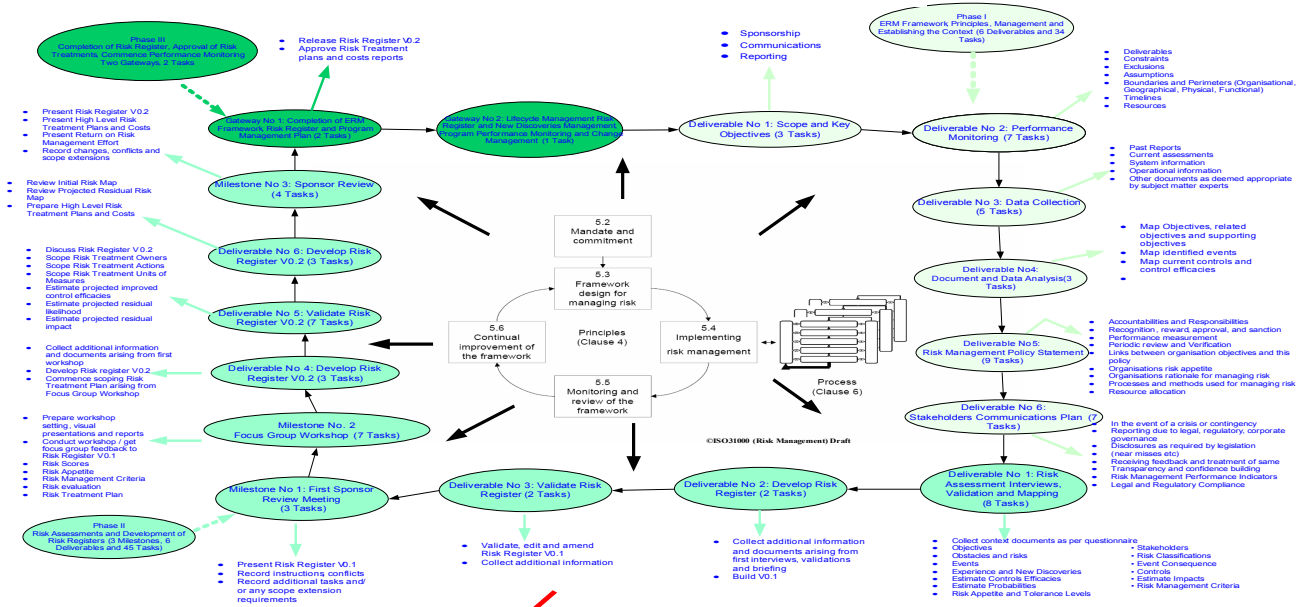
V0.4

3. The RMI ERM Register. The register is built on MS Excel and has the following characteristics:
 - a. Format for data capture which:
 - i. Adheres to the ISO 31000 risk management process, and which
 - ii. Makes visible the output from deliverables and tasks.
 - b. Drop down descriptors and values for risk classification, QPEs and QPIs,
 - c. High level project plan depicting risk treatment, owners, actions and units of measure.
 - d. Automated:
 - i. Calculation of risk scores,
 - ii. Calculated Levels of Risk,
 - iii. Population of Initial Risk Map,
 - iv. Population of Residual Risk Map,
 - v. Generation of reports as follows:
 - a. Summary of initial risks,
 - b. Summary of residual risks,
 - c. Top 30 risks, at all levels,
 - d. Top 30 risks by level,
 - e. My objectives and controls,
 - f. My objectives ad actions,
 - g. My risks and actions,

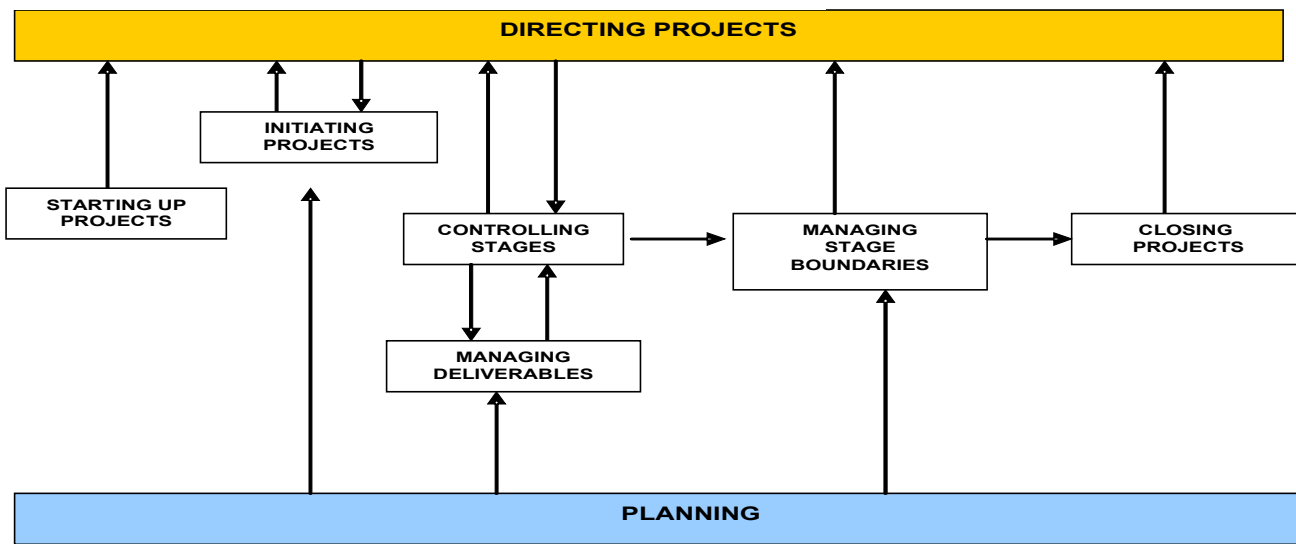
Section 4

RMI ERM Methodology Process Flow

RMI Enterprise Risk Management Methodology



Project Management Methodology



Responsibilities Project Manager Risk Management Programme Office

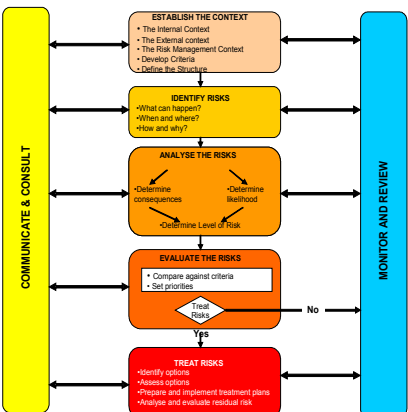
- Report directly to Risk Committee
- Oversight: Run Risk Treatment projects on a day-to-day basis
- Manage production of deliverables
- Manage and motivate teams of specialists
- Plan and monitor Risk Treatment projects
- Produce plans, reports and documents
- Manage project risks, corrective actions and contingency plans
- Prepare end-of-projects follow-on actions

Programme Quality

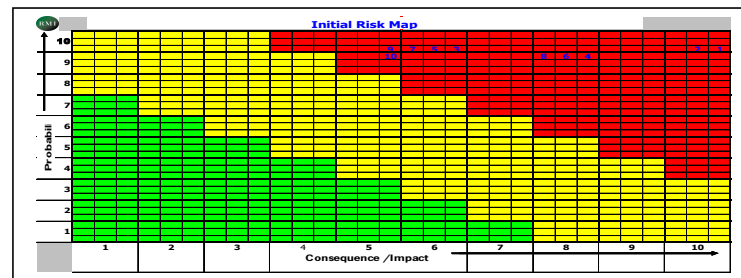
- The methodology includes:
- Checkpoint reports
 - Highlight reports
 - Exception reports

The Programme Office Risk Treatment Quality Plan generates monitoring profiles showing frequency of:

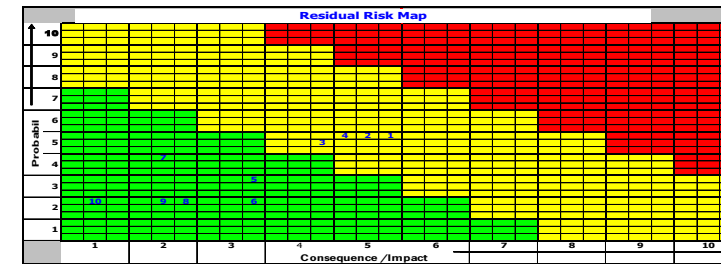
- Reports
- Meetings
- Document Reviews
- Project Plan Reviews
- Project Risk Reviews



Reproduced with permission from SAI Global under copyright Licence; AS/NZS 4360 may be purchased from www.saiglobal.com



Return on Risk Management Effort





V0.4

Peadar Duffy, having served 15 years as an officer in the Irish Defence Forces, Peadar is Founder and Chairman of RMI which he established in 1993. Peadar's experience spans many risk management disciplines including critical infrastructure protection, scenario planning and development, and the development of risk management programs across large organisations.

Peadar spent much of the period 2001-2005 in the US where he undertook considerable research into the areas of enterprise risk management and the development of methods of identifying major risks with potential to destroy value. Much of the research has involved the global insurance and risk management players in Chicago, Washington DC and New York who in recent years have discovered that typical hazard / insurable risks rarely destroy company value.

Peadar has a special interest in the identification and management of 'known unknown' risks. These are risks which are typically recognised by company managers but which when they do occur come as a surprise to senior company leadership. Many of these risks are associated with infrastructure and global interdependency issues in the fast moving and uncertain world in which we live.

Peadar recently located to RMI's Middle East Regional office in Bahrain from which RMI has established a leadership position providing a range of risk management services to many Petrochemical, Government Ministry and major Utility companies in the region.