

Andrew Graham

Integrated Risk Management

Implementation Guide





Andrew Graham

Website: <http://post.queensu.ca/~grahama/>

E-Mail: Andrew.Graham@queensu.ca

Andrew Graham researches, teaches and writes public sector management, financial management, integrated risk management and governance. He teaches at **Queens University School of Policy Studies** as well as its **Industrial Relations Centre** and the **Canadian Police College**. He is a research associate of **The Conference Board of Canada**, having completed a variety of studies on strategic planning, financial and human resource management and risk management

He has recently published the first textbook on managing public money, entitled, ***Canadian Public Sector Financial Management***, available through McGill-Queens press at <http://mqup.mcgill.ca/book.php?bookid=2079>

Mr. Graham teaches in both the graduate and professional development programs at Queens and elsewhere. He also writes extensively, now writing a regular column on management issues, ***Briefly Noted for the Public Management***, a periodical of the **Institute of Public Administration of Canada**.

Mr. Graham has focused much of his academic work, combined with his considerable experience in complex organizational management, in risk management. He has participated in several studies on implementing risk management in business and government for the **Conference Board of Canada**. He regularly teaches risk management workshops at the **Canadian Police College** and the **Industrial Relations Centre, Queens University**. He presents to conferences on a regular basis on risk as well as the governance of risk.

An Assistant Deputy Minister for 14 years in the federal government with over 30 years of service, he has experience in line operations (Warden of Kingston Penitentiary), leading a complex regional operations, and a number of policy and corporate leadership roles, including Senior Deputy Commission of the Correctional Service of Canada. He has extensive corporate management experience, including having served as the ADM, Corporate Services of Agriculture and Agri-Food Canada.

Table of Contents

1. Using this Guide

- Who this Guide is For
- What the Guide Does
- No One Size Fits All
- You Set the Pace
- Risk is Not Scary: It is Essential
- Organization of the Guide

2. The Business Case – Why IRM?

- What This Section Does
- External Drivers for Implementing IRM
- A Brief History of Risk
- Why Risk Management?
- Defining Risk and Risk Management
- Why Manage Risks?
- Are You Risk Fit?
- How To Convince Your Organization to IRM on Board
- Some Winning Strategies

3. How an IRM Systems Works

- What this Section Does
- A Systematic Approach to Risk Management
- The Risk Management Model
- Linking Risk Management and Business Operations and Planning
- Identifying the Risks Informs How You Will use Risk
- Listening to the Silence: A Special Challenge
- Ignoring Your Shop Floor at Your Peril
- Risk In Bundles: Categories of Risk
- Characteristics of Integration

4. Implementation

- What This Section Does
- The Questions to Ask and Answer
- The Key Decisions Guiding the Implementation of IRM
- To Pilot or not to Pilot
- A Phased Approach
- The Steps in Implementation
- Take a Sound Time Perspective

- Creating a Risk Management Policy
- The Role of Leadership
- Assigning Responsibilities
- Sample Implementation Plan
- Idea Marketplace: Some Leading and Learning Practices in Implementing IRM
 - Focus on Culture
 - Risk Championship
 - Risk Tolerances
 - Communications
 - Teams and Committees
 - Develop and Use a Common Language Set
 - Establishing a Corporate Risk Management Function
 - Communicating Risk Management Performance
 - Guidance
 - Training
 - Tools and Techniques for Putting Risk Management into Practice
- Appendix: Sample Integrated Risk Management Policies

5. Using Risk Tools

- What This Section Does
- Certain Maxims About Process
- Risk Assessment
- Making Risk Assessment Real
- Risk Ranking and Evaluation
- Risk Tolerances and Risk Appetite
 - What is Risk Tolerance?
 - How Do You Establish Risk Tolerances?
 - Creating a common Grid
 - Using Key Organizational Objectives
 - Use What You Already Have
 - Seek Out Industry Standards
 - Trial and Error
- Risk Evaluation Formats
- Analysis and Evaluation
 - Setting Priorities: Risk Maps and Decision-Making
- Risk Registers and Summary Reports
- Risk Reports
- A Closing Comment about Forms

6. Managing the Risks: An Overview of Strategies

- What This Section Does
- General Approaches
 - Low Impact/Low Probability
 - High Impact/High Probability

- High Impact/Low Probability
- Low Impact/High Probability
- Risk Mitigation Strategies
- Tolerating Risk of Self-Insurance
- Prevention
- Reduction
- Control
- Transfer
- Prepare
- Risk Management and Good Governance

7. Risk Communications and Reputation Protection

- What This Section Does
- The Risk Communications Conundrum
- Building Credible Risk Communications
- Risk Communications Failures
- Determinants of Reputation Risk
- Managing Reputation Risk
 - Assess
 - Evaluate
 - Close Gaps
 - Monitor
 - Find an Organizational Locus
- Planning Your Communications Approach

8. Risk Resources and Sources

- Websites
- Books
- Articles
- Standards

9. Questions and Answers

Section I: Using this Guide

Who Is the Guide For?

This guide is intended for anyone interested in implementing integrated risk management (from now we will call it IRM here – you can call it by whatever title works for you) in their organization, be it a private company, a voluntary organization or a governmental unit or department. It is designed to focus as much as possible on the steps needed to convince an organization that it needs IRM, to show one prototype of a risk assessment and mitigation process that can be readily adapted and to address the issues of aligning the organization, getting in place the governance and training to sustain IRM over time.

The people that are involved in these processes are the target audience. Therefore, they could be:

- Senior managers trying to determine the benefits and best ways to start,
- Operational managers trying to demystify IRM for themselves and their staff,
- Line staff trying to figure out what the consultants, staff responsible for implementation and their bosses are talking about, and
- Staff and managers charged with implementing IRM.

The focus therefore is on managers, both those involved in the operational side of the organization and those involved in various staff and control functions, such as finance, strategic planning and human resources. IRM only works when all are involved and there is effective buy-in on all sides.

What the Guide Does

In a sense, the various sections will have different benefits depending on the perspective that the reader brings to bear. In addition, there is a logical set-up that reflects the need to lay out the entire implementation picture. That always starts with what you want to achieve, not how. Consequently, there is a section that deals with what some would call the theory of risk and integrated risk management. One of the reasons for doing this is to ensure that you get the integrated into integrated, i.e. gets all the inter-connecting elements in place. Hopefully, there will be enough useful material for those involved in this to use when making their own presentations. For that reason, take-out boxes will also have useful quotations or points to remember. Much of the challenge in implementing IRM is the selling of it.

One of the challenges in outlining the implementation of IRM is that it has two faces:

- A focus on developing an organized approach that involves the integrated part of the title: this means setting up a policy, a governance structure, building linkages to existing business process and assigning responsibilities, and

- A focus on the substantive elements of risk management itself: notions of risk and what it is and is not, risk assessments, risk tolerances, risk mitigation and monitoring.

This guide will address both elements in detail. It will take the overall approach for each section:

- An overview in text
- Examples and leading practices,
- Checklists to test performance or assess situations
- Charts to map processes where possible.

In each case, this material is meant to provide information to the reader, but to also be of some use to the reader as implementer. While the text will emphasize the need to develop home-grown solutions, or, at least, processes and solutions that fit well into the culture of an organization, there is no need to reinvent the wheel here. Many organizations around the world have successfully implemented IRM. There is a lot to learn from them.

Idea Source: What's That? Throughout the Guide you will see text boxes with the heading Idea Source. These are ideas, tips and good quotations picked up from many interviews and discussions that the author has gathered over the course a much research in this area. They are designed to give you quick ideas, vignettes or key messages that will assist in explaining IRM, defining the key points or using a much needed argument to make your point. Some of the quotations will not be attributed as they were part of research projects in which anonymity was promised.

No One Size Fits All

One might well accuse the author of delivering a mixed message in this guide. The first is that IRM is an integrated system. Therefore, only with all elements in place will it work effectively for an organization. That being said, there are different ways to achieve that integration. Size and complexity are factors governing this to some extent. The reason for this approach is that this Guide and its author do not endorse any single IRM (or ERM) package from any one company. Organizations do well to set their own course. If they find useful software packages or are comfortable with the proposals of a particular consultancy firm to help implement IRM, that is their decision. Well managed organizations make decisions like this all the time.

As well, language can vary depending on the organization and its objective. The guide will use the term organization as a generic reference to businesses, government departments and agencies, not-for-profit organizations large and small. The spread here is wide. Therefore, at times there will be talk of impact on profit or business. At others there will be consideration of achieving objectives within a public sector context.

Experience and research have shown that there is very little difference between public and private organizations when it comes to IRM. The content may be different and some emphasis will be the same, but the core elements remain constant:

- Developing a consistent approach, call it a policy, directive or procedure,
- Applying risk management techniques in a consistent way across the organization,
- Developing tools that include:
 - Definitions of risk,
 - Risk assessment tools and processes
 - Risk evaluation and prioritization tools and processes
- Procedures for the regular review of risks and determination of risk mitigation at a senior level
- Reporting, communicating and follow-up.

Idea Source:
“A decision that does not involve risk is probably not a decision”

You Set the Pace

How these elements are implemented will vary considerably across organizations. Similarly, even what you call this whole process – which we in the Guide will call Integrated Risk Management, IRM – depends to a large degree on context. It also depends on what drivers or key sources of approval, authority or accreditation, your organization has to satisfy. Therefore, a mid-sized firm will want to ensure that the accounting standards that it follows to assure its owners of proper standards of reporting being followed may require that a risk management system be firmly in place. Increasingly, public-help companies, pursuing compliance with such legislation as Sarbanes-Oxley and Basel II, will want to have demonstrable risk management system. Governments increasingly are mandating their various departments and agencies to put in place risk management systems with specific guidance in some cases.

This Guide speaks in a generic way to each of these circumstances.

Risk is Not Scary: It is Essential

As a going-in proposition, we have to set aside a couple of notions, which we will also explore in more detail further on. The first is that risk is something that should frighten us, to be avoided at all costs and preferably left under a rock where the sun never shines. Of course, the reality is that risks have a life of their own that you can face at your pace or theirs. Risk is opportunity. Risk is also a vital signs issue. If you do not have risks, you are not really in the real world. Rather than being frightened of them, they need to be uncovered, exposed, and managed.

The second issue is that risk management is not the equivalent of crisis management. Bottom line: if you are always in crisis

Idea Source:
“Statistically speaking, there is a far greater chance of being run over by a motor boat than being eaten by a shark. The reality, though, is no one will ever make a movie called ‘Propeller’”
-- Kirk Smith, East-West Center of Hawaii.

management, you were never in risk management. There is no guarantee that organizations will prevent all crises with effective risk management. They certain will reduce the number and increase their overall capacity to effectively manage crises when they do occur.

Organization of the Guide

The Guide marches through the basic ideas of IRM. However it does so with the idea that what is being presented here could be adapted for internal use within your organization either in making presentations about risk management or in developing training material. So we begin with looking at the business cases for IRM, centering again on how to sell it as much as why. Then follows what IRM is. Core message: it's a full meal deal and if you start, finish. After that we look at implementation. From there we look at the various risk reports and formats that you should make part of your system. Here again, we try to offer some options as organizations really need to adopt their own look and feel. We will briefly touch on risk management strategies. Here we will focus on typologies, i.e. general approaches, rather than specific solutions. One reasons is that there are so many, most of which are really inherent to any well managed organizations. The other is that solutions have to be part of the organizational culture that you work with and try to build into the future. So, after all this process, no quick fixes. Sorry. We will end with two sections of helpful material. One is a resources section, focusing on website, books and articles. There is plenty out there. Google at will. The other is a series of Questions and Answers for commonly posed questions about IRM gleaned from many conversations and readings.

Idea Source: How is Risk Management Different from Every Day Good Management? “Risk manage is different than traditional management because it allows us to examine what is missing in our routine business process, and why those missing elements expose us to risk. Risk management encourages better up-front planning and allows us to determine if our polices and capabilities are well aligned to the strategy we desire to executive. It also facilitates post evaluation to help assure improvements actually occur as intended.”

- Bob Busch, Vice President Newell Rubbermaid, from Enterprise Risk Management in Practice: Profiles of Companies Building Effective ERM Programs, Protiviti, www.protiviti.com

Section 2 – Building the Business Case

What This Section Does

Before anything can happen in implementing IRM, some basics have to be completed. Senior management has to understand what the scope of IRM is, see it as a desirable and necessary part of its management strategy and decide to move forward. Otherwise, advocates for IRM will be left adrift and waste a lot of time, energy and focus continually testing commitment. This section provides background to build the business case. Because IRM involves concepts of risk, there is a need not only to develop a desire to move forward, but also a need to be clear about the what it is you are moving forward on. Therefore, the section has a number of parts to assist in this:

- External Drivers
- A Brief History of Risk
- Risk, its meaning
- Integrated Risk Management – what’s that
- Responsibility for IRM
- Checklist: are you risk fit?
- Selling IRM: pointers, speaking notes, arguments for and against.

***Idea Source: “A pessimist believes that nothing can be done. An optimist, on the other hand, believes that nothing can go wrong. A realist knows that something can go wrong, but that the situation can be managed. Risk management is realism, and it acts as a necessary counterbalance to an organization’s other best resource: optimism.”
- European Agency for Safety and Health at Work Risk Management Toolkit***

While there are many external drivers to implement a formal IRM system within most organizations, it is only going to happen when senior management and the rest of the organization buy in. This does not mean that they convert to some new salvation for the organization. IRM is not about that. Rather, they must come to see the value of IRM, accept that creating and operating it will require focused attention and resources, and get on with it. This section outlines some of the thinking behind IRM, provide some definitions and outlines and then focuses on two key elements of successful IRM implementation:

- Assessing the organization’s present state of risk management capacity, also know as its **risk readiness**,
- Finding ways to sell IRM within the organization.

External Drivers for Implementing IRM

In many cases, executives and managers in both public and private organizations do not need to be reminded of a stream of incidents over the past twenty years that have driven both governments and key accounting standards boards around the world as well as organizations concerned with corporate governance to push for a formal system of risk management as part of the array of tools that make up good corporate management. Many tend to dwell on scandals such as Enron in the United States and

Barrons Bank in the United Kingdom as wake up calls for risk management. Within government, various themes around the world that emphasize better managerial practice, call it public service modernization in Australia or modern controllership in Canada. Within the specific context of various industries and governments, these iconic events are well known. It has been argued that many organizations have not effectively managed their risk situations or not exposed them to scrutiny in such a way that mitigation would either be openly embraced or forced through external or board pressure.

In response to this an IRM industry has arisen around the world. Firms totally devoted to helping organizations implement risk management abound. All major consulting operations have a risk management focus. Large corporations may also appoint a **Chief Risk Officer** as part of the executive team. There is also IRM software available. Good risk management has become part of what is expected of a well managed organization.

It is, however, useful to remember that the concept of IRM has been in development for almost a century now. This development reflects the increasing complexity of modern organizations and the world in which they operate. It also reflects the increasing sophistication in intelligence gathering, in the capacity of stakeholders to understand and assess organizational management and in the potential impact of loss or failure of key systems. Therefore, in setting some of the context, the following section on a brief history of risk is presented to help those considering it and those promoting it to an organization understand the context a little better.

Brief History of Risk¹

The idea of risk management took some time to develop. It emanates from the sense that a logical, consistent and disciplined approach to an organization's uncertainties will allow it to deal with them prudently and productively, avoiding unnecessary waste of resources. It goes beyond faith (e.g. pray) and luck (e.g. buy a lottery ticket), the twin pillars of managing the future before we began learning how to measure **probability**, a key idea in thinking about risk. As Peter Bernstein wrote in his book, **Against the Gods: The Remarkable Story of Risk**, (1997): "If everything is a matter of luck, risk management is a meaningless exercise. Invoking luck obscures truth, because it separates an event from its cause." What has happened in the past century is that we have become more and more capable of applying thinking about probability to risk and acting upon it.

The 20th century had more than its share of destructive wars and a wide range of natural and environmental disasters. It was also the first century in which information about them could be spread instantaneously around the world. It would be dangerous, however, to assume that thinking about risk management, about actually looking into

¹ This material is adapted from Risk Management Milestones: 1900 to 1999 by Felix Kloman, Sourced at: <http://www.irmi.com/Expert/Articles/2001/Kloman03.aspx>

the future, applying common sense and sophisticated analysis to establish probabilities and taking some actions to mitigate undesirable outcomes, is simply a reaction to these. Rather, what the century also saw was a growth in intellectual capacity around key elements such as game theory and probability theory that showed that this kind of projection could actually be done and could be meaningful. So, when the stage was set at the end of the 20th century with a series of private sector scandals along with major changes within government such as downsizing and outsourcing, a lot of framework was in place to create an expectation that organizations should be doing better risk management. Some of these developments will, in fact, surprise.

1905-1912 The creation of workers' compensation laws in Europe and the United States signaled that it might be possible to mitigate against personal disasters.

1920 The formation of the first captive insurance companies to insure the risks of a parent company. Captives illustrate the idea of prudent internal financing of risk, as compared to trying to shift it outside the organization.

1921 Frank Knight publishes **Risk, Uncertainty and Profit**. Knight separates uncertainty, which is not measurable, from risk, which is.

1921: A Treatise on Probability, by John Maynard Keynes, appears. He emphasizing the importance of relative perception and judgment when determining probabilities.

1926: John von Neumann and Oskar Morgenstern publish **The Theory of Games and Economic Behavior**.

1952 *The Journal of Finance* publishes "**Portfolio Selection**," by Dr. Harry Markowitz. It explores aspects of return and variance in an investment portfolio, leading to many of the sophisticated measures of financial risk in use today..

1956: *The Harvard Business Review* publishes "**Risk Management: A New Phase of Cost Control**," by Russell Gallagher.

1962: In Toronto, Douglas Barlow develops the idea of "**cost-of-risk**," comparing the sum of self-funded losses, insurance premiums, loss control costs, and administrative costs to revenues, assets and equity.

1965: Ralph Nader's **Unsafe at Any Speed** appears and gives birth to the entire consumer movement, first in the U.S. and later moving throughout the world. The ensuing wave of litigation and regulation leads to stiffer product, occupational safety, and security regulations in most developed nations.

1966: The Insurance Institute of America develops a set of three examinations that lead to the designation "Associate in Risk Management," the first such certification.

1973: The Geneva Association holds its first Constitutive Assembly and begins linking risk management, insurance and economics.

1974: Gustav Hamilton, the risk manager for Sweden's Statsföretag, creates a "**risk management circle**," graphically describing the interaction of all elements of the process, from assessment and control to financing and communication.

1975: The American Society of Insurance Management changes its name to the **Risk & Insurance Management Society (RIMS)**

1975: The first major risk analysis study, **WASH-1400** which analyzed the 45 weeks of nuclear power plants was published by the Nuclear Regulatory Commission.

1976: With the support of RIMS, *Fortune* magazine publishes a special article entitled "**The Risk Management Revolution**". It suggests the coordination of formerly

unconnected risk management functions within an organization and acceptance by the board of responsibility for preparing an organizational policy and oversight of the function

1980: The Society for Risk Analysis is formed in Washington to represent public policy, academic and environmental risk management advocates. **Risk Analysis**, its quarterly journal appears the same year.

1983: William Ruckelshaus delivers his speech on "**Science, Risk and Public Policy**" to the National Academy of Sciences, launching the risk management idea in public policy.

1986: The **Institute for Risk Management** begins in London. That same year Dr. Vernon Grose, a physicist, student of systems methodology publishes **Managing Risk: Systematic Loss Prevention for Executives**, a book that remains one of the best, and clearest, primers on risk assessment and management.

1992: The **Cadbury Committee** issues its report in the United Kingdom, suggesting that governing boards are responsible for setting risk management policy, assuring that the organization understands all its risks, and accepting oversight for the entire process. Its successor committees (Hempel and Turnbull), and similar work in Canada, the U.S., South Africa, Germany and France, establish a new and broader mandate for organizational risk management.

1993: The title "**Chief Risk Officer**" is first used at GE Capital, to describe a function to manage "all aspects of risk," including risk management, back-office operations, and business and financial planning.

1995: A multi-disciplinary task force of Standards Australia/Standards New Zealand publishes the first **Risk Management Standard, AS/NZS 4360:1995** (since revised several times), bringing together for the first time several of the different sub-disciplines. This standard is followed by similar efforts in both Canada and Japan (1997).

1996: The **Global Association of Risk Professionals**, representing credit, currency, interest rate, and investment risk managers, starts.

What this brief run-down shows is that much thinking about risk began in areas such as insurance, games theory and finance. However, as it emerged and with the increasing involvement of real executives in industry and government, the concepts of risk, combined with the new analytical capacities that had been developed, made the use of risk as a management tool inevitable.

Why Risk Management? What it is and the Business Case for It.

What makes risk management different from good management? The first thing you will hear when this topic comes up is: "We all do risk management here. How do you think we get through the day?" True, but, does everyone know what they mean by risks. Often there is confusion between risk and problem solving. As well, is everyone signing from the same song sheet: a common understanding of any word is hard enough. With something like risk, in the absence of a common approach, policy and use, the definition is in the eyes and ears of the user.

Risk management is an inherent part of good management. It requires an agreement on an approach integrated with corporate strategy that outlines exposures, issues and potential problem areas. It makes it explicit. In addition, IRM creates a system, not dissimilar from regular organizational performance review (and, hopefully, as part of it) where you look not just at performance and events, but identify, in a systematic way, important gaps, variations and exposures that let you get ahead of their possible impact, i.e. mitigate. Risk management is different from traditional management because it allows the organization to examine what is missing in the routine processes and why those missing elements expose the organization to risk. It encourages better up-front planning. It also equips the organization to assess if its policies and capabilities are adequately aligned to the desired strategy.

For the purposes of explaining what risk management is, here are your **key messages** about risk:

- Risk is about the future
- Risk is based on the notion of probability of an event happening
- Risk is then assessed in the intensity or impact of that event
- Once you decide on probability and impact you can then compare various risks you are facing and set priorities.
- After that it is all about mitigating, managing and controlling your risks.

Sounds easy, right? Well, experience across governments and the business world has shown that the hurdles are as much about understanding risks as they are managing them. So, most organizations spend a lot of time sorting out their understandings of risk. Experience has also shown, as we will discuss in the implementation section, will experiment with the language and emphasis they want to have on risk before they get it right.

Idea Source: "Risk management must be opportunistic. Even in the throes of disaster, we should seek possible strategic advantage for our stakeholders. This means understanding that risk embodies both favorable as well as unfavorable unexpected outcomes. Risk management is a technique for improving our risk taking. This idea is hardly new. Jacques Bernoulli, one of the fathers of the art of probability, suggested the same theme in 1713, in his Art of Conjecture. Adam Gopnik confirmed this understanding in a recent article in The New Yorker ("Read It and Weep," August 28, 2006) when he wrote, "Terror makes fear, and fear stops thinking." If we look only at possible downside results, we create fear, and then we stop thinking rationally. We become risk averse, crippling initiative. Risk aversion leads to a narrowed focus, then self-assurance, and finally the absence of doubt and curiosity. This is the death knell for any organization"

- The Future of Risk Management, Again, Felix Kloman at <http://riskreports.com/protected/archive/rmr1006.html>

Defining Risk and Risk Management

You will find no end of definitions of risk management in the world. In fact, a Google search will yield 3.8 million hits and its definition section will offer 20 choices. That speaks to the need for your organization to know what it is talking about. The choice of how you define risk will also drive the way in which you approach it. Some will focus on the possibility of loss or threats to the organization. Others will be concerned about financial issues. Others will deal with errors or the possibility of mistakes being made. Some will focus on public reactions, stakeholder interests or political embarrassment. Complex organizations will have to deal pretty well all of these. Be careful how you define risk. Avoid being entirely negative. A focus on error or threats alone will certainly lead to a focus on controls and risk avoidance. This may well cost the organization some opportunities or possibilities to actually use risk management to effectively advance their objectives and even improve on them. Not all risk is bad.

For that reason, this Guide has adopted a balanced view of risk.

Definition of Risk

An event or circumstance in the future that could significantly enhance or impede the ability of an organization to achieve its current or future business objectives.

Here are few more that have been in use through standard setting bodies:

Australian and New Zealand Public Sector Guidelines for Managing Risk (HB 143:1999) defines risk as the "chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood."

The Canadian Institute of Chartered Accountants defines risk as "the possibility that one or more individuals or organizations will experience adverse consequences from an event or circumstance."

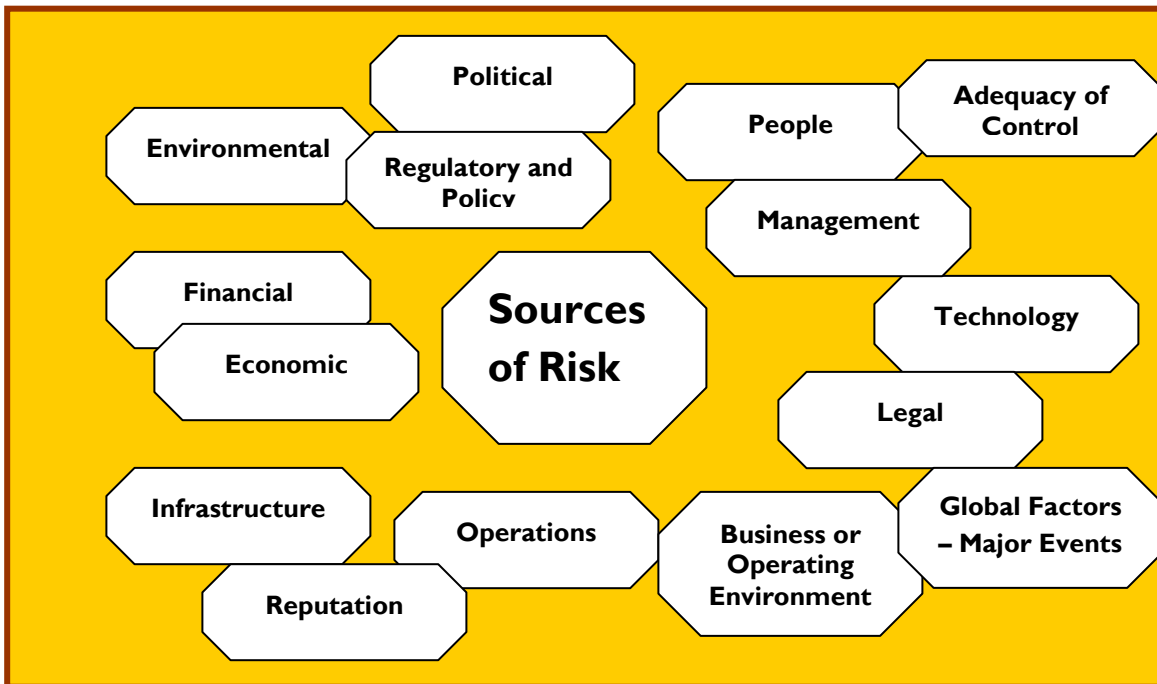
The **Canadian Standards Association Risk Management: Guidelines for Decision-Makers** (CAN/CSA -Q850-97) defines risk as "the chance of injury or loss as defined as a measure of the probability and severity of an adverse effect to health, property, the environment or other things of value."

We will be discussing extensively in **Section 5, Using Risk tools** for identifying risks, setting risk tolerances, weighing and prioritizing.

Risk can come from many sources, sometimes unexpected. In developing analytical tools for the organization, it pays to cover all the bases. As we will see when we discuss the

need for an integrated approach, many sources cross organizational lines and affect the whole organization. However, there is another reason for analyzing risk using a source lens. Such a set of categories force people who may have seen risk in terms of their immediate concerns or have disregarded what some call the 'big picture' issues as irrelevant to the day-to-day and, as a bare minimum identify them and discuss them. The following chart provides a list of various sources, not all of which are applicable to any one organization all the time. However, in starting up, you may not acknowledge all the sources that emerge over the developmental process. This chart will be reflected in the **Vulnerability Analysis** forms that will be discussed in **Section 5, Using Risk Tools**.

Sources of Risk



Why Manage Risks?

Risk is good. It creates opportunities. It forces an organization to look at events or weaknesses in terms of its objectives. It also makes an organization aware of its vulnerabilities and pushes it to do something about them. You cannot claim that all risks will ever be eliminated. That is foolhardy and unrealistic. However, having a systematic approach to risks, which is the essence of risk management, guarantees that you will have the tools to reduce the negative effects to the best extent possible and identify the potential for positive use of risk. Of course, in these days of increased oversight and accountability, it also demonstrates sound management and is increasingly an expectation of boards, oversight and standards setting bodies and governments and their external auditors.

Definition of Risk Management

Risk management is the process of managing risk through the following steps:

- **Understanding the risks to the business**
- **Building vigilance into the organization in a systematic way through effective controls, operational measurement and strategic scanning**
- **Creating a culture that encourages effective risk identification, mitigation and monitoring,**
- **Orderly management of the process**
- **Linking risk management to rewards and resourcing**
- **Communicating to the organization, its stakeholders and owners.**

In Section 6, **Managing Risks**, we will be reviewing a variety of risk management tools. Section 7, **Risk Communications and Reputation**, will focus on the later elements of this definition.

Integrated Risk Management (IRM)

The systematic application of risk management has many names. One often hears the one adopted here, Integrated Risk Management. But there is also Enterprise Risk Management. Many names are on offer. Choose the one that works for you. But the choice of integrated is deliberate. Risk management cannot be seen as a new management system, existing independently and separated from the way in which your organization manages itself, makes decisions, allocates resources and holds people accountable.

The focus of this Guide and much of its rationale that you will see unfold is that risk management cannot exist alone and be effective for the organization. Further, risk management cannot take place in only some parts of the organization (what we would call vertical silos) and not others. However, it cannot also take place at some levels and not others (what we would call horizontal silos.) Many of the earlier risk frameworks stood by themselves, and thus tended to be implemented within functions. Therefore, you will see risk management applied to finance exclusively or to project management, just to name a few. Further, risk management tools and measures apply in a wide range of technical and scientific fields. As a result, many risk management practices have been implemented in silos, i.e., in one part or one function, of the organization. Consequently, risk management may be done very well in one section, but not consider how actions of other parts of the organization affect their risks, or it might not capture the overall significant risks that the organization faces. *Integrated Risk Management* requires an enterprise-wide perspective of risk and standardizes terms and concepts to promote effective implementation across the organization

Some of the important elements of IRM are:

- It is a continuous and systematic process to understand, manage and communicate risk from an organization-wide perspective.
- It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives.
- It integrates the risk management process into the planning and decision-making of business processes and aggregates all types of risk across the organization, and monitors and manages risk on a comprehensive basis.
- An inherent part of sound corporate management.
- It is integrated into the organizational governance process

Managing risk in an integrated way can mean everything from using financial instruments to managing specific financial exposures, from effectively responding to rapid changes in the organizational environment to reacting to natural disasters and political instability or changes in direction. Within this wider understanding of integrated risk management, three competencies are especially important.

- **Financial risk management:** Accurately evaluating market, liquidity and credit exposures and proposing courses of action to buffer the risks. In addition, it entails projecting spending patterns against budget to make course corrections that could threaten budgetary discipline. .
- **Operational risk management:** Continuously assessing the effectiveness of internal controls, measuring and identifying weak areas to mitigate the risk of failure of those controls. It also entails the observant use of operational data to identify risks and potential opportunities for system improvement.
- **Strategic and business risk management:** Assessing risks related to planning and management processes that support an organization's business plan and model; evaluating the impact of external and internal variables, such as market dynamics and major events.

These competencies also form the basis for an overall framework for integrated risk management, enabling organizations to address the unique character of different types of risk while also ensuring that risks are mitigated in an integrated fashion and from a strategic perspective.

Above all, IRM is a full deal. It does involve more than simply a risk identification process that is treated as input to an environmental scan. You can do that. If you do it well, you will put your organization at further risk since you have identified risks, made yourself and your organization aware of them and done nothing. Once you start with risk, you follow through.

We will exploring more of this in **Section 3. How an IRM System Works** and **Section 4. Implementation.**

Are You Risk Fit?

Before you start implementing IRM, you have to come to some conclusions about how ready your organization is to do so. This may sound simple, but a key element of doing that is seeing if everyone is on the same wave length, particularly your leadership team that will have to drive implementation. You need a clear minded assessment of the situation. Many organizations will start a conversation about risk with something like: “We’re pretty good at handling crises around here. It’s just seems to happen a lot.” Or “Of course we manage risks. It’s those outside pressures from headquarters that keep popping up and surprising us.” You need to break out of that and sit back and see, given all that has been developed in companies and governmental agencies around the world, where you sit. You need it to be systematic. You need to get to a decision about moving forward.

The following risk management checklist is a good example of the kinds of questions you need to ask. It can be modified to suit your needs, but it does have all the elements of an integrated approach.

Risk Readiness Checklist

This is a quick means to assess where you are as an organization in terms of risk readiness. Once you and your leadership team have developed an understanding of organizational risk and what it means, these questions can lead to some interesting and provocative conclusions about your readiness and capacity to manage individual risks but more importantly to develop a strategic control of risks.

Scoring – You can assign a score to each of these questions to come to an overall rating. Alternatively, you can make qualitative judgements with examples and information to back it up. Remember, scoring may well inhibit a full discussion. Very few organizations are either completely perfect or total wrecks. Often there are strengths that can be identified to build towards a more complete response.

	Score/Comments
<p>Risk Culture: Do we have a culture that understands that risk is part of the business, accepts that and works within that reality? To answer this, look for such signs as:</p> <ul style="list-style-type: none"> ▪ Do we understand there will be setbacks even with the best of plans? ▪ Do we factor that into how we work? ▪ Do we invite reporting on events that help us identify risks? ▪ Do we temper our expectations in such a way that there is an acceptance that we can have problems achieving our objectives? 	
<p>Risk Assessment: Do we have procedures or systems that regularly identify, measure and document the risks that could impact on the achievement of our business objectives?</p>	
<p>Controls: Do we put in place and regularly review the control systems needed to mitigate inherent risks? Do we have the means to evaluate their adequacy?</p>	
<p>Control Costs: Do we understand what our control frameworks cost relative to</p>	

Integrated Risk Management: Implementation Guide

their effectiveness? Are we over-controlling with no real evidence of risk?	
Defining Risk: Do we have a common understanding of what risk to our business/organization looks like? Do we have a common approach that ensures we understand each other when we talk of risk?	
Policies and Training: Is there a universally applied training approach that develops a common understanding of risk and its use? Is a policy about risk articulated for the organization in the normal way that policies are with the organization?	
Using Risk in Decision Making: Do we document and evaluate risks when making important decisions, launching new products or programs and preparing strategic plans?	
Underlying Risk: Are institutional risk factor adequately taken into account when assessing risk? This can include outmoded processes and policies, skills sets and knowledge, inadequate infrastructure.	
Planning for the Improbable: Are there contingency plans in place to deal with potentially high risk but low probability situations that could cripple the capacity of the organization? Are these periodically assessed?	
Is there data?: It is understood that the effective management of risk, just like any other management process, depends critically on the collection, analysis and dissemination of relevant information.	
Does the organization keep a grip on its vital signs?: Management recognizes the necessity of combining reactive outcome data (i.e., the near miss and incident reporting system) with active process information. The latter entails far more than occasional audits. It involves the regular sampling of a variety of institutional parameters (scheduling, budgeting, fostering, procedures, defenses, training, etc.), identifying which of these vital signs are most in need of attention, and then carrying out remedial actions.	
Early Warning Systems? Are there monitoring systems in place that identify potential areas of risk or that identify changes in risk status of known risk areas. Do these shake out complacency in environmental assessments?	
Risk Transfer Tools: To what extent does the organization use risk transference through risk sharing and insurance to mitigate risks?	
Regular Review of Risks: Is there a process for regularly reviewing identified risks? How effective is it? Are risks removed when mitigated or controlled?	
Effective Oversight and Governance: Is risk managed at the appropriate level of the organization? Is senior management and board involved at the appropriate level? Do they engage regularly and consistently? Do they see risk in the same way as the rest of the organization?	
Does the organization communicate risk effectively? To your employees, to other managers, to your shareholders and stakeholders? To the public Is there feedback on risk: The organization has in place rapid, useful and intelligible feedback channels to communicate the lessons learned from both the reactive and proactive safety information systems. Throughout, the emphasis is upon generalizing these lessons to the system at large.	
Organizational Support: Is there a clear organizational focus for risk management in terms of supporting the process? Is it connected to how decisions are made within the organization?	

How do you use this? Assuming you are interested in getting senior managers on board, you have to decide. You can use numeric scores and an interview process for the senior management team. You can simply do an assessment and submit it. Numbers tends to be stark and can be taken out of context without narrative. However, because of that, they can also quickly convey a forceful message, as in, "Do we really only want to be a 3.5 out of 10 organization when it comes to risk?" Such a message will either be very powerful or quite melodramatic depending on your working environment. At the very least, trying to answer these questions will stimulate considerable discussion.

How to Convince Your Organization to Take IRM on Board

Selling a concept like integrated risk management is a lot like selling any change process. You can have all the arguments in the world that make sense, but people still have to want to do it. So, the selling process, whether it be one individual or the organization's leadership team, has to think through how to do this. Here are three steps you can learn from sales techniques to facilitate change:

1. **Communicate a clear outcome.** Have a clear, strong vision of the benefits of the change. And be realistic. IRM will not shock-proof an organization, but it might make it more ready to take them when they come.
2. **Build relationships and Engage All Players:** To sell this kind of change, you must build relationships and a consensus about IRM as a course of action.. You have probably heard how people want to "buy" and not be "sold." It is equally true that people want to "buy" from people whom they care about and who care about them. Therefore, if you are in a responsible position, assigned or seeking the job of getting IRM implemented, remember it is about getting people to buy into the concepts that have a face on them: yours.
3. **A Consistent Approach Over Time.** People are most afraid after they have made the commitment to try something new. To keep people's trust and see them through, you have to stick around and give them good the support they need. In this instance, we are talking about the organization about to implement IRM. Changes can take years to fully implement. That means that you avoid flashy announcements with no follow through. It also means that you have to build internal or continuing consultancy capacity to get through the implementation bumps and grinds.

Recognize Some of the Inherent Dangers in IRM and Deal with Them

If some expert or consultant tells you that introducing any new systematic approach in your organization has no risks or dangers, fire them. There is always a down-side, some elements of which zealots or advocates will either downplay or ignore in order to win the day. As well, senior managers, who can actually get excited about things like IRM, may also under-estimate the dangers inherent in risk management in order to bowl ahead. It is far better to understand that such dangers exist and that you have to design for success, recognizing, as we will see in **Section 4, Implementation** and **Section 5, Using Risk Tools** that there will be bumps along the road. In addition, if your role is to

lead the implementation or propose the policy to your board, senior management or governing body, then you owe due diligence to them to inform them of the dangers that have emerged in other circumstances.

Here is a sample of some of the dangers inherent in IRM and possible responses to them:

- Formal risk management systems will often pit experts against stakeholders or the public: the research is clear that there are great differences between what an expert in a field sees as a risk and what the general public may. This forces organizations to find ways to bridge these gaps, something we will discuss in **Section 7, Risk Communications and Reputation Protection**.
- Reality versus perception: formal systems, which demand evidence, will often downplay the role of perceived risks. This challenges organizations to use both formal and informal means to gather information on risks from different sources. It also challenges them, and this is not easy, to address the gap between perception and reality.
- IRM can stifle creativity in the organization. First, it can create a risk filter and set of tolerances that readily communicate a no-risk philosophy in senior management sometimes when they do mean to do so. Second, it can force the consideration of initiatives or changes through such a forceful risk analysis that you end with paralysis by analysis, an endless loop of paperwork. Organizations have to guard against this through multiple channel input on risks, avoiding excessive paperwork and creating idea-creating zones within their organization.
- If not done properly, IRM can tend towards the quantitative and monetary elements over the qualitative, softer elements of risk. Clearly, this is a challenge of design and ensuring that all parts of the organization are involved in the IRM process, not just those who count beans.
- The process you put in place, if it is complex and not easily understood, can disenfranchise those unfamiliar with them, even if their views on the organization's risks may be useful and robust. For instance, corporate board members often complain that they do not understand multi-coloured reports with weighted scorings with too much detail. The solution centers around the KISS principle.

Idea Source: IRM is:

- ***Is a process***
- ***Is effected by people***
- ***Is applied in strategy setting***
- ***Is applied across the organization***
- ***Is designed to identify potential events***
- ***Manages risks with risk appetite***
- ***Provides reasonable assurance***
- ***Supports achievement of objectives***

Two Major Mistakes

Often, executives make two major mistakes in selling change.

- **Refusal to sell at all.** An aversion to the selling process is seen when an executive refuses to become involved as a "sales" advocate. People will have a natural resistance to change that affects them when you outline the program and present it in a purely rational manner and do not show commitment.
- **Hard selling:** How many times have we read stories or lived a few about organizations that go holus bolus into some new management philosophy, barreling ahead without regard for bringing the organization with it. The hard sell will by its very nature generate resistance. Remember your own resistance when you're pushed so you can empathize with how other people feel.

Experience has also shown that there are some unsettling elements to integrated risk management that lead to resistance. For example, some organizations are concerned that a focus on risks will increase their potential liabilities (when, in fact, it reduces them) or their efforts to better control risks will be misinterpreted by the media leading to political embarrassment.

Another source of resistance will be the fear and loathing that often accompanies yet another management initiative. Is this the flavour of the month? Here we go again. This is a disservice to the general thinking about integrated risk management, but a valid concern nonetheless. Part of the solution here is to avoid creating unrealistic expectations. Under-promise and over-deliver, a worn a cliché as that it is nonetheless a good starting point.

Some Winning Strategies

Using again the language of change process, here are some of the ways in which you can generate support for the adoption of IRM:

- **Create a sense of urgency:**
 - As Sir John Bond, chairman of HSBC, once said: "It used to take years of dedicated bad management to destroy a company. Now it can be done almost overnight." It is not just the range of hazards – from fraud and financial upheaval to terrorism and failures in supply chains – that can threaten a company; it is the speed with which such risks can strike.
- **Create a sense of opportunity:**
 - When there have been a series of events that have destabilized the organization, it may be looking for ways to get control back. IRM can do this. New management may be on board and trying to bring some

systemic managerial tools to bear. Here it is. Yes, it is also reasonable to promise that risk can reduce vulnerabilities.

- **Understand what some of the impediments are:**
 - People are not stupid. Just because they resist something does not mean they are either totally negative or lack comprehension. It is important for you to understand what the impediments to using integrated risk management are in your organization. See what the Economist Intelligence Unit reports on this.

What are the principal obstacles to making risk management integral with the overall business strategy of your organization?

Competition with other priorities	53%
A lack of cost-effective risk management tools	45%
Directors consider risk management a task for line management, not the board	35%
Poor awareness among staff inhibiting implementation	25%
The board does not understand or appreciate the principles and benefits of enterprise risk management.	21%
Governance requirements (e.g. Sarbanes-Oxley)	18%
Opposition from a key board member or groups of members	10%
Other	4%

Source: Economist Intelligence Unit, 2005

- Counter with a linkage to results and profit. A key message of integrated risk management is that an organization, when it does it well, is in greater control of its own destiny. It can assure its stakeholders that it is using its resources effectively. The Economist Intelligence Unit reports that these can be some of the results that better risk management will create.

Which of the following have results from your board taking greater responsibility for risk management?

Improved internal controls	50%
Improved standards of governance	45%
Improved business strategy	41%
Reduced compliance risks	40%
More robust corporate approach to risk-taking within the organization	31%
Improved shareholder value	25%
Reduced cost of risk management	24%
Lower insurance costs	24%
Improved returns on investment	23%

Source: Economist Intelligence Unit, 2005

- **Link to emerging business practice, not just compliance**
 - A lot of new governance and risk management tools are seen as meeting compliance requirements imposed from the outside. This may be one step in the process, but is hardly going to get a high level of commitment to IRM as a tool to manage the organization. A key selling message is that IRM will help the organization manage itself better while also meeting compliance requirements. Some of benefits at the practical level are:
 - Creates early warning systems that anticipates problems before they get out of hand,
 - Gives better linkage of performance information at the front end of the organization with business goals
 - Engages all levels of the organization
 - Creates a common understanding of risk
 - Gives tools to sort and prioritize risks
 - Helps identify resource demands well in advance
 - Bolsters the case for preventive actions and investments over reactive and more costly repairs.
- **Link to business planning**
 - IRM adds a rich layer to the business planning process. It moves environmental scanning from being a descriptive exercise to being a textured one that should drive business priorities.
- **Sell it as a concept about how the organization thinks, not another process.**
 - IRM does require some form of disciplined process to be successful. However, this can be home grown to suit the working culture of the organization. It only works, however, when it becomes ingrained into how the culture works. IRM can help turn around a culture that focus on reaction and “things happen” into a more responsive culture that prides itself on identifying emerging risks and actually turning them to its advantage.
- **Don't sell IRM as the newest, greatest and best fad going – link to well grounded, common-sense use**
 - The first line of resistance is: “Hey, we all do risk management around here.”. What do we need another report, meeting, form, piece of software for that? There are several messages to address this and work with it.
 - First, the ‘we’ is really a bunch of ‘I’s’ – everyone has risk management skills (assessing risks in the future, assessing their important, doing something about them), but is everyone really satisfied that the ‘we’ does it effectively.
 - Second, what I understand by risk may not be what we understand: we need a common platform. This is a good one to try.
 - Third, this is about the organization as a whole and the need for some systematic rigour to get everyone on the same wavelength.

- Fourth, we have to not just do it but we have to show that we are doing it. Our owners, board, auditors, stakeholders, political masters all expect us to do. Can we as an organization answer the question: what are you doing and show me how it works.
- **Understand that commitment to move forward will only come from within the organization even if the appropriate drivers are at work.**
 - That means finding a champion, preferably the CEO or key operational executive.
 - An important message to convince people to move is that the organization is serious about it. That means that senior management has to be committed through a policy, training resources to actually do it. Without this, managers, especially middle managers, will not see this as a priority.
- **Don't sell IRM as a replacement for strategic planning, business development or even internal controls and audits – it is an enhancement and underpinning of all of these**
- **Address the issue that many managers will feel that making risks more explicit will constitute a risk in itself.**
 - Address it with the counter-argument that failing to acknowledge risks and manage them is a form of neglect leading to potential liabilities or the 'when did you know and what did you about it' questioning after a problem arises.
- **Advance the benefits of a common approach and a single focus.**
- **Push the value of having a full system, not just one that may identify risks, but have no formal process for actual mitigation and monitoring.**
- **Give assurances that effective risk management does not demand excessive quantification or engage senior managers in numbers games.**
- **Address the *Not Invented Here* syndrome:** IRM is a way to manage that can be moulded to the organization.
 - There can be as few or as many colour bars in the charts, but in the end it brings a lot of personal involvement and direction to make it work. It has the advantage of not being a set of software and charts.
- **Middle managers will be the hardest to convince. They are busy, suspicious of new strategic direction. Champions need to be found.**
 - Middle managers need to know what is in it for them. They need to know that the effort to change will make their lives easier or better.
 - IRM is an important way of identifying performance and resource gaps. In fact, because there is some systematic rigour, it can be a way for managers to highlight the pressures they are facing.
 - Find examples of how IRM could identify issues such as staffing process, under-funding replacement and maintenance requirements, etc, that the manager had not been able to get attention previously.
 - Make it clear that managers can use the approach within their own organization to identify risks, engage staff and anticipate pressures. They have a new tool.

- **IRM has the advantage of taking time.**
 - It is not an overnight wonder. It is as much about culture as it is about process. This permits experimentation until you get the right fit. No one has to drink the Kool Aid.
- **Point out that effective risk identification is a very good way to win the budget game. This involves a much more objective process than simply asking for more. It also, if the process is accepted, places budget decision makers in a better position.**
- **Some of the benefits to focus on:**
 - A common understanding of the concepts of risks and risk management process throughout the organization;
 - Better business planning process. Ensures more well thought-out management strategies;
 - By anticipating scenarios before they arrive as problems, agencies can be better prepared. Mitigation strategies and plans can be developed and acted upon;
 - Better decision-making based on more relevant and complete information;
 - Communicating with partners and stakeholders (politicians, media, taxpayers, etc.) to identify and understand risks leads to greater trust and confidence.

Some pointers in communicating what risk management and, just as importantly, what it is not.....

Sensible risk management is about

- Ensuring that workers, the public and the interests of owners and legislative authorities are protected,
- Benefit society by balancing potential benefits with risk with a focus of scarce energies on the really significant risks
- Enabling innovation, learning and smart risk taking not stifling them,
- Ensures that those who create risk risks manage them responsibly and understand that there are serious consequences to not managing them properly.

Sensible risk management is not about

- Creating a risk free society, investment, operation or organization
- Generating useless paperwork mountains
- Scaring people by exaggerating or publicizing risks for short term advantage
- Stopping important activities with risks where risk can be and are managed
- Reducing protection of people from risks that cause real harm and suffering.

This list was adapted from a similar list created by the Health and Safety Commission, United Kingdom

Section 3: How an Integrated Risk Management System Works

What this Section Does

The next two sections are going to focus on getting going. This Section will deal with what a fully integrated risk management system looks like and the next will address what you need to have in place to get there. This Section will there, look at:

- A systematic approach to risk management
- Linking risk management and business operations and planning
- What integration looks like and how to know you have it
- Organizing to manage risk and risk management: the strategic fit.

Getting into systematic risk management is worth it for your organization. But it also takes an 'eyes wide open' approach to what it means and the kind of commitment needed to get the most out of the investment. Once you have sold your organization on the need for an integrated approach, lined up your internal allies and taken on the task of next steps, you have to understand how the system works.

A Systematic Approach to Risk Management

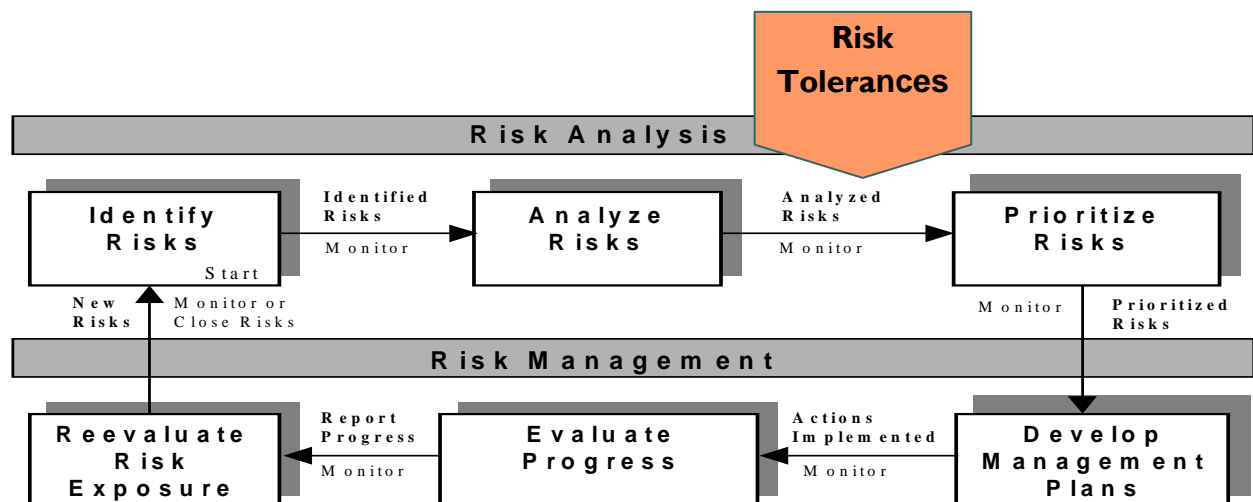
It is probably a rule of all implementation, but it is particularly true for risk management implementation: do not start unless you are determined to complete the project and believe that you have the tools you need to be successful. There are risks in simply doing the first phases of risk identification without actually following through on what your identified. These are real. For example, identifying a potential liability without either taking action to operationally reduce the liability or increasing insurance needs, will lead to further risk exposure down the line. Equally, getting staff and stakeholders all wound up about a risk identification and prioritization process and then not taking action based on their input will simply create internal cynicism and a nagging doubt that this was all done just to appease some outside driver. Like any major initiative or shift in processes, it has to be thought through. This one, however, could leave your organization is that old "when did you find out about or recognize this risk, what did you do and why did you not act?" type of question.

***Idea Source: "As we continue implementing ERM strategies throughout the organization, we anticipate more educated business decisions and greater return on investment. The results are not immediate. ERM should be views as a marathon, not a sprint."
- Lance. J. Ewing, Vice President of Risk Management, Harrah's Entertainment***

Risk management is a full process. It involves the following steps:

- Risk identification that is systematic
- A system of documenting and reviewing major risks
- A system of risk mitigation strategies with clear assignment of responsibilities
- Risk communication management
- Risk governance – someone is overseeing what is going on and making decisions.

It can be best understood, however, in a dynamic form, such as is outlined in this diagram:



This is a good way of explaining the system within a organization and how it works internally. Many of the steps in this process will be explored in detail in **Section 5, Using Risk Tools**. A note needs to be made here about the concept of Risk Tolerance, which we will explore in much greater detail in Section 5. This chart suggests that risk tolerances are taken into consideration as a kind of filter or gate in analyzing risks to help prioritize those risks. This is indeed what needs to happen. However, as we will point out, risk tolerances do not spring magically out of some manual or simply at the direction of the senior management. Most organizations face many challenges setting risk tolerances. These challenges involve the relative benefits and use of quantified tolerances, political nuances, and lack of experience. Therefore, the risk tolerance process is a highly dynamic one. It can also be a protracted one in which the organization ‘tries on’ certain kinds of tolerances, finds that they do not work or are not readily understood and tries again. Of course, you will never get to a reasonable set of tolerances that are useful without fully engaging senior managers over time. Often, it is a

case of trying something out and seeing if it works rather than scientifically setting levels. More to follow.

What gets in the way of an effective risk management process:?

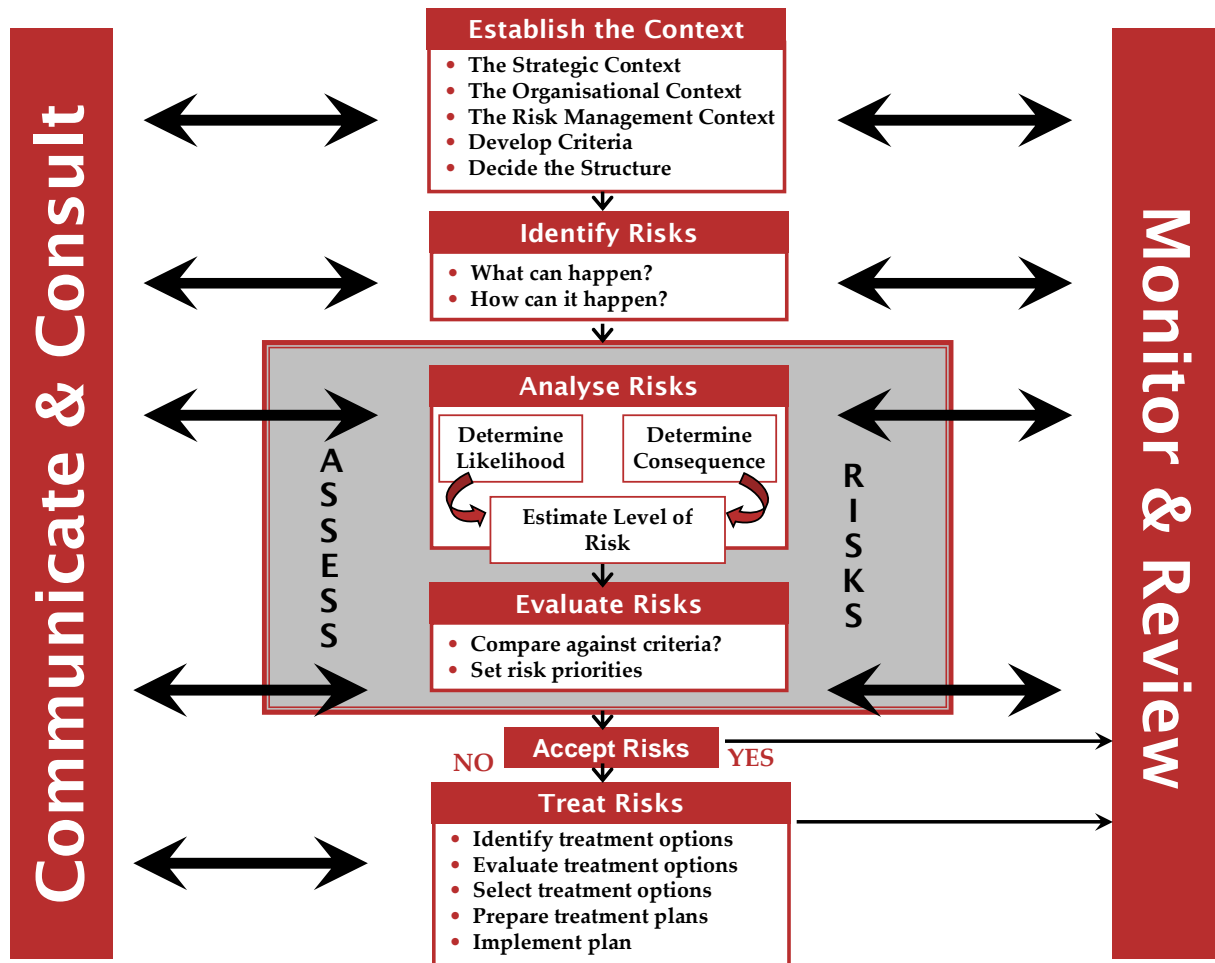
- Too narrow a focus on risk -
 - Extend focus from financial risk to include non-financial risk at the strategic, business, process and "control-culture" levels
 - Don't just focus on the "comfortable" areas
- Failure to manage risk complexity and materiality
 - Support enterprise-wide consistency, yet provide opportunity for local customization
 - Set parameters to ensure focus is on the most critical risks rather than every risk
 - Use materiality factors based on risk tolerance
- Complex reporting and communications
 - Develop a communication plan early in process
 - Use simple, colour-coded charts and reports
- Unclear accountability for risk
 - Allocation of accountability usually performed after the "event"
 - Establish accountability (ownership) for risk management to appropriate operational managers
 - Create linkages to compensation
 - Ensure appropriate executive sponsorship
 - Need one clear owner (at executive level)
- Undefined roles and responsibilities
 - Executive committee must set direction and strategy
 - Executive management must accept residual risk
 - Senior management must accept ownership of risk
 - Risk Policy & support through the development of guidelines, tools and measurement
 - Operations management responsible for identifying, assessing, mitigating and monitoring and asserting.
 - Business Systems and Control must perform periodic assessment and assurance

- Halifax Regional Municipality Business and Risk, Planning, available at http://www.halifax.ca/business_systems/risk_management.html

The Risk Management Model

A fully dynamic outline of risk management working in an integrated way on a strategic level is best represented with the following chart:

Integrated Risk Management



Points to Note When Introducing This Chart

Charts which try to integrate a number of processes to offer a whole picture can also confuse and complicate. This is unavoidable to a certain extent and this chart is as guilty as many others. It does represent, however, an attempt to both display the full characteristics of an integrated risk management system and also show some of the dynamics of the relationships among the elements. Here are some points that are useful to note when introducing and explaining such a chart. Remember, they do not always speak for themselves.

- The central column represents a classic view of the basic steps of a risk management system and its basic elements
- The column appears to move in a logical sequence and to a significant degree, all elements need to be in place, but this is hardly a static, step-by-step process once its goes live – there needs to be continuous loop-backs over time. Similarly, various steps can be taking place simultaneously within the dynamic of an organization.
- Note that the first steps of integrated risk management have nothing to do with risk, but with context – the objectives and strategic goals of the organization. Risk is inextricably linked to organizational objectives.
- Communications are a constant throughout the process.
- Note that there are two-way arrows for both communications and monitoring: this means that communications is also listening, learning and re-evaluating the facts as you know them. In terms of monitoring, risks, particularly that vital few that are urgent and close at hand, cannot wait sometimes for orderly reports on a quarterly basis.

Linking Risk Management and Business Operations and Planning

Risk management is not a stand alone item. In fact, if it is, it will either be seen as excessive or an organizational orphan of little use to the rank and file or in helping management guide the organization. Risk and how organizations address it is just part of a suite of management tools an organization should have. Seldom will you hear someone say “All we do is risk management around here.” Hopefully, the organization is also

***Idea Source: “To obtain buy-in from the organization, ERM must not be a discrete process, but rather, part of the DNA of the company. It’s vital to listen to the front line and present ERM as a process that can solve real problems.”
- Joel Schmidt, Chief of Audit, Alliant Energy***

trying to accomplish some goals, reach some project or program objectives or keep financially stable and profitable as well. You could even argue that if an organization is excessively preoccupied by risk, it is in some danger of losing its way or unable to move forward with its objectives due to zero risk tolerance or a total risk aversion. This is a sure formula for paralysis.

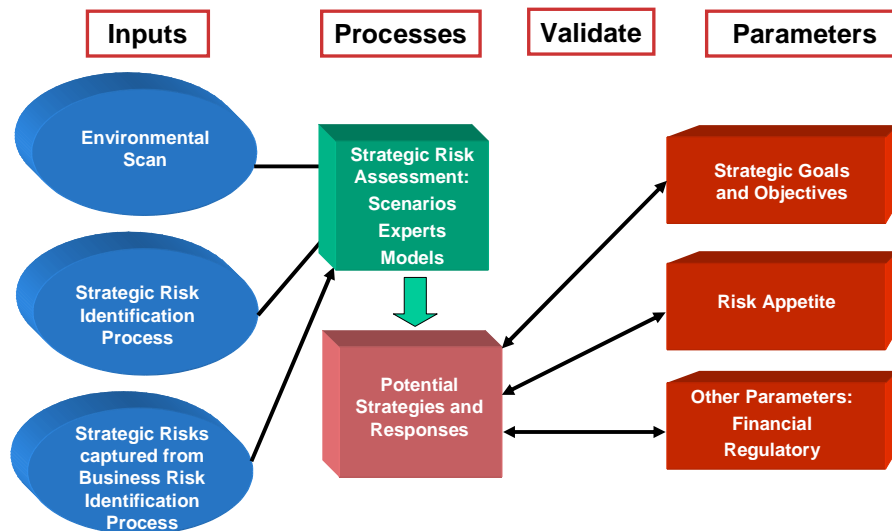
On the other hand, risk management as a stand along function is rare. There will be organizations that need it. You will often find robust and large risk management groups in financial organizations. However, even there, they feed into decision making in very important ways. The point here is that risk management disconnected from how the organization makes decisions will be an organizational orphan. While it may generate lots of activity and have its advocates, it will not make a contribution where it is needed.

What follows is a description and set of pointers about some of the key elements to ensure that risk management is properly linked to business operations and planning. The first is how an organization has to think about identifying risks. The second is a series of tests about integration with the business processes, culminated with a **Risk Integration Checklist**.

Identifying the Risks Informs How You Use Risk

How an organization assesses its risks will tell you a lot about how integrated its approach is to risk management. We will be discussing this in more detail in **Section 7 Risk Communications and Reputation Protection**. However, the point here is that an essential part of a full IRM is an effective means to canvass the environment of the organization in a way that permits it to assess risks not only through self-identification but through outside and, preferably, non-traditional sources. The process of gathering risks for assessment and evaluation, looks like this:

Strategic Risk Identification Process



Points to Note When Introducing This Chart

More than anything, the risk identification process is about harvesting information, a lot of which you will already be gathering. Often, as well, organizations will use some or all of the processes outlined here in their business planning, depending on how sophisticated or detailed that is. Here are some of the pointers that you can make to clarify the chart, but also to drive home some key message about IRM:

- While this chart shows three sources, they are at a pretty high level: the risk resilient organization will seek many sources of information about risk,
- The term Environmental Scan is used a great deal. Beware of that. Some words have to be said about the quality and depth of such a scan. Also, you can point out that an effective environmental scan involves multiple and potentially contentious sources.
- A word or two about the other two sources. The first – Strategic Risk Identification Process – assumes that your organization will want to engage in some formal risk identification methodology. Certainly, this is healthy and desirable. It can be integrated into an environmental scan. However, it can also get diluted in that process. Certainly, some kind of autonomous process, even if it involves an executive committee identify risks or a working group, helps focus the process.

What is a Resilient Organization?

The term resilient organization is more than a positive description of a well managed organizations. There is a considerable literature and research that show that some organizations adapt better to risks, learn from their mistakes and manage their objectives, often associated with high risk enterprises in business and government. Some of the definitional characteristics of resilient (also called highly reliable organizations) are:

- They withstand discontinuities and adapt to new risk environments,
 - They have a high awareness of their operating environment and systems to detect risk or error with scanning at a high level,
 - They agile and internally networked to permit the rapid flow of information and corrective action,
 - They dynamically reinvent business models and strategies as circumstances change, and
 - They have the capacity change before the case for changes becomes desperately obvious.
-
- The second, however, is a different animal and one of the keys to successful risk management integration. Business risks here mean risks encountered or identified in the normal course of operations. These can be, for example, equipment failure rates showing disturbing increases or accidents rates rising or shifts in client satisfaction. Resilient organizations find ways of ensuring that these day-to-day occurrences, often resolved with a short-term response, are recognized as possible signals of strategic shifts or risks. It takes judgement and experience to separate the daily bump and grind of operating a unit from emerging patterns or signals that define emerging risks. Often organizations lose sight of these. As is often said, the distinction to keep in mind is between risks (short term) in the business and risks (medium and long term) to the business.

- The second element – Process – brings out a very important point to make. You can have all the gathering of risks information you want and even apply models and quantitative analysis. But, there is a key step that is at the heart of IRM. You have to actually decide that you agree there is a risk that the organization has to take on. Without this you are lost. You are also potentially a victim of either too much input or what is commonly called the Chicken Little Syndrome.
- One final point about this diagram. Note that the parameters that help you defining and ‘recognizing’ risks work both ways. Seldom will all parameters be cast in stone. Some are. Some are also well defined. Others will involve situational responses. That certainly is the case with most of risk appetite or tolerances which we will discuss below.

Listening to the Silence: A Special Challenge

Healthy organizations find ways to scan their environment for those risks that are neither self-evident nor necessarily directly related to the current preoccupations of the managers and staff. Further, they will find ways to ensure that they break the very real danger of what is called **groupthink**². In these instance, vital information is often blocked out by organizations which have developed a way of looking at the world and fail to see that there are other views or that the world they are looking at has changed. In many public organizations, there will be groups that are highly critical of the organization’s performance or that are stakeholders in one way or another (recipients, other governments, observers) who are not regularly involved in feeding into the organization information about their perceptions.

Idea Source: “The most significant risk assessment tool we use is face time, getting in front of the business units on a regular basis to ensure that we understand the full context of the risk. Face time also helps foster an open environment for communication exchange. Other than this, we have kept out tools simple.”

- Joel Schmidt, Alliant Energy

Effective organizational leaders will find ways to incorporate these concerns into their risk assessments. In fact, healthy organizations use techniques to ensure that decision makers, who are generally busy and focused, break out of their intelligence gathering patterns to see things differently.

Some of the tools that successful organizations use to break outside their traditional informational flows are:

- Do a **Strategic Audit** – have an independent organization come and provide an assessment of on the risk process you use to develop strategy,

² [Irving Janis](#), **Victims of Groupthink**. Boston. Houghton Mifflin Company, 1972 defined *groupthink* in the following manner: A mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action.

- Assessment your strategy independent of management – independent assessment of technology, efficiency, traditional metrics, customer view against its objectives,
- Use of surveys of key client groups,
- Ensure that board and senior management composition brings varied experiences and perspectives: avoid duplicating yourself.
- Regular exposure to new ideas through speakers or site visits
- Building risk and strategic groups from staff across the organization and not just a specialized units: mix true believers with sceptics, understanding that they all work for the same organization,
- Leaders should assign the role of “critical evaluator” in the risk identification process. Alternatively, a challenge function could be built into the risk management office.
- Leaders or decision-makers should not express an opinion when assigning a task to a group.
- The organization should set up several independent groups, working on the same problem.
- Each member should discuss the group's ideas with trusted people outside of the group.
- The organization should invite outside experts into meetings. Group members should be allowed to discuss with and question the outside experts.
- Use an **Appreciate Inquiry Process** with stakeholders. Appreciative Enquiry Process means that an organization regularly assesses the quality of its interaction with key stakeholders – using survey, interviews, some form of formal evaluation
-

Listening to the silence takes special effort. It also exposes the organization to potentially useful ideas and information that could well advance its objectives. It is not intended to create a higher level of risk aversion or, alternatively, increase risk appetite. Either could emerge from an organization taking a serious look at information or ideas in an unconventional way. Rather, it is a check, meant to answer the question: “Are we getting the information we need from as many sources as possible before we move forward?” In addition, seeking out alternative sources of information can also address other key risk questions, such as:

- Is the business model to which we are so committed actually understood, working and still viable?
- Are there major change factors – demographics, cost of money, regulatory environment, shift in public priorities – that we are failing to take into account?
- Are we missing real opportunities to grow our business or meet our objectives in more powerful way?
- Are we really aligned with our clients?
- Do we have the respect or reputation we think we deserve?
- Is there an elephant in room where we make decisions?

Ignoring Your Shop Floor at Your Peril

So much of the literature on IRM focuses on the higher-level and the strategic. This is fine and vital. Otherwise, you lose sight of the relationship between risk and your objectives. In doing this, however, operational information and the front-line perspective can be lost. Organizations that are resilient learn constantly from their errors, their experiences at the front-end and variances in the expected performance of internal process and the reality. Taken in the appropriate perspective, this information is vital to the risk identification process. As has been shown in a large automotive company like Toyota³ and the application of *Lean Management Techniques*, organizations that focus on front-end processes, engage staff in their continual reassessment and improvement, also gather up an amazing amount of information about the risks they face as well as the opportunities to grow the business these insights provide. The same holds true for all organizations, regardless of how large or how small.

Idea Source: “Internally we began to question problems to see why we had not identified them as a risk. Slowly, we developed a debriefing mentality on incidents that encouraged us to see even accidents as opportunities.” – Corporate Executive

In this vein, Karl E. Weick of the University of Michigan points out that organizations that the most resilience are the ones that pay close attention to what happens in their operations. He studied varied organizations such as aircraft carriers and nuclear plants to establish not simply that errors were reported, a simple first step, but that the information such variances offered was taken seriously and used as an opportunity to assess overall performance and identify risks.⁴

There is an extensive literature on organizational resilience. It has many elements, all focused on creating organizations that can recognize and respond to change in an effective and successful manner. Running through much of it is the need for organizations to listen effectively to their own life signs and learn from them. Does this sound like an important part of IRM? It certainly is.

Here are some questions to ask to test if you use effectively use operational information in your risk assessment process:

- Is operational data regularly assessed against plans to determine if you are on track? (If not, well, you may not be managing at all.)
- Are errors and anomalous events reviewed on a regular basis by senior management?
- Is time spent trying to learn from the anomalies that pop up? Do you encourage employees to report these?

³ For a good description of this see **The Toyota Way** by Jeffrey L. Liker, ISBN 0770391399, McGraw-Hill.

⁴ Kark E. Weick, **Making Sense of the Organization**, Blackwell Publishing, ISBN 0780631223191, 2001

- Is information about operational performance hierarchical reported or is it available in a networked fashion for all to view?
- Does your organization, as a matter of practice, seek out and examine potentially disturbing information in order to test their current models of understanding reality?
- Does your organization give deference to the expertise of your operational staff in balance with the managerial concerns of the hierarchy?
- Do you regularly conduct debriefing sessions after significant events, problems or major challenges, events that leave open the possibility of all participating regardless of rank with the intention of examining what went right, what went wrong and what needs changing?

Risks in Bundles: Categories of Risk to Examine

After discussing the ways to ‘listen to the silence’ and to seek out various perspective on operational events, it seems a little strange to now turn to categories of risk, supposedly neat bundles that help us niche various risks. That is not the intent at all. Rather, every organization has to develop, if only to sort out things, various categories of risks that they must review on a regular basis. Once again, they also have to find ways to ensure that these categories do not become ways of not seeing. That being said, recognizing that there are various categories of risk is a good starting point for helping your organization think about risks.

Commercial and Legal Relationship Risk

- Leases of property.
- Franchise agreements.
- Licensing agreements.
- Supplier relationships/contracts.
- Customer relationships/contracts.
- Employer/employee relationships.
- Contractor/subcontractor capacity to deliver in timely way
- Liability for performance

Financial and Economics

- source of funds
- credit risks
- economic climate
-

Human Behaviour

- Clients
- Stakeholders
- Employees
- management

Environmental

Natural and Human Caused Disasters

- internal emergency response capacity
- evidence of pandemic like events

Government and Political

- new policies
- new government
- shifting regulatory framework
- shifting priorities
- spill over from other political issues

Technology

- Dependability
- Cost of maintenance
- Match of need to supply
- Redundant capacity
- Security

Management

- Leadership
- Control and oversight
- Quality and client services
- Resources

Infrastructure

- Age
- Adequacy
- Changing requirements

Organizational

- Structure
- Communications
- Staffing
- Resources
- Health and safety

Partners and Suppliers

- Reliability
- Reputation
- Cost

Characteristics of Integration: A Checklist

One of the challenges and issues that often comes up when implementing IRM is the degree of integration with how the organization does its business. This is another one of those ‘are we there yet’ issues. Without taking away from the fact that integration of business processes in general is a continuing challenge, some tests can be applied. The following checklist was adapted from several now in use around the world. It is put here as a way to answer questions such as those just posed, but also as a way to provide some measures for moving forward so that the organization can assess itself. It is as equally important when looking at implementation, but put here as part of the descriptive process of IRM.

Risk Integration Checklist

An organization that has successful integrated risk management into how it manages, how it governs and how it sets strategic directions will adapt certain behaviours. Remember none of these absolutely guarantee that risks will be effectively managed. This takes individual judgement and leadership. They do ensure, however, that a healthy process, founded upon the experience of many companies and government agencies around the world, will maintain some visible rigour.

	Comments/Evidence
Does the organization apply risk management as a clear part of its strategic and business-planning considerations at all critical levels of these processes? How?	
Expected board or executive management behaviours: <ul style="list-style-type: none"> ▪ Are they properly and consistently informed of risk exposures? ▪ Do they confirm that suitable risk management strategies are in place and working effectively? ▪ Are they fully and directly involved in setting and reviewing the organization’s risk management strategies? ▪ 	
Does executive management lead and strategically manage the organization’s risk management process?	
Do senior managers, boards where present and key decision makers become involved in the identification and assessment of the organization’s risks?	

Does your organization ensure that executive management confirm that the organization's risk management framework and strategies match the key risks of the organization?	
Are risks reports and risk management actions reported in sufficient detail to the executive and board to ensure these are properly understood?	
Are key performance indicators of risk and risk management incorporated into the organization's governance processes?	
Is there formal oversight of the risk management process through an audit committee, risk committee or the executive committee itself?	
Are resources allocated for the continuing implementation of risk management policies, plans, training and procedures?	

Section 4 – Implementation

What This Section Does

- Raises the key risks in the implementation process and questions to pose to mitigate them.
- Outlines the elements that will be needed to ensure full implementation and strategic fit, and
- Points to a variety of practices now in place

The Questions to Ask and Answer

Let's assume at this stage that you have decided that you want to get your risk management act together. You understand that it is more than just another report. You have taken on board the key 'whole meal deal' message that constitutes the integrated in IRM. You also want to avoid creating more risks. You are also aware that there tend to be significant gaps between what you might expect out of an IRM process and what you actually get in various industries in governments around the world.⁵ Your objective in implementing is to get it right at the right cost.

Idea Source: "We don't think ourselves into a way of acting, we act ourselves in a way of thinking." - from Execution: the Discipline of Getting Things Done by Larry Bossidy and Ram Charan, 2002, Crown Business

Implementing any organizational change and ensuring its sustainability is more than having a staff member 'go out and buy you one'. That is why this book will repeatedly advise that the IRM be home-built. Get all the help you need, but in the end, it has to be yours. Here are some good questions to ask in thinking about implementation.

Question 1: "Why are we doing this? In other words, , what are we hoping to accomplish with IRM that we cannot accomplish otherwise?"

You need to develop a clear statement on this. You will have a number of audiences that are going to be wondering what management is up to this time. Is this the next best thing? A new fad? Generally, this important step in clearing the way will involve a statement that will take into account such features as:

- Better equipping the organization to respond to risks,
- Ensuring greater compliance in a regulatory framework
- Creating a healthier perspective on risks and their management where zero tolerance can cripple an organization
- Improved control, pure and simple

⁵ For a good survey of issues, see **ERM Lessons Across Industries** by Jerry Miccolis, Tillighast-Towers Perrin, a summary of which is available at <http://www.irmi.com/Expert/Articles/2003/Miccolis03.aspx>

- Coordination/integration—Breaking down internal silos by coordinating various pockets of risk management activity for efficiency's sake.
- Moving beyond purely financial risk management
- Exploiting opportunities and creating value—Appreciating how risks interact across the organization and exploiting opportunities among them.

These are just a few example of why an organization may chose to implement an IRM. The point is that the reasons need to be clear in order to articulate anticipated outcomes. Eventually somewhere in this process someone will say that this is too much work, that it is not working or that it failed to achieve its objectives. You can only address such issues if you knew why you started to do this in the first place.

Further, from a communications point of view, stakeholders or oversight bodies such as boards or legislatures will need to be comfortable that IRM is a sound management decision.

Question 2: "How extensive will our IRM be? What types of risks will an IRM cover and what management processes will an IRM influence?"

This is a useful question to ask at the outset, but be prepared to keep asking it as you go along. The anticipated answer in the thinking about implementation phase would be fairly general and broad brush. You cannot define an end stage with absolute precision. However, the first answer has to be good enough to get the implementation or team going and to be able to ensure that no one that you want into the process is let off the hook through some vague and general statement. In addition, it is seldom the case that organizational leaders develop a yen for IRM out of the blue. There is history and there are issues. Therefore, building on them, the start-up notion of scope, which is what this question addresses, should be inclusive.

For instance, with respect to what types of risks to be included, one simple answer is all risks. Simple trap that. The trap is that you can involve senior management in micro-managing risks that organizational units have authority and responsibility to manage and only report when they are beyond their capacity. Similarly, every organization has boundaries of external interests. While it is important to be able to scan and sense currently unacknowledged risks, an IRM can get lost in a strategic fog.

In answering this question, here are some others to ask yourself and the leadership team:

- Will all organizational units be involved?
- Do you want to cover both financial and all other risks?

Here are some categories that may help in defining your scope:

- Financial—e. g. interest rate, investment, credit, liquidity, asset market value, budget and cash management

- Operational—e.g., technology, people/intellectual capital, political/regulatory
- Hazard—e.g., legal liability, property damage, natural catastrophe
- Strategic—e.g., changes to program framework, major market shift, new developmental opportunities.

The second element of this question is what management systems presently in place do you want to be affected by the IRM process. This will define who needs to be involved and where you normally expect to see IRM processes visible. It will also walk right into the mine field of turf, an issue that is part of the genetic structure of virtually all organizations. However, stepping back from that abyss and looking at the this in relation to Question 1, some of the fundamental processes in the management of the organization to consider are:

- Strategic and business planning,
- Environmental scanning,
- Internal audit
- Program evaluation
- Budgeting and asset allocation
- Investment and capital decision-making
- Financial control systems
- Performance reporting:
 - Financial
 - Operational
 - Compliance
 - Outputs and outcomes
- Performance monitoring and rewards: staff
- Project management.

Idea Source: Here's a good test of how far IRM has become part of the culture:

- *All decision making within the organisation, whatever the level of importance and significance, involves the explicit consideration of risks*
- *Examination of the records of meetings and decisions show that explicit discussions on risks took place.*
- *All parts of the risk management process are represented within key processes for decision making in the organization; allocation of capital, major projects and, re-structuring and organizational changes.*
- *Risk management is seen within the organization as providing the basis for effective and prudent governance.*

Question 3: "What kind of organizational structure do we need to implement and sustain IRM?"

IRM does not create itself. It takes work and, over time, concentrated effort. Therefore, treating it like a corner of the desk project will be a sure guarantee of its untimely death, underachievement or quiet disappearance. As we will see below, the various steps involved in implementation and the IRM process itself as outlined in **Chapter 5, Using Risk Tools**, require some commitment of personnel and other resources. While you may not want to fully address the sustainability issue, it cannot be far from mind. The essential worth of an IRM is that it adds value to an organization over time and that you get better at it as you use it consistently. Therefore, consideration has to be given to its full implementation, not just to the end of the project phase.

Some defining elements to the answer to this question, some of which will be discussed below, are:

- Which organizational entities will play a role in managing IRM or do we create a new one, and which functions will they be integrated with, e.g. our present audit committee?
- What will be the responsibilities of the person or organization that manages the IRM process? You do not need final answers here, but certainly some direction is needed. For example, your internal audit group could lead this until a new organization is created, or you could create a special team independent of any organization reporting to the CEO or CFO initially.
- To whom does the IRM function report. This may have two answers: short-term to the CEO or CFO and longer term, to be determined. The point here is to ensure profile and capacity to move across organizational silos in the implementation phase.
- What are the skills and competencies we are looking for in an IRM function? The answer to this will reflect the objectives of the organization and skill set of its people. Organizations that want to develop their project risk capacities for complex construction operations will have quite different needs than ones that provide front-end services to a defined client group. Nonetheless, the following list has to be taken into account when determine skills needed:
 - Technical capabilities in risk modelling and assessment
 - Financial systems and controls
 - Use of sophisticated mathematical models for risk determination
 - Communications skills
 - Interactive and team skills

Question 4: “Is there one risk management tool or system that we are adopting?”

“We don’t know.” is a perfectly good answer to this question. However, many organizations, rightly or wrongly, want to buy a total package and import it to their organization. Someone, mostly notably a member of senior management, may have seen it operating somewhere else or become convinced of the merits of a particular organization and want to get it and use it. If that is the case, implementation has just begun. As we will see, the choice of process is just part of implementation. Knowing that a particular product is in favour will affect how to proceed. For instance, if the decision is to go with one of the many professional groups with expertise in risk management and one is chosen, it needs to get on board quickly. It needs to be integrated into whatever oversight and control processes are established internally.

On the other hand, another answer might be: “We will adopt whatever systems make sense, fit with our current business processes and are affordable.” That signals a deliberative process that various actors within the organization can have an impact on.

The third answer for many organizations may well be “We will adopt the tools that central office (or our central agencies) have identified as best practice.” That signals that the organization, as part of a larger entity, is adopting corporate models. Implementation still matters a great deal here. It also introduces the dynamic of fitting broadly established standards into your organization’s unique requirement.

The Key Decisions Guiding IRM Implementation

Effective implementation will hinge on a number of elements:

- A clear decision to proceed
- Resources to back that up
- Accountability for results
- A definition of the desired end state to measure progress against
- A learning and adaptation loop that doesn’t sink the ship, but may change its course a bit.

Section 3 made it clear that IRM involves a series of linked steps. Without them all, you will not really have the full benefit of the effort involved. Implementation is about defining those steps in your organization and making sure they get done.

Implementation takes time. Often you will hear a statement like “This is as much about cultural change as it is process change.” This is true. Therefore, take into account a couple of factors when setting up an IRM implementation plan:

- This will take and will require considerable training effort,
- Be prepared to change and adapt as you go – this is not about a simple process or software change.

No one size fits all. That is certainly the mantra of this Roadmap. However, research in the field has shown that any organization will have to fill in the blanks for certain key questions. These should guide how you implement.

- How do we define risk in our organization?
- How do we prioritize risks in our organization?
- Do we need to implement a formal integrated risk management framework?
- What would anyone be opposed to a comprehensive risk approach?
- What works better for this organization: a centralized or decentralized approach?
- What role should certain central staff functions play versus line management?
- How do we staff and resource the risk management program?
- How can we embed IRM into existing business processes?
- How can we convince line managers and staff of the value of IRM and use it to drive change?
- What information about the process and results do we provide to key stakeholders, e.g. a board, senior managers, central agencies, political masters etc.

To Pilot or Not to Pilot

Many organizations will test out a risk management process in one unit. Many just go right across the board. Certainly the former is a lower risk approach. However, a number of factors need to be considered in choosing the pilot approach. These are:

- What are you piloting, the idea of IRM or the methodology? If it is the first, then the organization clearly is having commitment issues. If the second, then it may well want to both encourage a front-line champion and find the best match of methodologies and corporate culture.

Recommended course of action: Pilot if that will increase overall commitment and genuinely permit the organization to learn what works best. But, the executive must be committed to an IRM policy and direction in order for anyone to take the pilot seriously.

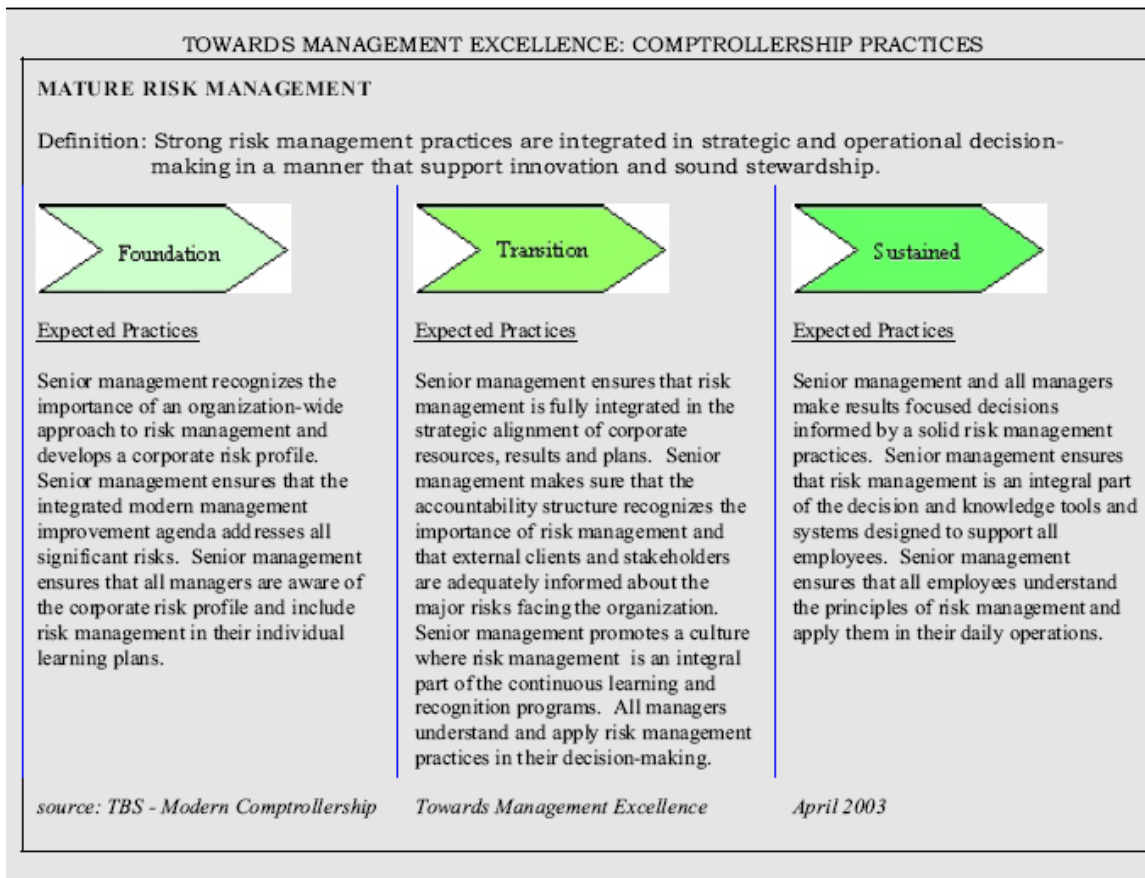
- Pilots can go on a long time and people forget why there were put in place. Commitment dilutes and objectives morph into something else.

Recommended course of action: Create a project management approach that builds in timeframes, expected processes and resources to meet them. Regular reporting is essential. The ultimate organizational responsibility centre for risk management has to be a full partner in the pilot.

Pilot by all means, but do so wisely.

A Phased Approach

A common theme in conversations with those you have implemented IRM is that it takes time, focus and a preparedness to adapt. While many organizations want to press forward quickly, it has been lesson that rapid implementation will fail to address issues such as ensuring that there is a risk adaptive culture or that various risk tools can be moulded to the organizations needs. So, even if you have to move quickly, do so slowly. The following phased approach, without time frames that Health Canada, a federal government department, has adopted is a good example both of an understanding that implementation has different phases, but not ones tied to a specific time frame.



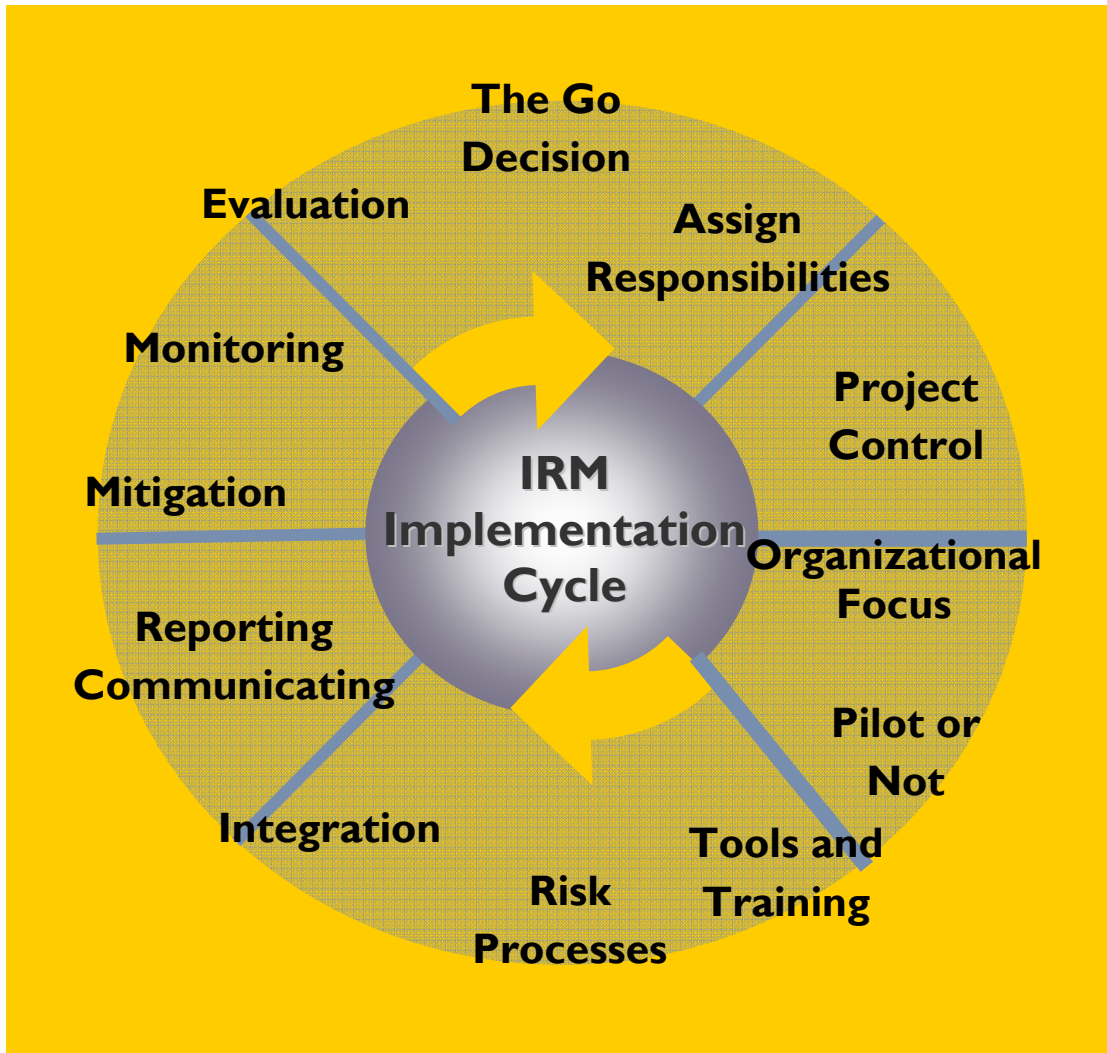
Strategy for the Implementation of Integrated Risk Management in Health Canada, June 2003

The Steps in Implementing IRM

What needs to be done in order to start the implementation process? This will depend on the organization, but there are certain key features:

- Signalling your decision to go: through a policy, statement, direction
- Establishing responsibilities for implementation.
- Establishing projects controls and performance expectations
- Creating an organization focus of expertise and support
- Developing tools and training methodologies
- Integrating risk management practice into business operations
- Developing pilots
- Training and familiarization
- Creating risk profiles
- Integrating with existing planning and control systems
- Monitoring and evaluating

The IRM Implementation Cycle

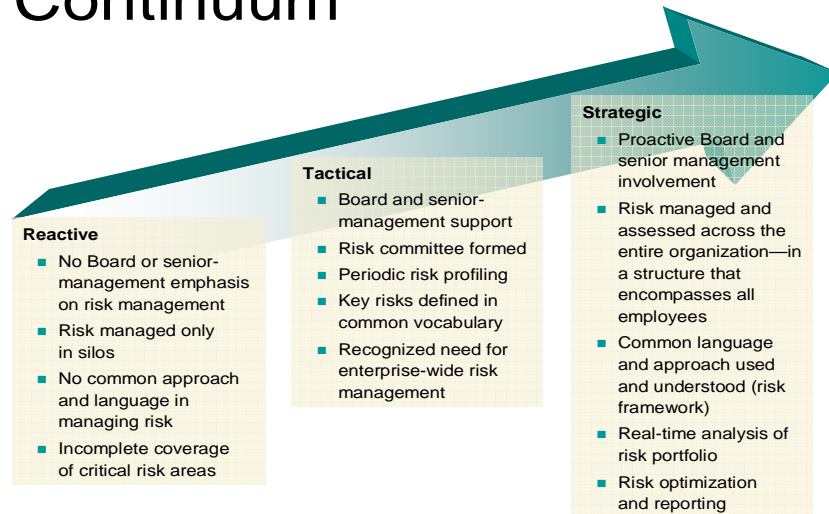


Take a Sound Time Perspective

In a hurry? Great, but expect that no matter what kind of hurry you may be in the implementation of IRM will take some time. Why is that? An elemental reality is that implementing effective IRM is a cultural as well as a procedural process. Most organizations that have been successful – and more than a few that have failed – have also learned that they have to experiment to get it right. That may mean going down one path, finding it wanting and starting down another. Finally, there is certainly a life cycle in all implementations, as outlined in the diagram below.

From: *ERM: Presentation to FMI , Ontario Chapter, 2006*

Risk Management Maturity Continuum



Creating a Risk Management Policy

If you answer the four questions above, you have a policy framework. The idea of a detailed policy at this point does not make a lot of sense. However, it depends on your organization and the way in which it normally articulates policy. If there is a formal system and a standard documentation, then use it. An articulated policy statement does speak to the intention of senior management to move forward. It also assigned responsibilities and states, to varying degrees of generality, the objectives of having an IRM.

If your organization has a board of directors or an oversight body, having it adopt an overall policy is a means not only of setting the direction, but also of locking in commitment to the concept. Before looking at sample policies, some of which are surprisingly short, here are some of the key elements that you will need to cover in such a document.

Policy Statement on Risk Management

Overview/Summary

Responsibility Centre:

Approved by:

Policy Statement:

- Intent of Risk Management Policy
- Scope of Policy
- Approach to Implementation
- Roles of
 - Board/Governing Body
 - Management
 - Staff

Definitions:

Related Policies:

Follow-up Responsibility

Periodic Review of Policy Effectiveness

A few pointers on a policy statement. Keep it short and to the point. This is, after all, a statement of intent, not to be lost in a lot of detail. Link it to relevant existing practice and policies. Therefore, as most organizations have some type of hazard management systems that are risk based, create the link to ensure an understanding that these policies should relate to each other. Use this policy to define prime responsibilities. From a board perspective, the greater part of IRM will be the responsibility of the CEO. This needs to be articulated. Similarly, organization that wish to make it clear that risk management responsibilities are pervasive to the organization and not restricted to risk management specialists, should state this in the policy. For larger organizations with multiple business units, a corporate risk management policy is a means to direct those units to get on with their job of implementing the corporate will.

See the **Appendix** to this Chapter for some concrete examples of policies.

The Role of Leadership

Leadership: it's continually touted as a critical success factor in implementing and sustaining any significant organizational change. Executive leadership support is essential, without doubt. However, the real test is how the senior leadership in organizations demonstrate that leadership support and set the tone at the top. This goes into the realm of action and consistent attention. As more than one manager joked: "A memo from the CEO is not

Idea Source: "Senior leaders have to have the same training as front-line workers—and train with them."

leadership commitment.” Somebody has to step up: chief executive, chief auditor or chief risk officer. The power of the individual leader is apparent in how an organization approaches implements and fosters integrated risk management. On the other hand, talking about leadership at the level of cliché does not do much to get things done either. So, when a project team states, “Leadership is needed.”, they had better be clear about what they mean exactly.

Idea Source: “The only way you can legitimately talk about risk is to actively manage risk.”

Many leaders draw on a background and experience in risk management, and lead the charge for moving risk management forward in their organizations. They simply expect it to be part of how the organization is managed. However, other leaders have to be sold on the concept by champions in the organization, and then demonstrate their commitment to support the initiative. The significance of executive support can often be made quite clear when the sponsoring executive leader leaves the organization. Without that constant, consistent force, risk management activities can falter. In other cases, however, the initiative can survive and be sustained even with chief executive turnover—largely due to continued, strong leadership. The goal of a serious leadership effort is well beyond a boosters’ type of support. Rather it is in inculcating IRM into the culture of the organization.

Visible and constant support is required throughout the risk management implementation. Practical examples of leadership support include:

- Making strategic changes in organization structure to facilitate risk discussions;
- Appointing risk management champions to key leadership positions;
- Introducing risk management committees mandated with risk management responsibilities or expanding the role of the audit committee;
- Establishing performance agreements which hold executives accountable to manage both the risk management process and the risks that flow from it;
- Adequately resourcing the implementation and ongoing practice of risk management;
- Having the top leader serve as the Chair of the Audit Committee or a separate Risk Management Committee that is mandated and held accountable to manage risks;
- Meeting with senior managers individually to thoroughly discuss their risk management assessments and action plans; and
- Validating the quality and acceptability of their

Idea Source: Success Factors in IRM Implementation:

- **Top-down approach and management endorsement**
- **Execution on all management levels**
- **Full alignment with business planning and reporting**
- **Bottom-up reporting**
- **Risk management learning as an integral part of management meetings**
- **Driver function on process and content**
- **Recognized centre of expertise (in house or**

manager's risk analysis and action plans, and then demanding regular risk information and using it in a systematic and long-term fashion.

While executive leadership of the organization must demonstrate commitment, leaders from the program and business lines must also “walk the walk.” Personal involvement in sponsorship was deemed essential. That is, active participation by leaders in training, risk assessments and risk discussions; assigning risk accountability; and ultimately allocating resources to implementing and managing risk. Leaders must really want to know the risks and what they mean. This dialogue ensures positive synergy in understanding where the leadership wants to go and the risks to getting there.

A sure way to kill a risk program is not to use—or not be seen to use—the risk information in decision-making. A common truth in the implementation of almost anything in an organization is that staff are adept at identifying true commitment versus pretence. They can also readily identify the flavour of the month issue that they will have to ride out.

The goal for effective leadership is to create an environment where people are encouraged to identify risks and possible solutions. Link this to the reality that effective IRM takes time and some level of strategic patience. Therefore, a sure way for a leader to kill IRM is to over-react to the first wave of risk assessments that will probably have some element of ‘garbageing in’ in them. Of course, it can equally argued that consistent training and coaching will avert a wave of Chicken Little risk assessment. Leaders also have to find a way to both thank the messages but also reward those with the courage to raise issues. This is, of course, the standard early wins strategy that is so important at this stage.

Idea Source r: “Avoid alarmist approaches that paint everything red and ignore the existing controls and safeguard systems: force prioritization. This is where leadership really comes into it.”

The bottom line is effective leadership means hands-on leadership throughout the organization, for both implementing risk management practices and managing risks as an integral part of management. Take the main pointers from the Rickover list of what a leader has to do and fill in the blanks. Here are also some good questions to ask yourself as a leader in trying to inculcate IRM into your organizations:

- Have I made it clear what we want?
- Have I made it clear that I am serious and in this for the long haul?
- Have I put the structure in place that will succeed?
- Do I have the right people on it?
- Am I paying enough attention at the right time?
- Am I rewarding the bad news as well as the bad?
- Am I holding the right people accountable?

The Leadership Checklist: The Rickover Way

It is hard to beat the way in which Admiral Hyman Rickover, legendary head of the American nuclear fleet defined the elements that you need to lead. They apply directly to what you need to lead the implementation of IRM:

- Ownership: IRM belongs to the leadership not the specialists
- Responsibility: taking on responsibility for the end results
- Attention to Detail: not getting lost in the weeds, but being able to tell one from the crop
- Priorities: making IRM a priority and holding to it
- Knowing what's going on: combining knowing your way around a balance sheet with knowing your way around your business and making sure both are integrated into IRM
- Hard work: implementing IRM begins with senior management time and attention
- Checking up: holding people to account, demanding results and remembering to come back to directions given to make sure they were carried out.
- Facing the facts: IRM only works when the bad news is faced up and dealt with and neither punished nor rationalized

Theodore Rockwell, *The Rickover Effect*, 1992

Assigning Responsibilities

Assigning responsibilities is an integral part of implementing IRM. There will be responsibilities for implementation, but also responsibilities within the continuing operation of IRM. The goal is to ensure that responsibilities are clearly delineated and sustainable. Therefore, the actual implementation of IRM cannot be left as a 'corner of the desk' piece of work for a senior officer. In fact, there have to be two kinds of responsibilities within the implementation framework: championship and project management. Ideally, the champion will be a member of the executive committee, will chair a form of implementation committee and provide ongoing project support. The project manager or risk manager will absolutely need that support.

There are some pivotal roles that need to be defined:

- CEO
- Role of the executive committee
- Risk champion
- Unit responsible for overall implementation
- Creation of special committee of EC to oversee IRM

- Role of individual managers
- Role of specialist units versus operational ones
- Role of the internal auditor

Your organization's risk policy will, to some extent, outline responsibilities. One statement that you do not want to see (and that has shown up all too often) is: "We are all responsible for risk management." While that is broadly true in the sense that all members of the organization need to be alert to risk and be comfortable communicating it within the organization, such a general statement means that the specific tasks of implementation will not be sufficiently well defined to actually get done.

Sample Assignment of Roles and Responsibilities

This was adapted from an excellent paper An Integrated Risk Management Framework for Small Agencies, Prepared by Consulting and Audit Canada, March 2004

Specific responsibilities would be assigned as follows:

The **Executive Committee** is responsible for:

1. providing direction on risk management, including risk tolerance;
2. identifying and reporting the Department's risk profile, including significant risks and the strategies used for their management;
3. ensuring that strategic risks are identified, assessed and managed;
4. providing leadership on risk management and assigning departmental risk roles within the context of corporate governance;
5. sending the message from the top that IRM is a valuable discipline for understanding and dealing with uncertainty in decision-making; and
6. ensuring a supportive learning environment and appropriate communication exist for risk management.

Branch Directors General are responsible for:

1. incorporating IRM into the branch's management framework;
2. ensuring that significant risks are explicitly identified in the agency planning system and that they are managed;
3. providing a supportive environment that encourages effective risk management, sensible risk taking and learning opportunities;
4. providing clear direction on risk tolerance levels;
5. explicitly understanding and managing the level of risk associated with branch policies, plans and programs.

Operational Managers / Directors are responsible for:

1. explicitly assessing and managing the level of risk associated with their operations and contributing to the explicit assessment and management of the level of risk associated with branch policies, plans and program;
2. ensuring that there is appropriate ongoing risk management planning, communication, training, control and monitoring.

Specialists are responsible for:

1. ensuring that both central agency and agency policies on risk management, and senior management objectives, are respected when providing policy and related advice, guidance and assistance.

All Employees are responsible for:

1. staying informed on risk management issues related to their operations; and
2. considering risk as part of every business decision and taking prompt action to manage risk (including communicating information on risk) in accordance with direction on risk tolerance.

The Internal Auditor is responsible for:

1. conducting audits and reviews on the application of the IRM Framework; and
2. providing assurance on all aspects of risk management strategy and practice in the Agency (Risk-based Audit Framework).

The **Planning Directorate** is responsible for:

1. providing functional support to agency managers implementing IRM;
2. annually updating the IRM work plan and Corporate Risk Profile;
3. developing a corporate communication strategy for IRM;
4. maintaining the IRM Framework and Policy and monitoring their application; and,
5. maintaining the risk repository.

Sample Implementation Plan

1. Purpose: Focus here on the policy decision or business direction. Set this firmly in your organization's decision-making process.

2. Approach: Here you switch from why to how. This section will set up the overall approach of the implementation project. Sub-units of this section should include:

Time perspective: clear focus on quick results or process of building through experimentation and learning

Use of internal resources versus or with the addition of external resources, or entirely external in project phase

Risks, obstacles and supporting strengths

End state when the project ends and sustainability within organizational framework kicks in

3. Project Roles and Responsibilities: Here the structure of the implementation project have to be defined. Governance for the project and of the project need to be clearly set in place. Some of the common elements are:

- Project Head or lead
- Project oversight committee or group
- Working groups
- Role of line management

In addition, it is important in the Plan to build in a linkage to the organization's senior management through regular reporting.

4. Project Costs and Funding: This needs to be defined at the outset, as best you can. Implementation is not costless, nor can it only be a 'corner of the desk' effort, added on to other duties. Costs of the following will have to be addressed and decisions made:

- Project office (if set up) or cost of consultant
- Training material, development and delivery – staff or external
- Systems requirements – often this has to be scoped, but even that costs money

5. Tasks, Timeframes and Delivery: A list of specific tasks, who is to do them and be contacted for them, the hours required for all individuals involved, key milestone dates for accomplishment of tasks or parts thereof, and concrete deliverables, where applicable. It is preferable that a going-in draft GANT Chart of some kind be created.

Idea Marketplace: Some Leading and Learning Practices in Implementing IRM

This section was adapted from several very useful reports on leading practices in implementing IRM:

1. **"Best Practices in Risk Management: Private and Public Sectors Internationally"**, a 1999 report done for the Treasury Board of Canada, available in full at www.tbs-sgc.gc.ca
2. **"Review of Canadian Best Practices in Risk Management"** prepared by KPMG, 1999,
3. **"Risk Management: Moving the Framework to Implementation: Keys to a Successful Risk Management Implementation Strategy"** – a joint Deloitte/ Conference Board of Canada study conducted by the author in 2004, available at <http://post.queensu.ca/~grahama>

This list is necessarily a summarized version of these and other studies. It also contains ideas that may well apply in one environment but not others. Wherever possible (outside of direct attributed quotations), the term 'best practise' is avoided as it is very difficult to apply the word best from one set of circumstances to another. That is for the host or implementing organization to determine. The author prefers the term 'leading practices' as being worthy of note and possible consideration.

Practice Area I: Focus on Culture

The predominant practice for integrating risk management is to build an organizational culture in which risk management is seen as a normal way to do business. Many organizations find that this has to go hand in hand with developing and issuing extensive policies and procedures. Management of risk has to be embedded in the management philosophy.

Employees become risk managers when they take responsibility for their actions and outcomes. You cannot, however, make the assumption that employees intuitively understand the organization's goals and work towards them. Therefore, steps have to be taken and then measured to ensure that employees understand the organization's objectives, its understanding of its risks and what has to happen to manage them.

Idea Source r: "The only way you really manage your risks is to get the conversation beyond total risk aversion or the notion that all risk can be eliminated. Talk to the elephant in the room."

Examples of useful practice in this area are:

- Instilling a "sense of excellence" in the culture which encourages people to seek solutions and talk honestly about where they need help. This takes 'modeled behaviour' on the part of managers.

- Making sure you know what staff understand about the organization's direction through such tools as surveys, feedback sessions and external reality-check-type audits,
- Developing loop-back communication systems such as internal blogs, info@ e-mail destinations, e-news spots, websites that encourage debate on risks and organizational direction,
- Involving all staff in risk management activities through committees and holding meetings at different work sites.

Sometimes, the culture has to be developed. Practices to achieve this include:

- Setting up the risk management unit as a centre of excellence to spread risk management procedures and practices across the organization. The aim is to encourage people to be their own risk managers with the risk management department acting in a support capacity.
- Staff the risk management unit with up-and-comers from a variety of units across the organization,
- Recruiting on attitude that focuses on a preparedness to take in the bigger picture in the work setting and to see risk as something to manage, not something to seek out recklessly or to avoid absolutely.
- Develop internal leading practice and learning practice to help others who face similar issues. This is particularly useful for multiple office organizations. Just remember: do not bureaucratize this. Setting up recognition and reward initiatives that encourage employees to manage risks and take advantage of opportunities.
- A really effective tool in building an understanding of a risk management culture is stories – “We did this here and it worked”. Find ways for people to get together and talk things through. Some examples:
 - End of season get-togethers where the major events of the season are discussed,
 - Post-incident debriefings without formal reports that let people suggest how to do things differently the next time
 - “Chow down” sessions of mixed staff to discuss problems that they are having and what they are doing about them
 - Incorporated actual case practice into risk management training: this takes a commitment to having continuing training using trainers on a consistent and long-term basis who can pick up ideas from one session and incorporate them into another session.
- Implementing remuneration packages that discourage reckless risk taking. For example, some securities traders have moved to basing traders' remuneration on a formula which compares their profits to those of a benchmark reflecting returns in the market as a whole.
- Evaluating employees' performance in managing risks, through the performance appraisal process.

Idea Source: Risk management needs expertise not experts. Make sure that IRM is not isolated into one unit, even if you need that unit to move forward. Bring in all types of staff into that unit.

- Defining effective risk management understanding and practice as part of the requirement for all management positions.
- Reinforcing ethics and values by issuing a written code of ethics or communicating them through training, meetings or workshops.

Practice Area 2: Risk Championship

We have already said that the support of senior management (and/or the governing bodies such as the Board of Directors) is essential. So, how does that happen? As a start, senior management and the Board must be aware of and understand risk management. A sign that you have it wrong is if there is a real movement within the middle ranks of the organization towards IRM and senior management or your Board is absent or surprised or shows no sign of understanding the language and use of IRM.

Idea Source: “Managing risk is not just a discussion item for management committees behind closed doors.”

There is a wide variety of ways in which the senior leaders are involved in risk management. However, underlying these ways is the role of senior management and the board to send the message internally and externally about the importance of managing risk. Also, it is important that other managers, stakeholders, and employees see their involvement. Managing risk is not just a discussion item for management committees behind closed doors.

Ways that the senior management and Boards can lead risk management initiatives include:

- The risk management group uses senior management as sponsors to ensure the risk management message is taken up by their direct reports.
- The CEO attends each meeting for implementing risk management processes. The Chief Financial Officer of the organization is the first senior manager to develop an action plan for an item emerging from a risk workshop.
- Senior Management devotes a day of its annual strategic planning process to identifying and quantifying risks at a strategic level.
- Senior executives sit on an internal control committee and are tasked with providing their department heads with the appropriate internal control mechanisms.
- Senior management regularly review information on those operational incidents that they deem important. This demonstrates a focus not just on the so-called strategic and external risks, but those risks arising from the day-to-day internal activities of the organizations.
- Board members or senior managers are asked to think of one risk that kept them awake at night. (Be a little cautious of this term as it implied that you work

Idea Source: “The manuals can be beautiful. The real question is consistency and culture across the organization over time.”

- with a bunch of worry warts. Find the terminology that works for you. For instance, try: What is that top of mind issue that keeps coming back?).
- A safety oversight board, a subsidiary of the main Board of Directors, reports monthly to the Board of Directors on performance in health, safety and environment.
 - Board sign off for new business cases which must include a risk analysis.
 - A (external) Council has set the parameters which the risk assessment team uses.
 - Create a Risk Management Committee of the Board: this will depend on the way the Board works, the role of the Audit Committee and the dynamic in place.

Practice Area 3: Risk Tolerance

Setting risk tolerance is another important leadership role. In fact, once the IRM is up and running, setting and adjusting tolerances is the key role. This is seldom a one-time, cut and dried process as we will discuss in **Section 5**. Here are some potentially helpful practices that have been used for this:

Idea Source: It will surprise you to see how many tolerances you have already in place or have established for you. Build on those.

- Ensuring that there are clear understandings of the use of risk matrices,
- Developing a risk tolerance discussion in the risk identification and assessment process,
- Gathering together information about tolerances that are already used within the organizations, e.g. control frameworks for financial transactions, safety incident reports and accident levels, budget limits, specific operational tolerances such as level of production versus plan, overtime reporting.
- Develop a hierarchy of reporting that stresses risk levels, thereby signaling that increased management attention goes to those risks that cross tolerance levels.
- Workshops are another way to develop and communicate risk tolerances in areas where measurement is difficult or there is uncertainty.
- In a similar vein, canvas opinions on risks as part of the risk assessment phase, but ensure that the players interviewed clearly articulate what would be acceptable and what not – roll these up for senior management to confirm or redirect the tolerances: this may be source of surprise for senior managers.
- In risk discussions and exercises, insist that those defining risks also add in the time dimension: when do we think this will happen and for how long. This introduces the notion of ‘stacking risks’ in the sense that a long-term risk or one with a long-term likelihood can be subject to quite different tolerances and approaches than a short-term one.
- Before making any decisions on risks, determine your risk capital available: that is the amount of available capital (through credit, held in reserves or not allocated for other purposes) that could go towards mitigation.
- Above all, avoid asking “What is your risk tolerance.” You will get a series of possible answers that seldom answer the question, such as: none, don’t know, 3.988789 or very little. You create risk tolerances through experience.

Practice Area 4: Communications

Effective communication is necessary for IRM to succeed. IRM involves many internal business processes, but it also involves stakeholders and overseers. Therefore, assume going-in that an open approach with a strong effort to establish both good communication flow and commonly available communication tools will be part of the implementation work.

Examples of effective communication are:

- Using the development of a risk management policy as a communication and interactive process to engage all parts of the organization: consult and clarify before the get-go.
- Establishing a website with risk information as a training tool,
- Using the intranet to communicate the organization's efforts and involve all employees in managing risk.
- Appointing managers whose task is to communicate risks to employees and engage employees in the risk identification process.
- Holding quarterly meetings of a risk management committee to review and discuss the organization's exposure and protection measures.
- Using the risk management function to communicate objectives.
- Promoting awareness of risk management issues through monthly, quarterly and annual reports..
- Making presentations to senior management and/or the governing body on the risk management process.
- Encouraging people to discuss anomalous outcomes (avoid words like: mistakes, failures to perform, etc – these are part of the blame cycle not the risk cycle) in a predictable and regular way..

Practice Area 5: Teams and Committees

Informal and formal teams are a mechanism that many organizations report they are using to implement and then manage risk. Teaming brings to light the dynamics between disciplines, brings together various risk attitudes, and brings fresh thinking to issues, opportunities, strategies and solutions. It is a way to focus diverse disciplines on common objectives, one of which is minimizing risk. Teams provide balance. Also, teams pollinate a concern for risk management throughout the organization, rather than being the concern of a function or discipline. While the practice of teaming is recognized as a "best practice", there was no common practice concerning the composition of the team.

A risk management implementation team should have certain characteristics:

- Inclusive: line management, treasury, audit, compliance, public relations, human resources and risk management professionals should all be involved.

- **Guided:** as this may involve major process and behavioral changes, senior managers have to regularly review and give the work of the team an extra boost of support or course correction-type guidance; do not leave them alone .
- **Resourced:** make sure they have the resources they need to get the whole job done; this will include time, access to consultants, training funds, funds to develop materials and disseminate them, web-building capacity,
- **Accountability:** an implementation team, always a high-energy and exciting prospect for those involved also has to have some accountability going-in; it has to be more precise than simply an instruction to go in there and get it done; it has to focus both on successful process, set limits and define outcomes in concrete terms.
- **Coverage:** senior managers have to be there for the team when the going gets rough and the going will get rough.
- **Governance:** the team has to know how it gets decisions made or gets its own direction clarified; drift is deadly.
- **Time Limitation:** teams that go on forever develop **Groundhog Day Syndrome** (blame the author for this term) in that they continuously return to the same issues without settling them. Set a time limit.

Practice Area 6: Develop and Use a Common Language Set

In order to IRM into other management processes, the terminology should be easily understandable by managers. The approaches should also be simple to understand and use. By developing a common business risk language, managers can talk with individuals from the boardroom to the boiler room in terms that everybody understands. This is important also in cases where everybody is expected to manage risks.

The risk management approaches and processes must be simple to be accepted by business management. Complex and overly intellectual tools will prove to be unsuccessful. Though the process must be simple and useful across units, the process should not be oversimplified. The designers of the process must balance simplicity with usefulness.

They also must make these working definitions available in training, manuals and on the website.

Risk language must also be able to withstand the media test: does any of this make any sense when you say it in the real world or on television? The language must not be so arcane as to suggest a cover-up or complexity that cannot readily explained to important audiences.

Practice Area 7: Establishing a Corporate Risk Management Function

Once the decision is made to proceed with IRM some functional support has to be put in place. This will have to certainly meet the needs of the implementation phase and also be seen as the start of the sustainability phase: permanent support. IRM is not something

that will survive on its own. It will need to be supported organizationally over time. How that is done will be a function of the size of the organization, the degree of attention to be paid on a regular basis to risk, other residual expertise and leadership within the organization.

In this regard, larger organization's efforts are headed by a Chief Risk Officer (CRO) who defines consistent approaches to managing risk. As the organizational risk champion, the CRO is responsible for providing leadership and establishing and maintaining risk awareness across the organization. The CRO might also set up risk control objectives, a risk framework, and design ways to measure risk. These senior risk managers must have strong persuasion skills. The risk manager must deal with business risks, not just insurable risks. In this way, their importance within the organization increases.

Other organizations will turn to the CFO to take on the risk leadership role. In others it will be the audit function. Smaller organizations have to ensure that they have continuing resources to support IRM.

How organizations structure themselves is always a mix of science, art and wizardry. Some things to consider when assigning this function, both on the implementation and on the sustaining side are:

- Does our array of risks require a special integrative function?
- Is there a conflict in your view between the audit function which often deals with risks, but retrospectively, and risk management, which should take a prospective role?
- Would have a specialized function isolate it from the business practices?
- Are there existing and useful structures in place, e.g. an Audit Committee that can take on this role?
- Would creating a specialist make others feel that they were off the hook or, alternatively, would they see this as a useful help?
- Can we afford it? Can we afford not to have it?

Practice Area 8: Communicating Risk Management Performance

Once you launch into an IRM, assume that it will be part of how you report your plans and your priorities. Ways of reporting will vary with organizations. However, in implementing IRM, be prepared to introduce a risk discussion in all your plans and reports on performance. Also, you may, in the implementation phase, want to put some particular emphasis on risk reporting. Some general tools are:

- An internal control department can present the results of monitoring risk.
- Each Operating Division can be required to prepare an annual report on its monitoring results for the

Idea Source: "If you have identified risks in your organization and fail to address them in how you spend your time and money, then you have created a new risk. Your reporting will tell you is this is so."

- Internal Control Department.
- Business Unit Managers can be required to report regularly to a Finance and Risk subcommittee of the Board. The reports outline the units' top ten risks and how they are managed.
- Managers advise the Board on the risks of their ventures and key shareholders/stakeholders have their say.
- Regular reporting requirements for external reporting can include sections on risks.

The principle rule here is that once an open reporting process on risk begins, it must cover not just identification but mitigation and monitoring.

Practice Area 9: Guidance

Providing guidance is an important practice for IRM. Guidance is provided indirectly (documents) or directly (advice). Any material that is developed should be useful, stand up to the 'BS' test (that stands for blatant superfluity) and be readily available. Here again, wheels do not need to be reinvented. There is plenty of material out there. Steal with pride.

Examples of this practice are:

- A guidance paper for government departments that are preparing public sector construction projects. "Essential Requirements for Construction Procurement" integrates value and risk management with project management.
- A tool kit for agencies or business units. The kit enables agencies to self-assess their position relative to current best practices. It also helps them move to the best practice using generic improvement strategies.
- Internal consulting services provided by the risk management unit.
- A forum of managers. Managers are able to identify their problems/risks. The forum allows the sharing of best practices. Action items are proposed to deal with the risk. Another advantage is all line managers are now aware of the risk and the action items.
- Buying this Manual and distributing it to all business units.

Practice Area 10: Training

Risk management training, as part of a corporate training curriculum, helps integrate risk. Topic areas include:

- risk assessments;
- best practices; I
- legislative requirements;
- safety;
- objectives for managing risk;

- risk-awareness training to ensure that all managers consider risk.

Practice Area II: Tools and techniques for putting risk management into practice

There are many tools to implement and operate IRM in the market today. **Section 5** will outline some prototype tools that can be adapted to meet the unique requirements of your organization. Here are some to consider.

1. Business risk mapping

Organizations are developing business risk maps to identify key business risks to the organization. This helps the organization understand and address its risks. Management must quantify the magnitude of the risks and measure their potential impact. The use of a broad scope framework permits the consideration of different types of potential risk in risk mapping. The use of a framework can influence a discussion on the sources and types of risks, for example, external, economic, market, credit, information, human resources and strategic. This brings a multi-disciplinary perspective for looking at the risks.

Examples of this practice are:

- **Listing the various business risks.** Then, the risks are charted into four quadrants depending on whether an event has a high or low probability of occurrence and whether it could result in a highly severe loss or a low severity loss.
- **Developing a risk map on one sheet of paper.** The map provides a comparative evaluation of all operational, financial, hazard and strategic risks that the organization faces. By comparing risks on a single matrix of severity and frequency, senior managers can see a complete picture of all the risks facing the organization and their interrelationship.
- **Developing a 'major matrix of risks'.** It captures the most damaging threats to the corporation. Senior management and the Board can use it in decision-making.

Simplicity underlies these approaches.

2. Modeling tools

Modeling tools enable managers to manage uncertainty. Scenario analysis and forecast models are the predominant tools. Examples of using modeling tools are:

- **Using scenario analysis,** decision makers can see the range of possibilities and consider changes that they would otherwise ignore. These scenarios can also be built into the organization's contingency plans. Scenarios can be documented and analysed using computer spreadsheet software.
- **Using statistical analysis and Value at Risk techniques,** managers can estimate the variability of future losses. They measure the impact of a potential loss on earnings or cash flow, include sensitivity analysis, stress testing, and various types of simulations.

- **Financial models** which dynamically simulate the various financial risks and the impact of various scenarios on portfolios of debt and equity.
- **Anticipating hazards** in the production process that could make the product defective, and then identifying the points at which they can be controlled.
- **Assessing technical risks during new product development** by identifying, early on in the project, the potential errors in the manufacturing process. This gives the time to address the consequences.
- **Accumulating past project experience** and extrapolating it to provide a synthesis of the likely risk impact of a particular project.

Some tools, such as scenario analysis, modeling, technical risk analysis, have broad applicability to management areas. Others, such as financial models, are less applicable to other disciplines.

3. Risk identification and assessment techniques

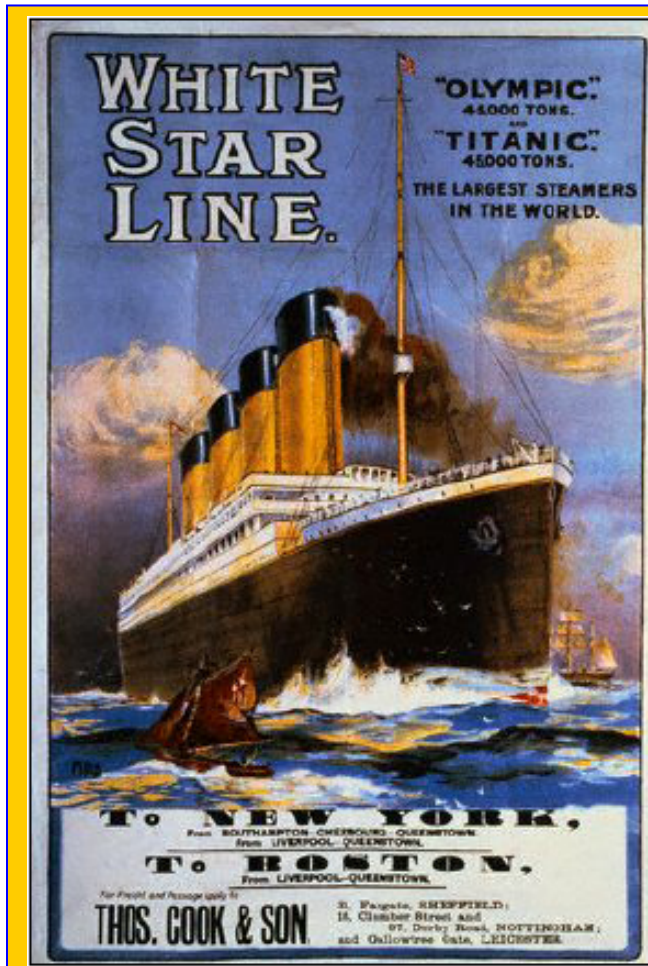
Techniques for identifying and assessing risks help managers identify where they should be focusing their attention and resources. There is no predominant technique.

Various techniques are:

- **Brainstorming groups.** Staff from multiple business units meet to brainstorm issues.
- **Workshops.** Organizations are starting to develop risk-focused facilitated workshops that help operating personnel determine and prioritize their objectives and identify and assess risks. Management in attendance would generally span a variety of areas.
- **Questionnaires.** Operating units are tasked with completing questionnaires on objectives and risks. For example, managers may annually update risks and progress on managing them.
- **Self-assessment.** Managers self-assess with support from Audit, Finance and an external accountant.
- **Control self-assessment (CSA).** Canadian Standards Association provides assurance that an end-point business objective will be met, taking into account controls and risks. Risk-focused workshops help operating managers determine and prioritize their objectives.
- **Filters.** Risks are evaluated against four filters: non-core function, low impact, risk well-managed, and low probability of occurrence.
- **Risk Quick Scan.** This is a technique for presenting risks (cost, timing, specifications, etc.) in such a way that the risks can be easily compared to each other in terms of probability and consequences. This is especially useful in projects.
- **Matrix to assess supplier capability.** The matrix is used to make an overall assessment of the ability of a potential supplier to deliver successfully the services/products specified in a contract. The matrix considers: the history and development of the supplier's business; legal background and capital structure; critical performance elements of the contract; management and employees; commitment, contingencies and litigation; financial viability.

- **Assessment matrix.** The matrix consists of a series of questions covering elements of risk management and internal controls. It also includes descriptions of best practices.
- **Risk identification templates.** Business units are given templates. These assist them in identifying and evaluating risks during their business planning process.
- **"Bottom up" risk assessments.** Operating managers identify and evaluate risks. These are then rolled up at the corporate level.
- **Value at Risk (VAR) model and worst case model.** These models are used to assess risk. The (VAR) model looks at the estimated potential loss in value of a position or portfolio within a specified period based on market factors. It allows the simultaneous trend comparison of, for example, currency fluctuations.
- **Prioritizing risks.** Based on their rank, the risks are addressed.

Avoid Complacency



When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like, but in all my experience, I have never been in any accident of any sort worth speaking about.

I never saw a wreck and never have been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort.

You see, I am not very good material for a story.

□

Edward J. Smith, Captain, RMS Titanic

© 2005 Christie's Images

Appendix: Sample Integrated Risk Management Policies

Sample 1: From a Business Emperor Mines Corporation Risk Management Statement

This statement provides an overview of the Company's risk management policies and its compliance and control systems.

Recognizing that there are inherent risks associated with mining the Board is responsible for overseeing the risk management activities of the Company. The management of risk is necessary to protect the Company's personnel, assets and reputation as well as the environment. It is also vital for effective business operation, achievement of objectives, reliable reporting and compliance with laws and regulations.

The implementation of the risk management controls and their effectiveness is the ultimate responsibility of the Board. The Board has implemented a combination of internal policies and procedures and engages external auditors to achieve an appropriate level of risk management and monitor developments in this regard.

Internal Policies and Procedures

The Board has implemented a number of risk management strategies covering areas of business risk relevant to the Company such as:

- o Occupational health & safety;
- o The environment;
- o Asset protection (insurances);
- o Continuous disclosure;
- o Securities trading policies applicable to directors, employees and key contractors;
- o Codes of conduct for directors and employees.

The various policies implemented by the board include mechanisms to ensure compliance, identification and regular reporting to the board of significant business risks and the management of those risks.

Financial Statements

Management shall ensure transparency and accuracy in all financial information for internal and external use.

Management shall ensure that financial information is timely, complies with statutory requirements and in particular, provides a true and fair view of the Company's financial status and performance.

The integrity of the Company's financial reporting relies upon a sound system of risk

management and control. Accordingly, the Managing Director is required to provide a statement in writing to the Board that the Company's financial reports

are based upon a sound risk management policy to ensure management accountability

The Company's Financial Statements are audited/reviewed by external auditors on an annual and semi-annual basis.

The Audit Committee assists the Board in this Policy by:

- o fostering in management personnel a culture of risk control and management, particularly on internal control and compliance;
- o overseeing the planning, implementation, establishment, monitoring, management, assessment and review of risk control management and information systems;
- o providing recommendations to the Board on the appointment and replacement or rotation of auditors;
- o meeting and liaising with external auditors

Occupational Health and Safety

The Board oversees risk control management and review of occupational health and safety issues.

Management is to establish and implement the Policy by establishing a system to identify, assess, monitor and manage risk by:

- o identifying and addressing risks at each Company project and setting up internal control and compliance systems;
- o devising and establishing a system for the ongoing review of risk control management and information systems for prompt response;
- o reviewing the systems and their compliance as well as their overall effectiveness not only for continuing or evolving risks but also for new risks;
- o reporting periodically on risk control and compliance as well as management information systems to the Board.

Management, staff and contractors of the Company are required to ensure that Occupational Health and Safety practices are of the highest standard.

Environment

The Board oversees risk control management in connection with environmental concerns.

Management is to establish and implement the policy by establishing a system to identify, assess, monitor and manage risk by:

- o identifying and addressing risks at each Company project, including consideration of environmental concern and setting up procedures for ensuring that appropriate action is taken to ensure compliance with relevant legislative and community expectations;
- o devising and establishing a system for the ongoing review of risk control management and information systems and reviewing the systems and their compliance and their overall effectiveness not only for continuing or evolving risks but also for new risks;
- o reporting periodically on risk control and compliance as well as management information systems to the Board.

Management, staff and contractors of the Company are required to ensure that Environmental matters are addressed at all times in accordance with the highest standards.

Guidelines for Risk Management

The Board will oversee the process that management has in place to identify business opportunities and risks. The Board shall be responsible for overseeing management and holding it to account.

The Board will consider the extent and types of risk that is acceptable for the Company to bear and will monitor management’s systems and processes for managing a broad range of business risks.

The Board will, on an ongoing basis, review with management how the strategic environment is changing, what key business risks and opportunities are appearing, how they are being managed and what, if any, modifications in strategic direction should be adopted.

The Board approach to risk management shall be guided by the following criteria:

Identification	Clarify the Company’s core values for the organization and identify these clearly.
Analysis	Examine the core values and develop a model for identifying events within the organization that could adversely impact on the core values.
Assessment	<p>Allocate priorities to the risk rated items and integrate these items within the existing (and/or contemplated) operational plans and structures including by reference to the following areas of opportunity/risk:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Strategic: for example, market conditions, new competitors, political/regulatory environment. <input type="checkbox"/> Operational: e.g. business processes, technology, human resources, business interruption, environmental issues, health and safety issues, crisis management. <input type="checkbox"/> Leadership: e.g. ability to innovate and motivate throughout the organization, choice of chief executive officer. <input type="checkbox"/> Partnership: e.g. ability to choose appropriate alliances, partnerships and make them work well. <input type="checkbox"/> Reputation: eg quality of products and services, consumer advocacy, public perceptions, illegal or unethical conduct, fraud.

From: <http://www.emperor.com.au/aboutemil/corporate.html>

Sample 2: From a Public Sector Organization:

**Thames Valley University
Risk Management Policy**

Definitions:

Thames Valley University - “The Institution”

Thames Valley University’s Risk Management Policy - “The Policy”

Purpose of this document

1. The policy forms part of the institution’s internal control and corporate governance arrangements.
2. The policy explains the institution’s underlying approach to risk management, documents the roles and responsibilities of the Board of Governors, the senior management team, and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.
3. In addition, it describes the process the Board of Governors will use to evaluate the effectiveness of the institution’s internal control procedures.

Underlying approach to risk management

4. The following key principles outline the institution’s approach to risk management and internal control:
 - the Board of Governors has responsibility for overseeing risk management within the institution as a whole
 - an open and receptive approach to solving risk problems is adopted by the Board of Governors
 - the Vice-Chancellor and the senior management team supports, advises and implements policies approved by the Board of Governors

- the institution makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks
- Pro Vice Chancellor Deans and Head and Directors of all departments are responsible for encouraging good risk management practice within their faculties and departments
- key risk indicators will be identified by the Board of Governors acting on the advice of the Vice Chancellor and closely monitored on a regular basis.

Role of the Board of Governors

5. The Board of Governors has a fundamental role to play in the management of risk. Its role is to:
 - a. Set the tone and influence the culture of risk management within the institution. This includes:
 - determining whether the institution is 'risk taking' or 'risk averse' as a whole or on any relevant individual issue
 - determining what types of risk are acceptable and which are not
 - setting the standards and expectations of staff with respect to conduct and probity.
 - b. Determine the appropriate risk appetite or level of exposure for the institution.
 - c. Approve major decisions affecting the institution's risk profile or exposure.
 - d. Monitor the management of fundamental risks to reduce the likelihood of unwelcome surprises.
 - e. Satisfy itself that the less fundamental risks are being actively managed, with the appropriate controls in place and working effectively.
 - f. Annually review the institution's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

Role of the senior management team

6. Key roles of the senior management team are to:

- a. Implement policies on risk management and internal control.
- b. Identify and evaluate the fundamental risks faced by the institution for consideration by the Board of Governors.
- c. Provide adequate information in a timely manner to the Board of Governors and its committees on the status of risks and controls.
- d. Undertake an annual review of effectiveness of the system of internal control and provide a report to the Board of Governors.

Risk management as part of the system of internal control

7. The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the institution to respond to a variety of operational, financial, and commercial risks. These elements include:

a. Policies and procedures.

Attached to fundamental risks are a series of policies that underpin the internal control process. The policies are set by the Board of Governors and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. Reporting.

Comprehensive reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the senior management team and the Board of Governors if appropriate.

c. Business planning and budgeting.

The business planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting business plan objectives is monitored regularly.

d. High level risk framework (fundamental risks only).

This framework is compiled by the senior management team and helps to facilitate the identification, assessment and ongoing monitoring of risks fundamental to the institution. The document is formally appraised annually but emerging risks are added as required, and improvement actions and risk indicators are monitored regularly.

e. Faculty risk frameworks.

Heads of faculty develop and use this framework to ensure that fundamental risks in their faculty are identified, assessed and monitored. The document is formally appraised annually but emerging risks are added as required, and improvement actions and risk indicators are monitored regularly by business units.

f. Audit Committee.

The Audit Committee is required to report to the Board of Governors on internal controls and alert governors to any emerging issues. In addition, the committee oversees internal audit, external audit and management as required in its review of internal controls. The committee is therefore well-placed to provide advice to the board on the effectiveness of the internal control system, including the institution's system for the management of risk.

g. Internal audit programme.

Internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation.

h. External audit.

External audit provides feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

i. Third party reports.

From time to time, the use of external consultants will be necessary in areas such as health and safety, and human resources. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control system.

Annual review of effectiveness

8. The Board of Governors is responsible for reviewing the effectiveness of internal control of the institution, based on information provided by the senior management team. Its approach is outlined below.
9. For each fundamental risk identified, the board will:
 - review the previous year and examine the institution's track record on risk management and internal control

- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.
10. In making its decision the board will consider the following aspects.
- a. Control environment:
 - the institution's objectives and its financial and non-financial targets
 - organisational structure and calibre of the senior management team
 - culture, approach, and resources with respect to the management of risk
 - delegation of authority
 - public reporting.
 - b. On-going identification and evaluation of fundamental risks:
 - timely identification and assessment of fundamental risks
 - prioritisation of risks and the allocation of resources to address areas of high exposure.
 - c. Information and communication:
 - quality and timeliness of information on fundamental risks
 - time it takes for control breakdowns to be recognised or new risks to be identified.
 - d. Monitoring and corrective action:
 - ability of the institution to learn from its problems
 - commitment and speed with which corrective actions are implemented.
11. The senior management team will prepare a report of its review of the effectiveness of the internal control system annually for consideration by the Board of Governors.

From:

http://www.tvu.ac.uk/files/The_University/Governance_and_legal_framework/Risk_management/Risk_Management_Policy.doc

Sample 3: From a Voluntary Organization

Policy

We aim to use the world's best practice in risk management to support and enhance our activities, in all areas of our organization.

- We will ensure risk management is an integral part of all our decision-making processes.
- We will use a structured risk management program to minimize reasonably foreseeable disruption to operations, harm to people and damage to the environment and property.
- We will identify and take advantage of opportunities as well as minimizing adverse effects.
- We will train our people to implement risk management effectively.
- We will strive to continually improve our risk management practices.

Responsibilities

- The Chief Executive Officer is accountable to the Board for the implementation of the risk management process and ultimately responsible for the management of risks in business.
- All personnel are responsible for managing risks in their areas.

Process

- A risk management systematic process has been established, based on the Australian Standard AS/NZS 4360:1999.
- Everyone involved with the application of risk management should use this process for guidance.

Monitoring and Review

- The Board will monitor and review the implementation of the risk management program.
- The Chief Executive Officer will facilitate the development of a common risk management approach across areas of our business by:
 - Implementing the risk management program;
 - Sharing information with broad applicability across all areas;
 - Reporting on the progress of implementing the risk management program.

Section 5 – Using Risk Management Tools

What This Section Does

There is a set of generic risk management tools that are in inherent part of developing and effectively using IRM. They will look different depending on design and the degree to which you want to create your own look. This Section reviews the basic tools and makes some recommendations about how to get the most out of each step. The following forms and processes will be discussed here:

- Risk Assessments: identifying and assessing your risks
- Risk Tolerance and Appetite
- Evaluating Risks: risk ranking and models for decision-making
- Risk Priorization
- Report Formats

Certain Maxims about Process

A consistent theme of this Manual is that you do not start IRM unless you are going to finish the process and sustain it within your organization. Of course, you can bail out at any time if it does not work for you. That is a business decision with attendant consequences. However, in moving forward an IRM agenda, the following steps have to be seen as more than just forms to fill out. In fact, the forms and charts presented are merely possible examples. You can adapt the basic steps to meet your needs and to the degree that you want a Made-in-My-Neighbourhood look and feel. However, the message here is deeper than that. Each step is an integral part of the process. Just as the Canadian Standards Association 1997 *Risk Management Guidelines for Decision Makers* points out, the steps, with whatever name works for you, are pretty clear. What is absolutely necessary is that each step be accompanied by decision-making, validation and evaluation to make sure that you got it right enough (note that enough – perfection is for angels, not mere mortals) to stand by it and go on. Many organizations report that they did not get their first steps right and either repeated them within the cycle, started the cycle all over again or were wiser the next time. Creating and inculcating IRM into your organizational culture means accepting that the individual effort of the moment may not get you where want to go. Direction and flow are important here.

The next maxim is that this process requires two-way if not multi-party communication throughout to work. This means that senior managers have to feed back and guide the process. Particularly at the outset, many organizations make the mistake of seeing the process of strictly a bottoms-up, democratic one or one that will use staff experts in audit, finance or planning (all good people and needed in the process). Both of these speak to a certain managerial style best characterized as: “Go out and get me some.”

rather “Let’s build this together.” Take note of this where stakeholders, those in governance roles and the public are involved. Two-way communications means that, at each step in the process, senior managers have to feed back to participants a number of messages:

- We have gathered your views and advice and are going to now bring the many perspectives into one place: you will hear back from us shortly,
- We see the priority issues as the following and intend to address them
- We see those risks you identified as being handled by current control systems adequately. We will monitor them, but not take any further action
- We have set the following parameters and tolerances to help you and ourselves start to address our priority issues.

Mostly, however, two-way communication takes the form of those invited into the process to hear and to be heard at each step in it.

What does this mean for the management of the IRM implementation process and these steps which follow? Simply, as was pointed out in the previous Section, this is not a free floating enterprise. Rather, it requires focused management that recognizes that there are risks in risk management. The explicit application of the simple formula of risk assessment, setting tolerances, evaluating risks, managing and monitoring risk also entails, at each step the evaluation of the results, feedback and correction, decision to move forward.

Risk Assessment

Perhaps the going-in maxim about IRM and risk assessment is, do this right, but do not get stuck here. Often one will find risk assessment attached to strategic planning documents or reports, plugged in as if an afterthought, perhaps serving some due diligence requirement or some maxim from on high that “We will do risk here.”

Idea Source: Remember, research clearly shows that the vast majority of systems failures arise through human and organizational problems, not technical ones.

Regardless of the process of risk assessment that you follow, you will need to adopt some common practices and guidelines. Some of the most salient are:

- Seek out a variety of sources for risk identification, most notably seeking out views from unorthodox viewpoints about your business or organization. In other words, avoid the dangers of **samethink**.
- Make sure that those whose views are sought understand what you mean by risks. This will avoid those being involved simply bringing known issues to the table or importing their particular baggage, although that is pretty hard to avoid. After all, if you ask someone’s opinion, you will probably get it whether you really want it or not.
- Remember, you are harvesting ideas. Do not panic. Do not rush to judgement. Make it clear to those consulted that the ultimate decision about the assessment of a risk and whatever, if any, mitigation strategy you put in place will be made by

- those responsible for running the organization. This is not a voting matter, although intensity of feedback and frequency of identification is certainly material.
- Understand that there are important psychological factors at play as people identify risks and their relative probability and importance. For instance, there is a well established tendency for people to identify risks similar to events that have recently occurred. Equally true is the fact that people will minimize real risks as improbable simply because they happen infrequently. For instance, many people will identify the possibility of terrorism as high, even though it is modest if not inconsequential for most while they will minimize the possibility of being injured in a car accident, something that is statistically much higher than having an airplane fly in through your window. The bottom line is to drive the identification process to those risks that are:
 - Evidence-based
 - Relevant to the business you are in, and
 - Within the scope of the organizations competencies and capabilities.
 - Risk and risk assessment, in spite of all that is displayed here is a matter of educated guess-work that can be highly distorted by emotions and bias. This makes it quite like the rest of life, right?
 - Gathering and identifying risks often stimulate a rush to assigning relative values to them and getting into mitigation too quickly. Of course, an imminent danger is an imminent danger. However, many managers want to fix things and good for them. Put on the brakes unless you want to shut off further input.
 - In a similar vein, seeking input about risks means shutting up, at least for a while, so that those providing input are not cut off with something like “Well, you just don’t understand.” or “We have systems in place to take care of that.” The later is known as the Titanic rule: we have watertight compartments and are perfectly safe.

Idea Source: “The biggest challenge you will have is convincing risk management experts that they have emotions?”

What are the best ways to develop risk landscapes? The following is a representative list of the kinds of activities that will do this for you. At the end of the day, the risk identification process has to be sustainable and consistent. If it is done once and not to be repeated or left in that organizational limbo known as ‘under further consideration’, do not bother to start. Of course, it can be modified over time, adjusted to take into account what you learned along the way. For instance, there remains considerable debate about the notion of gathering all organizational managers in a room and undertaking a risk identification process. On the one hand, it does bring everyone face-to-face and gets them to use a common tool, such as the **Risk Assessment** form below. It also encourages group discussion. Reporting out, however, takes considerable facilitation. There is also a common tendency in such large settings towards the great common view of the world without appropriate push-back or demand for evidence to support the identified risks. Treated, however, as a significant but not conclusive input to the process, this can work. All eggs in one basket rules apply.

Here are some of the ways that organizations develop risk identification inventories:

- Annual general meetings of managers and staff, with the conditional notes above taken into account,
- Client, supplier, customer survey or consultations,
- Stakeholder consultations,
- For those organizations with internal risk management expertise such as a CRO, individual interviews,
- Seeking external advice such as consultants, experts or key industry or government observers.
- Risk surveys, using an adaptation of the tools below,
- Using your strategic planning process to introduce an organizational risk identification phase.
- Harvest information from your existing risk control and mitigation systems and identify trends. Some of these are:
 - Financial variance reports: are there consistent trends that clearly point to an underlying risk?
 - Post-incident trends reporting: are there common features of incident response, e.g. increased injuries using specific equipment, that form an important pattern,
 - Have a look back at your accident and ill-health records – these often help to identify the less obvious hazards.
 - Remember to think about long-term hazards to health (e.g., high levels of noise or exposure to harmful substances) as well as safety hazards.
 - Audit results, especially those involving the operational element: too many organizations fail to use these in an integrated way, linking many audits over time to see patterns.
 - Look at key management indicators for trends. For example, is there an increase in mid-career departures that indicates corporate raiding, workplace issues or failure to attract the best.
 - Compare performance against key industry standards. Is your organization performing well or not? Is the pattern consistent over time. Are you happy being number 4?

Idea Source: Completeness Counts:
“Completeness in risk or event identification is critical. Risks and events left unidentified are excluded from further analysis. Unidentified risks represent unidentified opportunities. Strategic risks should be explicitly identified even and some would say especially) if they are apparently outside the control of the entity.” - Practical Guidance: Seven Steps to Effective Enterprise Risk Management, The Paisley Group

Risk Assessment Form

Sources of risk	Nature and Evidence of Risk	Who or What is Being Affected?
People in the Organization		
Management		
Occupational health and safety		
Economic		
Legal		
Political		
Property and equipment		
Environmental		
Financial/market		
Natural events		
Internal Operations		
Suppliers		
Outsourced Partners		
Reputation		
Adequacy of Controls		

What You Need to Think About When Using the Process

This is not the one risk identification form. It is merely an example of the kinds of forms you can for risk identification exercise. You can always create your own or you can adopt a more randomized process. Some will argue that any kind of category will limit input. While that it is true, categories force people to think about risks in those areas. In other words, they can serve as a kind of prompt.

With respect to the categories, select your own. Some of the ones listed here, all of which come from the risk source map in **Section 2, Building the Business Case**, will

remain fairly constant in any organization. Therefore, you would expect to find some variant on such matters as financial risks, safety, people, etc. Some organization will, over time, develop more precise areas of concern, e.g. customer response and loyalty, staff commitment, cost of borrowing/equity market stability

Making Risk Assessments Real

What are the constraints to getting good risk identification? There are many, actually, and they come from quite different sources. Perhaps the first is a resistance to identifying a risk as it will be seen as a criticism of the organization or put it in a defensive posture. This is where good training and consistent management pay off. Increasingly organizations in both the private and public sectors are learning that dealing with client dissatisfaction is the way to improve delivery. Denial is the first sure step to towards organizational failure.

Idea Source: Don't give the bosses a set of risks that they cannot possibly do anything about.

Another important, and somewhat contradictory element of good risk identification has to be the demand for evidence that there is a real risk to the organization's goals and that the risk is one that needs to be realistically addressed by the organization. In simple terms, a risk is not a risk just because someone has a hunch or a feeling about it. These play their role in managing organizations, but not in IRM. It can be argued, however, that the obverse of this is equally problematic: acknowledging only risks with hard data, preferably financial information. There is a middle ground and you need to sort out in advance what good evidence would look like before engaging in a harvesting exercise. The best gong-in approach is to ask for whatever evidence that a risk exists and that it will have an impact on the organization or its customers or clients. For instance, at a recent conference of front-line managers in a first responder organization, several tables involved in risk identification chose climate change as a risk to the organization. This is a good example of a highly generalized phenomenon that is so pervasive that you wonder what one organization can do anything about it. The challenge for the facilitator in this case was to send the topic back (remember that issue mentioned at the beginning of this section) with a request that the participants focus not on climate change as a global threat but as a threat to the functioning of their organization and show what evidence was emerging, even anecdotally, that would merit it going forward. Rising to the occasion, the participants did provide some hard evidence of long summers, drier fields, water sourcing issues. Some of these were already in evidence. Some were potential risks that would have an impact on future infrastructure issues such as water storage and availability and burn testing. That group got sent to the bar first for good and precise evidence directly related to their organization.

The final way to make risk assessments real is to ensure that those providing the input get some form of feedback from senior management and those involved in managing the process. It would be fatal to the overall sustainability of the IRM implementation if, at this point, a senior person gets up and makes decisions about who is right and who is wrong. They have to show that they are willing to move forward with what they have been given. They should not accept all the assessments, but rather say that these are

part of the process. Where they see real problematic issues that may not be risks, but reflect some internal problems or conflicts, they are going to have move these off the plate. Where they see real 'ahas', special note needs to be made of these. They should focus on how the assessments will be moved to the next stage – ranking and evaluation.

Checklist: Warning Signs: Is Your Risk Identification Process Giving You the Best Results?

Here are some things to look for that tell you that the process you have is not really working in terms of being thorough or actually getting to the risks you need to address:

- **Paint Drying:** The results are predictable.
- **Same old, same old:** You are hearing the same discussions that have been going on within the organization for years.
- **Right risks, wrong decade:** Your risks smack of yesterday's problems and ways of thinking.
- Symptoms of **availability bias:** this is a term that means that people will tend to estimate risks and their impact based on readily available examples such as found in the media without actually knowing how serious the risk actually is to the organization itself. If you see a series of unusually events listed as risks, check last night's news.
- **Small sample, big problem:** While similar to the availability bias, this one is evidenced when people will use a small number of events to project a risk as larger in scale or universally applicable when it is an isolated incident or its recurrence is not material.
- **The Fix is Already In:** Risks are identified that are already in an existing plan or for which mitigation strategies or controls are already in place. This can also be a sign that the process did not adequately inform the participants of the current situation within the organization.
- **Unforeseeable foreseeable:** The input of risks is so vague that it cannot possibly be used, predicted, evaluated or even believed at times. You have to be careful here as there are low probability/high impact events that demand emergency and disaster planning that slip into this category. Yes, sometime an asteroid will hit earth. Where does fit with your business plan. On the other hand, an avian flu-type epidemic just may.
- **We're Just Fine, Everything Else is Down the Tubes:** Risks are identified elsewhere in the organizations broader universe but not at home, leading to a massive transfer of risk and no take-up of responsibility internally. That suggest a bias that declines effective internal review.

Risk Ranking and Evaluation

This portion of the Section will address three elements:

- Setting risk tolerances
- Risk evaluation formats
- Risk mapping

Risk Tolerances and Risk Appetite

This is an important section of the entire use of risk management tools. It is difficult to know where to place it as the concept of risk tolerance and its sidekick risk appetite is woven throughout the entire IRM process. How an organization views risk will vary from a risk seeking organization with a high risk appetite to a totally risk averse one with no risk appetite. Neither exist much in the real world as there things like trade-offs and reality that intervene at both demands limiting the scope of risk but also creating the absolute need to take risks. However, organizations that tend towards less risk will have accompanying tolerances that are different than those seeking risks.

The placement of this discussion is also important in that it is important to convey that organization set their risk tolerances in a complex and dynamic way. In fact, all organizations have an understanding of what they can do, get away with, would invest in, would establish a new program area in – all of which are part of risk tolerances. As well, risk tolerances are often just given to the organization in the form of regulations which set limits for various activities, in the form of credit limits which permit only such much draw-down before a further business review or in the form of a budget variance limit that would require a review of spending patterns in an assigned budget. These are all forms of risk tolerances inherent I the day to day management of organizations.

The final codicil is that risk tolerances will seldom appear in one place at one time. One of the real benefits of IRM is that it can build a risk tolerance grid, over time and with experimentation, that actually focuses on the principle risk tolerances that the organization needs to manage its array of risks.

What is Risk Tolerance?

Very simply, risk tolerance is the degree of risk that an organization is will to tolerate in a given situation. To be more precise in the context of IRM, risk tolerance is a measure or set of guidelines that provide direction to the organization about when a particular risk moves from being at one level of concern to another. These can be stated as part of the overall risk framework, but must be linked to key organizational objectives. You do not establish tolerances without some reference to the impact on the organization. It is therefore essential that the establishment of risk tolerances be seen as part of the leadership function of the organization.

Idea Source: User Warning:
You are entering the land of disclosure – be prepared and use your smarts in the process.

How Do You Establish Risk Tolerances?

The mechanics of establishing level of risk, be it called risk tolerance or risk appetite, might be seen as fairly straightforward. It requires a number of specific steps:

- Creating and adopting a common grid of tolerance levels,
- Developing a grid of risk areas that you apply the levels to, and
- Creating processes that populate the matrix with meaningful information that will guide the organization.

That all sounds simple, but it is not. First, creating risk tolerances exposes the unspoken rules and values that govern how organizations function. Further, this will require, in some cases, a level of precision that will make many uncomfortable. Finally, there is the danger of public exposure of such a grid and its inevitable misinterpretation by stakeholders and the media. However, it has been done and published. The world continues to turn for those organizations.

Creating a Common Grid

This Manual does not offer a pre-burned set of forms. Many good examples abound of risk tolerance grids. The number of levels you choose is a matter of organizational preference. What is important in terms of guidance to staff, your participants in the IRM process and, inevitably, the public is that a good effort be made to define and distinguish the various level. This is not easy. Here is a good example of a grid definition coming from the university section, specifically, the University of Alberta.

University of Alberta Risk Tolerance Grid with Definitions

The success of the University is a result of effectively managing key drivers of value, which in turn support the key strategic initiatives outlined in the 2002-2006 Strategic Business Plan. The University accepts an element of risk in almost every activity it undertakes. The critical question in establishing the University's risk appetite is "How willing is the University to accept risk related to each key value driver?" This in turn can be expressed in terms of a continuum.

Assessment	Description
High Risk Appetite 5	The University accepts opportunities that have an inherent high risk that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents(s) of regulatory non-compliance, potential risk of injury to staff and students.
Moderate Risk Appetite 4	The University is willing to accept risks that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents(s) of regulatory non-compliance, potential risk of injury to staff and students.
Modest Risk Appetite 3	The University is willing to accept some risks in certain circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents(s) of regulatory non-compliance, potential risk of injury to staff and students.
Low Risk Appetite 2	The University is not willing to accept risks in most circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents(s) of regulatory non-compliance, potential risk of injury to staff and students.
Zero Risk Appetite 1	The University is not willing to accept risks under any circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents(s) of regulatory non-compliance, potential risk of injury to staff and students.

Things to Note from this Example

There is a good effort to draw distinctions, but, like all gradients, the middle can get mushy. What is the difference between accepting some risk and accepting risk? That will require some further refinement.

However, the definitions do move clearly towards both extremes and are nicely focused on key elements of this sort of enterprise.

Note the use of colours. Be careful here. One simple question is why is the least acceptable kind of risk do often red? The easy answer is that red denotes danger. The problem with that is that is also ensures a preoccupation with the red parts and not the others.

Developing a Grid of Risk Areas

Here you have a number of choices. You can:

- Establish your areas based on key organizational objectives,
- Use specified risk areas arising from your risk assessment process, or
- You can focus on key client, input, or results areas

Using Key Organization Objectives

The fundamental basis of IRM is that it is about events or circumstances that can happen that will affect you achieving your goals. Therefore, there is one track of logic that suggests that risk tolerances should be set with the goals in mind and that individual risks then be rated against this direction. This can be done using language of appetite such as above or language of tolerance. To simply illustrate another methodology, the tolerance scale below is being used. An example of such a list could be:

Risk Tolerances Related to Organizational Objectives

Note: This is not taken from any organization in particular, but is an example of the kind of language that had appeared in a number of examples.

	No Tolerance	Serious Concern	Moderate Concern	General Tolerance	Highest Tolerance
Financial Stability	Oversight concern for financial integrity Budget overshoot Credit ratings downgraded	Financial statements subject to strong audit comment Not within budget Threats to credit rating	Audit comments on financial reports Budget pressures appearing	Financial Reporting Sound Positive audit reports Within budget	Sound Balance Sheet Within Budget Strong credit rating
Staff Engagement	Major staff moral and commitment now a persistent pattern. Attrition is so great that replacements cannot be found and turn away offers. Grievances preoccupy the organization and threaten to move into arbitration and	Staff moral showing a strong downward trend over many months Attrition generally across the organization creating operational pressure Grievances are increasing and more pervasive.	Staff surveys report staff concern about their alignment to organizational goals Attrition increasing, but in isolated areas. Grievances show an increasing pattern.	Staff commitment reported positive Attrition within acceptable and replaceable range Grievances occurring but not in large numbers	Staff report high level of commitment to work – multi-year pattern Very low level of attrition Low level of internal grievances

	external review.				
Client Satisfaction	Client satisfaction becomes chronic, downward over four months. Complaint responses are generating multiple complaints.	Client satisfaction trends down over two months. Backlog of complaints and internal responses are slowing. No aggregate learning from complaints.	Client satisfaction is stable, but not high. Response to problems is more of a complaints function, itself subject to complaints.	Client satisfaction rising over the past several months. Response times adequate. Some reporting of problems as a learning tool.	Client satisfaction high over time. Rapid and positive response to specific problems that arise. Treated as a positive learning tool.
Safety	AFSR 20% below standard.	AFSR 10% below standard.	AFSR at standard	AFSR 25% above standard.	Accident frequency and severity rates (AFSR) 50% above standard.
Reputation and Reliability	Negative mention in national and provincial media.	Negative mention in provincial media.	No references of either positive or negative nature.	Positive reference in provincial media	Positive reference in national and provincial media. Number of industry awards.
Quality Service Indices	Meets 50% of established indices	Meets 60% of established indices	Meets 70%	Meetings 80%	Meetings 95% of established indices

Things to Note from this Chart

You can and will need a mix of quantitative and non-quantitative indicators. Do not rush to numbers if they do not exist. They may develop over time. It is wise to seek out external standards, such as the quality service indices above. These would be derived from some form of industry-based association, benchmarking or comparative standards, e.g. performance across various governments.

Populate the Matrix with Meaningful Information

Most **CROs** (that’s Chief Risk Officer) will tell you that risk tolerance chart or matrices are not built in a day. Further, getting them right, even when there are available measures takes some time. Finally, they are absolutely necessary in some form in IRM, but how and when they are communicated is tricky. Why are they so important? It would be impossible to reasonably create any sense of priority of risks without a notion of what risk the organization is ready to tolerate. Further, setting priorities is where the

rubber hits the road in terms of organizational leadership of the IRM process. Ultimately, those who have worked in this area will tell you that it is an iterative process that involves a mix of science, art and informed guesswork. They will also tell you that once you have established a form of risk tolerance matrix, you will have to periodically update it.

The following are important sources of defining risk tolerances:

Use What You Have Already

- Financial information from both the budgeting/planning side and the actual performance side. This is rich source of information already in a format that provides important triggers for action. Such areas with existing financial practices that are useful are:
 - Variance of expenditure over budget
 - Variance of revenue over plan
 - Major cost shifts in vital input factors, e.g. fuel costs
 - Credit costs, availability and draw-down relative to overall worth.
 - Payment and related control errors.
- Operational information reports, such as:
 - Sales over plan
 - Production over plan
 - Incidents relative to anticipated results
 - Time lost in shut-down or repairs
 - Systems support performance
- Safety information
 - Accidents relative to previous period or industry standard
 - Reports of sick leave resulting from accidents
 - Systems failures, frequency, cost and duration
- Quality Information: Most organizations have some form of quality control system in place. The use of this information is ideal in settings reasonable tolerances for risk. In fact, it plugs in rather well and has proven to be the capstone of the use of such efforts.

Mention has already been made of controls within the financial systems. In fact, there are controls throughout the organization. These essentially are gates of performance that, once passed, call for great scrutiny and supervision of the transaction. That is the essence of a risk tolerance entrenched within the organization and should be a good starting point.

Seek Out Industry Standards

If you like, go ahead and reinvent a wheel that is already well designed and used elsewhere. There are a myriad of ways to reach outside the organization, but still find relevant risk tolerance information that would guide setting yours within the organization. Time and space does not permit a proper listing as there are so many, but here are some:

- Established benchmarking systems with comparable companies or governments,
- Industry-led associations that research and set performance standards,
- Accounting and financial management national and international standard setting organizations.

Anything that can stand close scrutiny, i.e., the public, media or lawyers, and reasonably defend why a certain risk tolerance was established may prove to be useful in this area.

Trial and Error

Sometimes organizations have a hard time setting a risk tolerance that can be used within the organization to guide staff and allocate resources, but also be sufficiently robust to meet the 'explain that to a bunch of angry stakeholders' test. This is true in spades in public sector organizations where political masters and critics are involved. Given that, in this context, that the language of risk is so foreign, adding that of risk tolerances is really challenging. It can be done, but takes a hard data approach. What one then has to do for the soft risk issues is exercise considerable judgement. This will take time and deliberation. It is also the point at which the role of senior management becomes crucial. It has been described by more than one leader in both government and business as the talking-out side of risk tolerances. Seldom in these areas is the issue of setting a numerical risk tolerance with nicely balanced alternatives. Rather, it is one of identifying what conditions would lead the organization to re-open its controls, engage more actively or even turn to emergency response type techniques. Therefore, senior management will need to discuss out its risk tolerances and ensure that direction is provided.

The trial and error methods apply equally and just as importantly to risk appetite. In fact, they are two sides of the same coin. Risk tolerances and so much of IRM is seen as purely defensive and it is. However, risks also represent opportunities for organizations. How risk appetite is sustained in the face of many threats is a concern.

A final point on the trial and error element of setting risk tolerances. Senior management will set its risk tolerances whether it does so in a conscious manner or not. They will be set behaviourally. In a well run organizations, there is an alignment between the stated intentions about risk and actual actions that are taken. .

Risk Evaluation Formats

Risk evaluation is the point in the process when data meets feelings. Organizations need not simply to identify risks in a systematic way, but then to start to build information about them. In doing so, the following questions need to be addresses:

- What are risks?
- Who or what might be harmed and how?
- What are we doing already to address this kind of risk?

- What else has to be done?
- How should this be put in place and by whom?

Forms take many shapes and sizes. However, here is a fairly generic approach to take either in group activities or on an individual basis. Note that the key thing here is to gather information and relevance in order to make decisions.

Risk Evaluation				
Identified Risk	Existing Control Measures	Likelihood of Risk Occurring	Consequences	Degree of Severity for the Organization
Risk 1				
Risk 2				
Risk 3				
Risk 4				

What to Note about this Form

The initial step of risk identification now has to move to great precision. As noted above, most organizations act on perceived risks already. Sometimes they do simply as a matter of prudence or past practice. However, there will be some element of control in place, even if it is a basic as having locks on the doors! That is why the second column as part of the process is so important. Chicken Little had a good day running around, but in the end organizations cannot afford to have risks out there that either engender panic or create immense legal or political liabilities. Therefore, the risks have to be refined and brought down to a sizable few of real significance.

There is one very important qualifier to that statement, however. Controls may not prove adequate for a number of reasons and these need to be considered, especially in

an IRM process. Controls can provide considerable and generally justifiable comfort to organizations. They also shield the organization from an accusation that they have not done enough to combat clearly evident risks. However, controls may be inadequate for a number of reasons:

- Controls may have been put in place a long time ago and fail to respond to current risks, e.g. level of financial liability in the event of injury,
- Controls may be taken for granted and not appropriately tested, e.g. alarm systems and firewalls,
- Controls may not actually be in use, e.g. the frequent over-ride of pre-set cheque limits for local authorization may speed up individual transactions, but also destroy the control,
- The risk may have evolved into a different life form: talk to your IT people about that one.
- The control is *pro forma* but not really part of an active control system, e.g. there may be an emergency plant on the shelf, but when was the last time it was tested or even table topped?

The last three columns move us very close to Risk Mapping which we will discuss shortly. However, in the evaluative phase, you are not looking for simple numbers of categories. In fact, you will do that with the risk mapping. What you are looking for is evidence, information or signals. Certainly, where measurements are possible, e.g. stress levels on structural concrete on highway overpasses and their behaviour over time, this is very useful. The objective of the evaluative phase is to ensure that the organization develops a robust understanding of the risks it faces, works from as much information as it can and also ensures that its existing controls can play a positive role in the mitigation process.

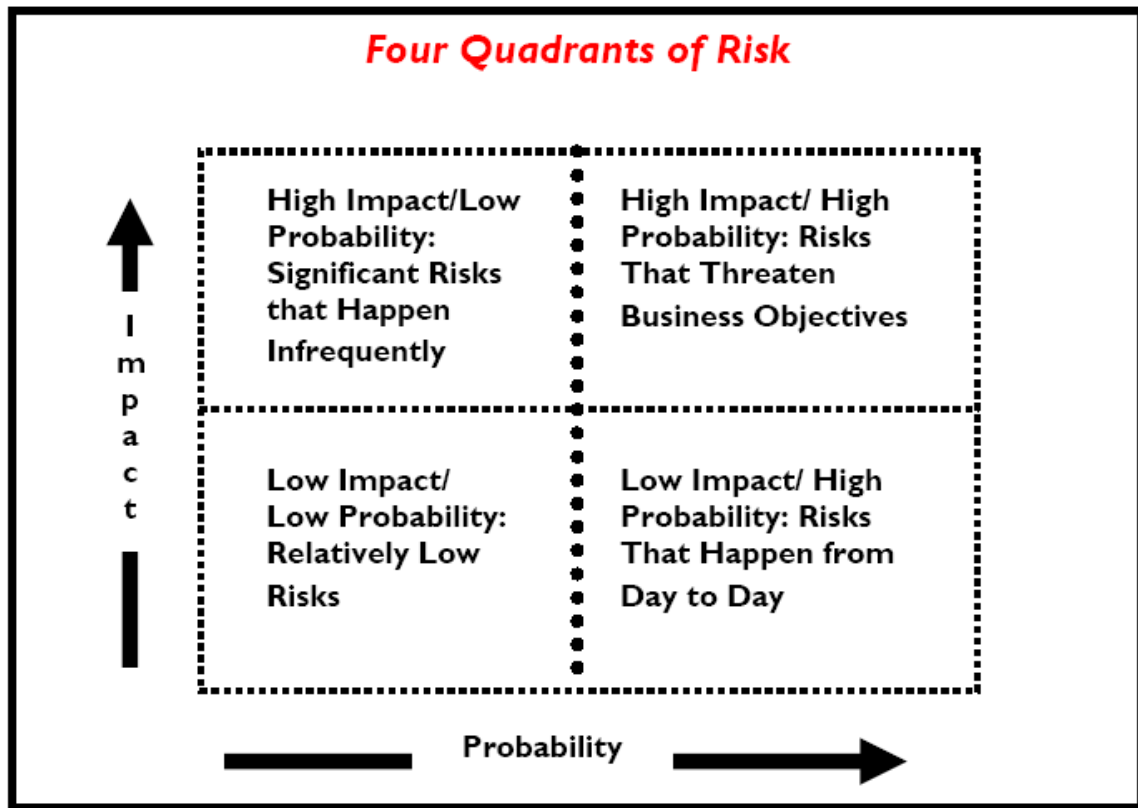
Analysis and Evaluation

It is at this point that some analysis of all this input has to take place. It also has to be challenged and sorted relative to corporate priorities and business plans.

Setting Priorities: Risk Mapping and Decision-Making

This section will deal with how you arrive at a set of risks with priorities in order to develop mitigation strategies for those that demand your attention and ensure that you have adequate controls and monitoring of lower level less likely risks. To this stage, you have identified and evaluated the risks. In all probability you have a wealth of information, so much that you could not possibly present this to senior management for decision-making or use it all in reporting to your board or governing authority. Some sorting has to take place. In doing so, it is important to keep in mind that risks are defined by two axes: probability and impact. Normally, risk maps are constructed using these two axes. They are important part of the process for they begin to set in place a collective understanding of the risk landscape as a whole. At its simplest, this mapping process will produce four quadrants, each of which has unique characteristics.

Here is a simple quadrant map that is simple and very clear:



More will be said about overall mitigation strategies in the next Section. However, once you start to populate this grid, it becomes a very fertile tool for setting priorities and for focusing on those issues that demand attention. The process for this arises from all the work that has flowed from the risk identification and evaluation process. The degree of specificity will depend on the work that the organization does. As the objectives of the organization may involve a high degree of complexity, you may wish to have a risk grid that is itself more complex. Perhaps the most common format that one sees is a variation on one of the following.

Risk Assessment Matrix I

		HAZARD PROBABILITY				
		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
SEVERITY	Catastrophic I	Extremely High			M	
	Critical II	High		M		
	Marginal III	H	Medium		Low	
	Negligible IV	M	Low			

Using a matrix such as this may create problems with language. Many will react to terms such as hazard and catastrophic. The term hazard is often used as the equivalent of risk, especially where there are many environmental or safety elements to the work. It does, however, restrict the scope of risk analysis to those areas. Of course, catastrophic is a term that indicates extreme risk if not more. Its use would require some very firm notions of what is meant by that

The advantages of a risk matrix like, even if one were to modify the language, is that it does not look like standards matrices, such as we see in **Risk Assessment Matrix 2**. By this is meant that the standards colour scheme is avoided and the place of Extremely High is almost counterintuitive. In some respects, this softens the visual impact without taking away from the analytical quality. This is a judgement call.

Take a look at the more standard display of risks in the following matrix:

Risk Assessment Matrix 2

Winnipeg

Risk Response Matrix (sample)

Likelihood	Impact				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Extreme 5
Almost certain 5	M	M	H	C	C
Likely 4	M	M	H	C	C
Possible 3	L	M	M	H	H
Unlikely 2	L	L	M	H	H
Rare 1	L	L	M	M	M

Legend

C Critical risk	CAO involvement essential, inform committee of Council
H High risk	Senior management involvement essential, inform CAO
M Moderate risk	Management mitigation and monitoring required, inform senior management
L Low risk	Manage by routine procedures

In this example from the City of Winnipeg, we have a more commonly found, but nonetheless effective, colour display. Note the legend that defines the risk levels and indicates what sort of managerial attention is needed for each level. Note also that the number of gradations or squares has increased from the previous example. Once again, all this will depend on the organization and how it anticipates using these grids. There is little question that this chart is more of an attention getter than the previous one. From the point of view of the decision-maker, she will know where to go first – the red. From the point of view of overall risk management, however, this may serve to minimize the low risk areas and also the high risk/low probability areas which we will discuss in **Section 6, Managing the Risks.**

Finalizing the risk priorities for the organization is the work of senior management, using its existing governance tools such as executive meetings and business plans. The use of charts such as the two examples above demonstrates that relatively few organizations face only one risk. Further, while priorities can be set, in risk, they will not be in a linear progression, but always a relative array. This is what makes the charts so useful. In addition, graphics of this kind serve as a very effective communications tool in and of themselves. However, they are high level and in summary form. For many organizations,

you can stop the IRM process work and get on with mitigation activities, often as part of your normal planning and operational cycles. However, for larger organizations and those with multiple stakeholders where communications and preparation of senior managers or political leaders is a necessity, some additional reports might be useful.

Risk Registers and Summary Reports

A Risk Register is a document or database that lays out the results of the risk identification, evaluation and prioritization process. It then adds additional information related to actions being taken and persons or groups responsible for that action. You can only really produce a Risk Register as an evergreen document after you have put in place the various mitigation processes.

The Risk Register serves several purposes:

- It creates a database that can be accessed by those who need to know how the organization is managing its risks on an ongoing basis.
- It provides a project control type of updating tool so that internal groups responsible for risk management can monitor progress on risk mitigation as it is spread across the organization.
- It provides senior management with a periodic update on risk mitigation, flagging areas of progress and those needing further attention or accountability.

In some instances, Risk Registers are publicly available documents and used as a means of holding public organizations to account. They also serve to signal the population in general how the organization views its risk profile and what it is doing about it. Such a phenomenon is almost exclusively in the public sector. However, risk registers are used extensively in the private sector for the last two reasons stated above. Ideally, these are reviewed and reported on an exception basis to senior management and discussed at meetings where performance is reviewed. Risk Registers require maintenance and updating. They must be updated when there is a change or status or the action outlined is complete. They also need to be updated as the organization's risk profile changes over time. Rules need to be set in place to ensure that the document is sustained. Otherwise, the information contained in it will create further risks to the organization as a Risk Register clearly addresses those core questions of accountability: What did you? When did you know it? What did you about it?

The following is an example of a Risk Register, based on that of a United Kingdom Police Service. These Registers are required by law in that country for all police services. It has been modified to avoid specific references..

Sample Risk Register

Risk #	Risk Name	Risk Area	Mitigation Strategy	Related Challenges and Comments Key Controls	Responsibility/ Risk Owner	Risk Severity	Review
001	Lack of resources	Organizational	Ensure existing resources are allocated efficiently and fiscally responsibly; Build business case for more staffing and infrastructure support	Community Policy Survey was only conducted with adults and was not community based; CPSB: Need to do more preventative work; CAO concerned about cross-jurisdictional policing costs; No resources to address computer crimes; Sr. Staff unsure of how to handle the potential for terrorist activity	CAO	High	Weekly at Senior Management Committee
002	Not deploying resources effectively	Organizational	Review of financial and operational controls		CAO/CFO Division Heads	Medium	Monthly Review at SMC
003	Current infrastructure for response becoming inadequate	Strategic	Hire a consultant to do some medium and long term planning for the service	Require an updated Capital Plan.	CAO	High	Three months
004	Inadequate strategies for retention and recruitment	Strategic	Develop a recruitment and retention strategy Develop a orientation process for new but experienced officers Implement a communication process with senior staff	Recruitment should focus on minorities	Chief, HR	High	Two Months with bi-weekly reporting to SMC

Date Prepared: xxxxxxxxxxxxxxxx
Nest Update: xxxxxxxxxxxxxxxx
Risk Profile Updated: xxxxxxxxx
Prepared by:
Contact

What to Note about this Form

While does no very generally, this Register does assign responsibility and attempt to set out some dates for action back to senior management. That is vital. The degree of detail (names, etc) will depend entirely on how public this document is. Note the numbering system – a simply way of connecting the control function with the data base. The use of the column entitled Risk Area is optional. It appears to exist here in order to distinguish between matter that can be fixed within the current framework and ones that require a shift.

Risk Registers are very useful for managing project risks. However, they should not be relegated to that role only. They also serve an important strategic purposes. In complex organizations, however, sub-registries may be necessary with the organizational-level Registry only dealing with those items that are of concern to senior management.

There are many ways of organizing a register. However, there is also amply software for sale that will do this for you.

Risk Reports

Forms abound for providing senior managers, governing bodies, stakeholders and the public with information on organizational risks. However, before you consider creating such forms, make sure that whatever you use will state the 'getting out in the public in an unanticipated way' or 'getting into the hands of our competition or their lawyers'. Life is full of surprises and it is always a revelation, not always a comfortable one, to many managers when information somehow walks out the door. Seasoned managers will expect this and try to resist wasting their time on a witch hunt for the transgressor. Therefore, anticipate an unanticipated public look at the information and be prepared. Therefore the report should have the following elements:

- A description of the risk
- The relative priority and severity measurement
- Existing control and mitigation process
- What you are going to do to further address the risk
- What is the important public message concerning this risk.

Risk Report and Update	
Note: This report is updated on an as needed basis using information from the Risk Management System.	Risk Category and Priorization
Corporate Lead: Information Contact Point:	Risk Description
Actions in Place to Manage the Risk	Actions Underway to Reduce Risk
Key Information Points	Next Update

What to Note from This Form

Many organizations add some version of a colour code to these forms. This certainly helps sort the risks and bring to most urgent to the attention of the decision-maker or intended audience. Once again, this can also create a sense of urgency but also of panic

if not handled well. It will depend on the operating environment and the possibility that such coding will be misunderstood.

A Closing Comment About Forms

An effort has been made here to offer some possible forms and discuss their use without prescribing the exact format that will work in all circumstances. You may well choose to buy an IRM software package that generates what you want. You may adapt forms and processes from similar organizations. The key is all of this is to make the forms as seamless as possible, minimizing the creation of yet more paper processes. It is inevitable that there will be an increase in information gathering, reporting and management time if you undertake IRM. You cannot promise that this will be work free. The benefits, by now, are clear. However, at all costs, avoid systems that over-burden an organization that probably already has plenty to do.

Checklist

Some Questions to Ask about IRM if you are a Member of a Governing Body, e.g. a Board of Directors

- **Does management involve the Board in a timely and effective way in discussing risk when strategy is being set?**
- **Does the Board understand what are the strategic risks facing the organization and what is being done about them?**
- **Does your Board devote sufficient time to discussing risk? Does it devote too much time?**
- **As a board member, are you satisfied with the Board's level of discussion regarding risk appetite of the CEO and the organization as a whole?**
- **Are you confident that the organization is not taking significant risks without the Board's knowledge?**
- **Do you cause to be concerned that the organization is taking significant risks even though it is achieving positive results? Are the issues of sustainability being adequately addressed?**
- **Does the Board receive good quality information about strategic risks in a timely and useful manner?**

Section 6 – Managing the Risk: An Overview of Strategies

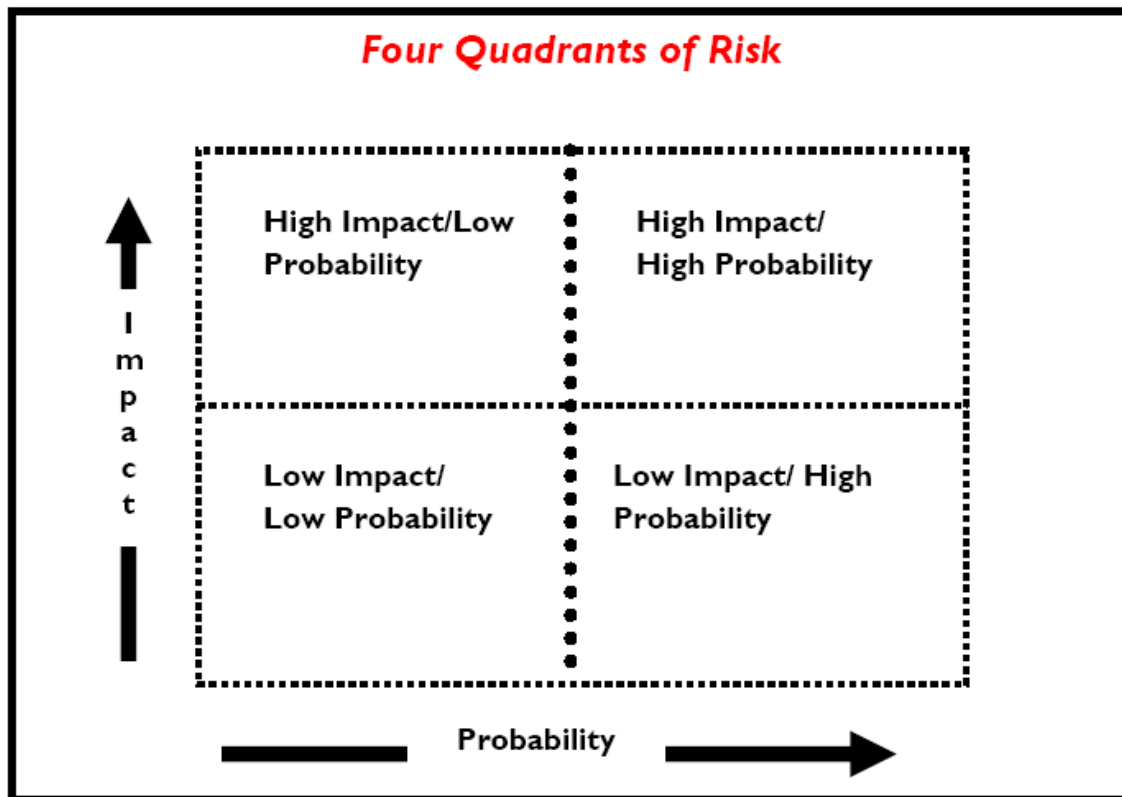
What This Section Does

Managing the risks that you identify and prioritize is part of the daily work of running organizations. In this Manual, there is no way to cover all possible risks and the tools needed to manage them. As well, all management takes place in a context – the context of the organization itself and its environment. What this section is intended to do is simply review the main avenues at your disposal to deal with risks that you identify. To that end, it will address:

- General approaches to the main risk categories in the probability/likelihood scales
- Review the principle alternatives for addressing risks
- Discuss the nature of residual controls, monitoring, insurance and operational oversight that serve to mitigate risk.

General Approaches

Let's take a look again at the four quadrants of the Risk Map:



Once your organization has completed a risk ranking, it is probable that each of these quadrants will be populated with identified risks. Ideally, a Risk Report will be created to monitor and control the risk and assign responsibilities. However, not all risks are equal and certainly there is no one single response required. Depending on how detailed you wish to get and if you actually do use weighed measures of risk, you will find that your risk exposure will vary. Here are some general considerations in terms of management approaches to each quadrant.

Low Impact/Low Probability

Generally, this is the area of the Risk Map that should receive the least attention. On the other hand, even least threatening risks are risks nonetheless. Therefore, if they populate the Map, they require some form of response. In general, residual controls, policies and standards are in place just for risks of this kind. Another feature of low impact/ low probability is who you would expect to pay attention to them. Go back to the Winnipeg Risk Map. You will note in the legend how lower level managers are assigned responsibility for lower risks. In this way, they are not forgotten, but then they do not take up more valuable senior management time.

Idea Source: All risk mitigation involves some form of cost/benefit analysis since there are very few mitigation strategies that are free

Many will argue that these are best left off risk reports to senior management. There is an issue that you do not want to crowd the agenda and you want to focus senior management on high risk/high probability risks. This is true. You also do not want senior management wasting time on risks that might be of interest, but essentially waste their time or, even worse, focus their attention on the wrong things.

High Impact/High Probability

Of course, this is the red zone. This is the zone that demands the most active attention and for which there are often not residual controls sufficient to meet the needs of these risks. These will be the risks that receive continuous or, at least, regularized review at the senior management meeting of the organization. Further, an individual at a senior level needs to be assignment responsibility for pulling together a response and overseeing its execution. Many high level risks do not fit comfortably into organizational divisions or silos. Therefore, the executive assigned responsibility has to be able work across those silos to arrive at a strategy for the risk area.

Some writers on risk classify this section as easy to manage. That is because it grabs management attention and there is a sense of urgency associated with the organization's highest risks. This is probably true. That does not mean it is not a lot of work as well. The key to managing this sector is active management, assignment of responsibilities in a clear way, follow-up and periodic attention of senior management in a structured way.

High Impact/Low Probability

While it is dangerous to categorize the risks in this area, they are often called the once-in-a-lifetime disasters that you have to prepare for, but seldom expect to happen. These have also been described that the big risks that are waiting in the wings and that can have a catastrophic impact on the organization. These risks represent a real challenge to an organization. The first challenge is sorting which of these to actually accept as something that requires active management. The second is to determine how many organizational resources to devote to doing so.

In the first instance, the possibility of the earth being hit by an asteroid fits well in this category. So too in a larger sense does something like global warming. Maybe. It would be dangerous for an organization that might be affected by the asteroid, but has no capacity to do anything about it, let alone even track those rocks out there to actively engage any energy in this area. However, serious infrastructure breakdowns or the possibility of a violent crime within the organization's scope of attention do require some thought and probably contingency planning. It is perhaps best to set these risks into the zone of what level of contingent response has to be set in place and maintained for that rare but devastating event. Turn this around and look at it from a liability point of view: if something like this happens, what will be our accountability in terms of being ready to respond in an appropriate manner?

Organizations are always challenged to be sufficiently ready for catastrophic events. Those with strong operational outputs will want to ensure that business continuity plans, accompanied by table-top exercise or, in the event of high level concerns, mock exercises.

Low Impact/High Probability

This quadrant will contain risks that are generally manageable through techniques such as insurance, training, regular monitoring or transfer, all of which we will discuss below. If you identify risks in this category, there is also an element that you have accepted them as being in your universe, worthy of recognition and monitoring, but would seek passive ways to deal with them, if at all.

Risk Mitigation Strategies

Organizations have an array of tools for reducing or managing their risks. Some are risk specific and some are inherent in the way well managed organizations are expected to function. In other words, good management is the first risk mitigation strategy. Even with this array, not all risks can be eliminated in an affordable way. Organizations have to carefully weight just how much time and effort they are prepared to put into risk mitigation. Think back to the discussions of risk tolerance and risk appetite. Much of that will be driven by the cost of mitigation or the danger of

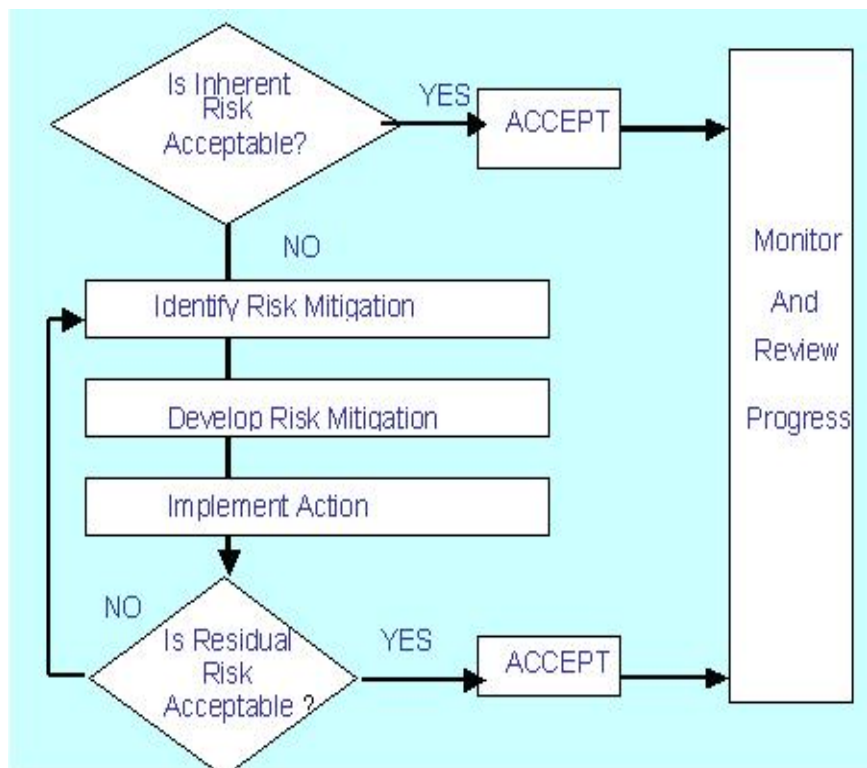
Idea Source: "When a risk is assessed as "judgmental boundary", management has to decide whether it is cost-effective to take further actions to mitigate this risk. This decision will also be based on the level of risk that management is willing to accept." – Treasury Board of Canada

losing perspective on corporate objectives by seeking a zero-risk environment.

For each risk, you should first document the applicable list of mitigation activities. When thinking about what risk mitigation activity is in place (or should be in place) it is useful to think of the following three things:

- **Prevention** - What is in place that will attempt to stop the risk happening in the first place? (eg: security, awareness & training programs, qualified staff, planning, and/or procedures);
- **Detection** - What is in place that will let me know if and when the risk does happen? (staff / customer reporting mechanisms, financial reconciliation, fire alarms, audits); and
- **Response** - If the risk happens anyway, what measures do we have in place to lessen the impact? (eg: contingency plans, back ups, insurance, resolution processes).

Risk Mitigation Process



The principal means of risk mitigation are:

- Accept or Tolerate
- Prevention,
- Reduction,

- Control
- Transfer
- Prepare

These are very general categories, each with a multitude of potential actions. It would be impossible to document them all, but we will look at each one in turn.

Tolerating Risk or Self-Insurance

Tolerating a risk may mean recognition that no amount of internal resources will cause it to go away or be effectively managed. It may mean that no insurance is available at a reasonable rate. It may also be a calculation that, even if the impact might be severe (High Risk/Low Probability), the potential for the risk to actually manifest itself is very low. Tolerating risk then becomes a form of self-insurance in which your own organization takes back all the risk. In some cases, prevention or transfer is therefore neither practical nor affordable.

Idea Source: The minute that you made a decision not to protect against all possible risk, you accept the possibility that mistakes will happen and that you have residual capacity to respond.

Regardless of the decision to accept a risk and take no specific remedial action, it is necessary to continue to monitor the risk, as your risk management process has identified it and you have kept it on your chart, scoreboard or reporting system. There is ample experience across companies and governments that High Impact/Low Probability risks can change

quickly, demanding a new response.

Prevention

Here the organization has to decide what not to do in the face of the risks. Prevention has several aspects:

- Ceasing the activity or operation in the face of unacceptable risks,
- Changing procedures, rules or regulations to reduce the likelihood of the risk occurring,
- Boosting internal controls to a high level,
- Use of information and training for both staff and the public about the risk and how to respond
- Banning risky activities, either internally (smoking in the office), or to the client (no single person visits).
- Installing safety equipment.

Reduction

Risk reduction is a general category for a range of activities that will reduce the potential of occurrence or impact of the risk if it does. This could involve such steps as:

- Increasing investment in risky infrastructure,

- Replacing dangerous equipment,
- Finding new suppliers or delivery tools that reduce risk,
- Fixing that which is not working effectively,
- Setting in place review and research processes to study the risks and come back with recommendations,
- Establishing special task groups to come back with recommendations.
- Changes in management systems
- Changes in human resource strategies
- Continuous review of pre and post control gates against errors and adjustment.

Control

Some examples of how controls play a role in risk mitigation have already been offered. The organization should review its financial and operational controls as it sets out its risk plans. Too often, these controls are assumed to be functioning in an invisible and quiet way, when the flow of events that are there to control may have changed dramatically. Similarly, new risks may have arisen that demand new measures. Some of the key control areas are:

- Financial
- Operational
- Budget performance
- Performance measure in relation to plan
- Safety issues
- Security controls: physical, personnel and the public

Transfer

One can rarely fully transfer a risk to someone else or some other organization. However, it is possible to transfer some of it or the financial uncertainties associated with it. This means causing another party to accept the risk, typically by [contract](#). [Insurance](#) is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an [insurance premium](#). However, you have to remember that what this does is not actually transfer the risk, but rather smooth out the potential impacts.

In situations where you are using suppliers, contractors or have outsourced an element of the work, you will want to ensure that some elements of risk transfer or risk sharing are built into the contractual relationship. Therefore, you will want to ensure that issues of personal safety, security of data, public accidents or damage and similar risks inherent in the operation of a contract are anticipated and negotiated as part of the risk transfer process. The greatest risk in this instance is that the contracting process failed to address the issue in the first place. In that instance, risk flows back to its original owner. It pays to be clear.

Risk transfer, to the extent that it can be achieved, can be an effective tool of spreading out risk. However, it will seldom do much for an organization when issues of trust or

reputation are involved. In that sense, this mitigation tactic, while valuable, does not absolve the risk owner of a need for watchfulness.

Prepare

Risks in the categories of High Impact/Low Probability demand some form of preparatory response. This could involve the preparation of detailed emergency response plans. These should be accompanied by training and readying the organization in the event of such an occurrence.

In addition, organizations need to have in place business continuity plans in the even of major shut-downs over which they may have limited control. Unlike emergency response planning, business continuity is about restarting the organization, ensuring that vital data and process capacity has adequate back-up to enable this. It is very clear that organizations that lack any plans for generally unlikely but nonetheless serious events, respond poorly to them and recover more slowly. They also face major damage to their reputations and credibility with the public, their clients and customers. Experience has also shown that organizations that fail to prepare for these events face liabilities associated with their governance responsibilities.

Is There a Difference between Risk Management and Crisis Management?

You bet there is. If all risks escalate into crisis, requiring the full resources of the organization to fix, then you are doing effective risk management. That being said, crisis preparedness is an important part of effective risk mitigation. Remember that High Impact/Low Probability quadrant – that is where effective crisis preparedness is so important.

Risk Management	Crisis Management
Systemic and ongoing	Episodic
Examines range of risks	Addresses a specific threat of a very serious nature
Environmentally responsive	Event responsive
Focus on mitigation	Focus on resolution and recovery
Risks cover a range of threat and opportunity levels	Crises are organizationally threatening in a serious way
Responses vary	Responses deploy and concentrate organization resources in short term resolution
Works effectively within normal decision-making structure.	Creates an extraordinary structure to enable mobilization of resources and response.
Time perspective varies.	Time perspective is short term.
Focused on normal business activities.	Focused on abnormal business (and potentially other) activities.

Risk Management and Good Governance

Organizations that embark on systematic IRM will soon discover just how many risk mitigation strategies they already have in place. In some cases, they have no choice. For instance, occupational health and safety regulations demand that certain precautions be taken as a normal part of doing business. Similarly, financial controls, to varying degrees and with many different aspects, are always part of the financial system. Taking stock of these mitigation tools, making sure they are robust and effective and monitoring them becomes part of the IRM process. This should not be cause for indifference to risks that are not being managed or those that will only occur in a rare and catastrophic manner. Therefore, a variety of tools are available. In the end, active management of the vital view is the goal for a resilient organization. That means that residual controls are working, adequate contingency and business resumption plans are in place for catastrophic emergencies and that senior management is focused on high level risks that will affect the organizations' capacity to meet its objectives.

All of this is, of course, good governance. It is important that IRM be fully part of the strategic and tactical governance of the organization. Otherwise, it is not integrated, seen as a separate piece of work and will reek of flavour of the month. To this end, and recognizing that this repeats some already stated but important themes, the following are some of the principal elements of having effective risk management strategies integrated into your management structure:

- Having an explicit risk management policy,
- Having the necessary level of central co-ordination of the risk management process and plan,
- Having clearly assigned responsibilities,
- Having a defined formal process,
- Having a good linkage between risks and goals,
- Having a full application of risk analysis, not just pockets of enthusiasm,
- Having risk mitigation plans clearly articulated,
- Having adequate contingency (crisis and business resumption) plans in place.

Effective response strategies for risk are as much about process as they are specific responses. By that is meant that keeping the organization's eyes and focus on its principal risks takes some discipline and consistency. That is what governance is all about, not just forms, meetings and colourful charts. In this instance, effective governance is a form of overall risk mitigation itself. In general, this means:

- Integrating risk management into normal business processes at all critical levels of the organization,
- Explicitly incorporating indicators of risk on a regular basis into decision-making,
- Ensuring the organization's senior management and governing bodies have:
 - The right information in a format they can readily work with,
 - Make judgements about the risks and the adequacy of the response at the right level,

- Have a direct involvement in setting these directions.
- Have the means to
 - Clearly set out the objectives to manage the organization's risks and desired outcomes, and
 - Allocate suitable and sufficient resource to risk management.

Checklist – Do You Integrate Risk Management and Governance?

- Does senior management directly lead and strategically manage the organization's risk management process?
- Is senior management involved in the identification, assessment and validation of the organization's risks?
- Does senior management effectively line up the organization's risk management framework and strategies to match the key risks of the organization, e.g. are key risk addressed in planning?
- Is risk management an explicit part of strategic and business planning considerations and is it applied to all critical levels of the organization?
- Are risks reported in a formal way and with sufficient information that senior management and governing bodies can fully grasp their significance and identify them for response?
- Does the organization have a formal means of overseeing risk management, e.g. a risk management committee, a CRO or an expanded audit committee?
- Has the organization allocated sufficient resources to make IRM work effectively?

Section 7 – Risk Communication and Reputation

What This Section Does

Risk communications, or more directly, the role that communications plays in IRM, is more than just a question of public relations. It involves the development of language and tools that ensure that, both internal to the organization and with stakeholders; there is an understanding of the use and application of risk language. This section will:

- Outline the communications requirements of an effective IRM,
- Examine the issue of reputation risk and how that plays in the development of risk mitigation strategies, and

Risk communications, as part of the IRM, is a two-way street. One often hears clichés such as the usefulness of open consultation and transparency. Effective inflow and outflow of risk information,

Idea Source: “A crisis is a terrible thing to waste. “ We need to learn from it.

however, is vital to the survival of organizations, not just a nice-to-have. It has to be two-way in order for organizations to effectively gather valid information about the risks they face that are outside their control. It also has to provide robust enough channels to permit those with contrary views to present information or impressions that senior managers may not want to hear, but have to hear. Similarly, the outward flow of risk communication must be based on a confident understanding about the organization, its objectives and its competencies. Recipients, be they internal or external, should not be surprised to get such information and should have confidence in those sending it.

Risk communication must carefully consider the following components:

- Creating effective channels for both receiving information about risk and for communicating the organization’s risk position and plans,
- Establishing credibility and trust issues with the source and as a source,
- Ensuring that messages and information do not get lost in the complexity of the issues,
- Understanding and adapting to perception issues with the receiver ,and
- Overcoming channel problems such as timeliness or media distortion.

There is the real danger of creating panic and lack of confidence through the inappropriate application of risks and the organization’s failure to effectively communicate their integrated approach. A common theme of this Section will be that risk communication must be fulsome and complete, never leaving the receiver any doubt that the organization has used a sound system of risk management, had identified risks appropriately, understands risk and is taking sufficient actions. In the end, effective risk management communication should and does increase confidence in the organization’s capacity, thereby building further trust and enhancing its reputation. This means that it is

important to communicate how risks are identified and managed on a continuing basis as it is to communicate about actions and plans associated with individual risks.

The Risk Communications Conundrum

The idea of risk and uncertainty can take on very personal and emotional dimensions very quickly. Even where a strong scientific presence helps define risks, there is a tendency to associate risk with danger. In many organizations, risk is anathema as a concept that might be explicitly managed. However, only a fool would say that an organization faces no risks. The challenge is to find the process and language that exposes risks and identifies their mitigation as positive proof of sound management. However, this does create a reluctance to be overly explicit about risks.

Similarly, there are challenging issues associated with risk perceptions. For instance, the

***Idea Source: "Risk analyses and risk analysts serve the public to the extent that they create the facts that it needs for effective decisions making and, then deliver those facts in a comprehensible, credible form."
- Canadian Standards Association***

public, as we have seen, will assign high risk values to phenomenon that experts know fully well are not high risk. However, intervening political or market forces will ensure that the fear that many experience because of these risks will often outweigh expert opinion. As well, in risk communications, any official attempt to downgrade these fears will often backfire on the organization which will be painted as insensitive or, even worse, withholding the real information about the risks. Similarly it does not pay to simply put experts in front of the media as a means to assuage such fears about risks. Effective risk

communications centers on having a steady stream of risk information flowing, not an episodic one that comes out only in a crisis. Second, the role of the expert can be very helpful as long as that expert is well supported, understands how to act in front of the media and is prepared to accept that irrational fears legitimately will drive both market and policy decisions.

In contrast to this is the growth of demand for greater transparency. It is a fact that "risk transparency" is increasingly expected and even mandated for organizations in both the public and private sector. Stakeholders want, and will get, more disclosure. Telling the world about your risks will be awkward, even painful in many instances, but it is the future.

Some Risk Communications Myths and Realities

Myth	Reality
Risk Communication is more likely to alarm than calm people.	Not if done properly. Most people expect organizations to be assessing and working on their risks. They will react more strongly to a lack of information.
Risks are too complex to explain, let alone understand.	No, they aren't. Part of your job is to help staff, governing bodies and the public understand these issues no matter how complex they may be. The public may not make technical decisions, but they expect information and help in understanding risks.
Risk communication is the job of the communication people, not me.	Wrong, wrong, wrong. If senior managers do not visibly 'own' the risks of the organization, no amount of spin will help. Even where communications support is needed, and it often is, those folk need direction and messaging guidance from senior managers.

- Taken, in part, from Covello VT, McCallum DB and Pavlova MT (Eds.). **Effective Risk Communication**. New York: Plenum Press., 1989

Successful risk communication serves many purposes. It increases institutional and interpersonal trust and confidence. It has the potential to reduce the length, strength, and frequency of controversies. It may also reduce the frequency and magnitude of legal challenges. This in turn improves the programmatic success of a given venture. It also affords management more flexibility or breathing space to address risks over the long haul.

Building Credible Risk Communications

Credibility in risk communications begins with a preparedness to see it as a two-way street. Risk communication includes the appropriate sharing of information and acknowledgement of concerns. It incorporates and appreciates diverse opinions and perspectives in an atmosphere of relative openness. It accepts that the dialogue sometimes may be more about feelings than facts. If messages are consistent, if the process is identified and followed with integrity, the success of the planned project increases dramatically. It has to be remembered that risk communications has both

internal and external dimensions. Similarly, many organizations will identify risks that may either have security implications or have a direct bearing on their competitive position. Therefore, while the objective is to be as open as possible, it would be foolhardy to not recognize the constraints to such a value.

There are essential elements of communication that form a solid foundation of understanding. Once the foundation is laid, it is then possible to build upon it and customize it for various groups.

The first step in developing a risk communications approach is to decide who needs to be involved in a communications process. As we have seen in developing IRM from beginning to end, it is build upon the notion of drawing in both internal and external forces to provide the organization with a full picture of its risks. Therefore, the communications process has already begun at the intake level. This is key. IRM is not just about discovering risks: it is about managing them. Therefore, a regularized process with known steps and outcomes will go a long way to reducing the surprise element of risk identification. A normal process avoids shock and awe. It also, as we have seen, is a staged process where risks that may be identified in the scanning process are subject to analysis and assessment. This often has the effect of dampening both the shock value but also getting closer to the facts about the risks, thereby enabling a more reasoned assessment. Finally, as risk assessment, analysis and evaluation are rolled into business processes, it can be seen that the organization is incorporating the information in a business-like fashion, not panicking. This sounds dull. In the realm of risk communication, dull is good.

“Perceptions of risk can vary due to difference in assumptions and conceptions and the needs, issues and concerns of stakeholders as they relate to the risk or the issues under discussion. Stakeholders re likely to make judgements of the acceptability of a risk based on their perception of risk. Since stakeholders can have a significant impact on the decisions made, it is important that their perceptions of risk, as well as their perceptions of benefits, be identified and documented and the underlying reasons for them understood and addressed.”

Risk Management Standard, AS/NZ 4360-1999

Who are the key players in risk communications? This will vary from organization to organization. What you have to do in your planning process is to identify those groups and individuals that are part of the communications infrastructure of your IRM process. Start by mapping. Here are a few examples:

- Internal users who will need this information for their own work planning,
- Internal users who may be affected directly by the risk at a personal or organizational level,
- Senior managers as a whole,
- Governing bodies such as boards, commissions, oversight bodies,

- The public who consume the products of the organization and may be directly affected,
- The interested public who may have a larger interest.
- Media with either a specialized interest in the organization or a 'front page' interest in transitory stories,
- Banks, credit raters,
- Budgeting authorities.

The relationship of the organization to each of these groups varies considerably. The first thing to consider is whether they are involved in the risk gathering and assessment process. Are they regularly consulted when putting together an annual environmental scan that involves defining risks? If so, they will need to know both about the IRM process and about the business objective well enough to be able to provide meaningful input. Are they consulted when trying assess the level and intensity of risks? This is a bit more complex, but certainly will apply to internal stakeholders but also to key credit-setting agencies (In the public sector, read oversight bodies or central agencies monitoring performance – in the end, they establish your 'credit rating'). Are they recipients of information about your risk profile and how you are managing it? This would be at the output end. A principal and important sub-group here would be those who become part of the risk solution. In other words, are they resources who need to be kept regularly informed as your organization will need their help in coming to a solution. This will particularly be the case if they are informed experts or commentators on your organization and its line of business. They will need to be well briefed, comfortable with what you are saying and have the capacity to push back and clarify your language and intent.

Pitfalls in Communicating Risk

Here are just a few things to think about when putting together an approach to risk communications.

Pitfall	Do	Don't
Jargon	Define technical terms	Use language that anyone in the audience does not understand
Humor	Direct it at yourself	Use it in relation to environment, health and safety issues
Negative Allegations	Refute the allegation without repeating it	Repeat or refer to them
Negative Words/Phrases	Use positive or neutral terms	Refer to national problems (e.g., "This is not Love Canal")
Reliance on Words	Use visuals to emphasize key points	Rely entirely on words
Temper	Remain calm. Use a question or allegation as a springboard to say something positive	Let your feelings interfere with your ability to communicate clearly
Clarity	Ask whether you have made yourself clear	Assume you have been understood
Abstractions	Use examples, stories, and analogies to establish a common understanding	Talk about new or unfamiliar topics without grounding the audience
Nonverbal messages	Be sensitive to nonverbal messages you are communicating. Make them consistent with what you are saying	Allow your body language, your position in the room, or your dress be inconsistent with your message
Attacks	Attack the issue	Attack the person or organization (e.g., "You're being irrational")
Promises	Promise only what you can deliver	Make promises you can't keep or fail to follow up.
Guarantees	Emphasize achievements made and ongoing efforts	Say there are no guarantees
Speculation	Provide information on what is being done	Speculate about worst cases
Money	Refer to the importance you attach to EH&S issues; your moral obligation to public health outweighs financial considerations	Refer to the amount of money spent as a representation of your concern
Organizational identity	Use personal pronouns (I, we)	Take on the identity of a large organization
Blame	Take responsibility for your share of the problem	Try to shift blame or responsibility to others

Covello, V. "Risk Communication, Trust, and Credibility," *Health and Environmental Digest*. Vol. 6, No. 1.1992.

Risk Communication Failures

In the book *"Mad Cows and Mothers' Milk"* (1997), Power and Leiss reviewed recent examples of risk communication failures, including the case of communicating the risks of PCBs in breast milk, mad cow disease, and silicone breast implants, to arrive at a few lessons for risk management communicators. The advantage in looking at what they learned is that it applies to all types of organizations – private and public.

Some of the lessons are:

- A risk information vacuum is a primary factor in the amplification of risk. Silence or failure to communicate creates anxiety and the vacuum will be filled. This applies both internally and externally.
- “Educating the public” about scientific or technical elements of risk is no substitute for good risk communication practice. This means that the communicator has to have both technical and communications skills.
- There is always more to a risk issue than what science says: public perceptions, values and opinion are crucial. This is driven by the fact that most people will personalize a risk, especially one of broad application, into a known point of reference.
- Organizations should begin discussing the possible responses to emerging risk controversies as soon as they arise, and continue to do so throughout their life history. Never wait for the perfect communications package.
- Risk communication failures can be costly: often, they will force organizations into taking a series of actions that are not really required ‘in fact’ but are done to re-establish lost credibility.
- Risk communication is a continuous process: timeliness is everything in effective risk communication
- Banish “no risk” messages: ironically, although citizens and environmentalists are often taken to task by government and industry officials for advocating zero-risk scenarios, pronouncements of the “there is no risk” variety are a favourite of government ministers and sometimes of industry as well.
- Risk messages should address directly the concerns of the audience: if government regulators and industry have the primary responsibility for effective risk communication, these officials cannot avoid confronting the issues as they are posed in society.
- Communicating well has benefits for good risk management: good risk communication practice can be regarded as the causeway that links all the organisational elements in a well-functioning risk management process, especially in the face of scientific uncertainty.

Checklist: Have We Built Communications Effectively into our IRM?

- Have we identified those who will be formally consulted in doing risk assessments?
- Have we defined the nature and scope of that consultation?
- Do those being consulted understand the nature of the IRM process within our organization, why they are being consulted and what will be done with their views and information?
- Do we undertake the consultations in a business-like, consistent way so that it is seen as part of our business process and not just passing the time of day?
- How else do we scan the environment in order to bring in information and communications about what will affect our business objectives? In other words, do we use non-personal sources of information, e.g. websites, blogs, media reports, audit reports, etc?
- Does senior management have the results of such efforts presented to them so that they can clearly identify this input?
- Is feedback given to those consulted?
- In determining risk strategies, are communications elements taken into account?
- Do we establish a form of **Risk Register** for use by those within the organization or externally as a reference point?
- Are communications targets and themes built into the risk management plan for each risk?
- Do you have a list of approved targeted audiences for risk information arising from the IRM process?
- Do you have designated spokespersons for your top tier of risks?
- Do you have a spokesperson who can actually explain IRM?
- Do you have a list of key media persons or outlets that need to be briefed on risks in your organization?
- Do you explicitly address risk issues in such documents as annual reports and performance reports?
- Is risk reporting a regular item on your governing body's deliberations?

Determinants of Reputational Risk

Three things determine the extent to which an organization is exposed to reputational risk. These are:

- Is the organization's reputation an inflated and unreal representation of its real capacity?
- Are there changes in external expectations and beliefs about the organizations and its products?
- Are there changes within the organization that will change its reputation?

What is Reputation Risk?:

Reputation Risk is the risk that an activity, action or stance performed or taken by an organization or its officials will impair its image in the community and/or the long-term trust placed in the organisation by its stakeholders, resulting in the loss of business, credibility and/or legal action. It would also result in the loss of long term credit with investors or credibility with stakeholders in terms of future actions.

Reputation-Reality Gap.

Effectively managing reputational risk begins with recognizing that reputation is a matter of perception. A organization's overall reputation is a function of its reputation among its various stakeholders, overseers, clients ,media and the public. A strong positive reputation among stakeholders across multiple categories will result in a strong positive reputation overall. However, it can also be expected that an organization's reputation may well vary across this range. This is always a challenge as most organizations prefer to listen to positive news than negative. Further, weighing the relative significance of having a solid reputation, for example, with overseers and creditors but not necessarily with the media is a judgement call and a situation that can not always be fully balanced.

One of the challenges for organizations is to recognize that they do not own their reputations. It is distinct from the actual character or behavior of the organization, as sound as that may be. When the reputation of an organization is more positive than its underlying reality, this gap poses a substantial risk. Eventually, the failure of a organization to live up to its billing will be revealed, and its reputation will decline until it more closely matches the reality. Worse still, there will be a sharper decline in overall reputation, with accompanying risks, as a result of this discontinuity. Life is not fair, especially in this area.

The first challenge in effective reputation risk management is to determine if your organization's expectations for performance are lined up with what you can actually achieve. Of course, this will involve some variant on promising less or, more accurately, promising what you reasonably believe you can deliver.

Of course, organizations that actually meet the expectations of their various stakeholders may not get full credit for doing so. This often occurs when an organization's reputation has been significantly damaged by attacks from special interest groups or inaccurate reporting by the media. It also can happen when an organization has made genuine strides in addressing a problem that has hurt its reputation but can't convince stakeholders that its progress is real. Once in this situation, you are past risk management and into rebuilding organizational credibility.

From an IRM perspective, what is of first importance is that organizational reputation be seen as a valuable resource to be managed and to be taken into account in building an IRM. The second is that reputations are not cast in stone but can be severely damaged in a number of ways. The impact of that damage is not just a communications concern, but a business concern.

Managing Reputational Risk

Effectively managing reputational risk involves five steps:

- Assessment
- Matching reputation to reality
- Actively working to close reputation-reality gaps
- Monitoring reputation
- Keeping a senior eye on things.

Assessment

Since reputation is perception, it is perception that must be measured. Three questions need to be addressed:

- What is the organization's reputation in key areas such as reliability, sound management, credibility, capacity to follow up, truthfulness, confidence in its leaders.
- What are the causes and sources for these views?
- Are there any sources of comparison that are useful?

Various techniques exist for evaluating a organization's reputation. They include media analysis, surveys of stakeholders (customers, employees, investors, NGOs) and industry executives, focus groups, and public opinion polls. Although all are useful, a detailed and structured analysis of what the media are saying is especially important because the media shape the perceptions and expectations of all stakeholders.

The old tool of clipping services that are now fully integrated into internet services needs to be supplemented with strategic media intelligence whether done internally or outsourced.

Regardless of how information is gathered, it is a challenge for an organization to assess its reputation and the risks that it faces. This is hardly an area that is readily quantified. It is also often personalized in the person of the organization head, be it the President, Director or Chief. In making such assessment, the organization can confuse its sense of its character and mission with its reputation. Often the news is discordant and hard to accept.

It is often wise in the IRM context to identify the risks to reputation with trying too hard to fully develop all the defining elements of the reputation itself. While this may sound somewhat contradictory, the objective of effective risk management is to put in play strategies to address key risks to the organization achieving its objectives. Just as with reputation, those objectives are not subject to intense review within the IRM process. They are part of the given. Of course, the IRM process may, over time, cause shifts in objectives just as it may in terms of the aspirational reputation of an organization. Therefore, the assessment should yield an identification of risks that would affect the reputation of the organization as it can best define it. To aid this process, here are some questions to ask:

- Will the credibility of the organization be affected by this risk?
- Will doubts be raised about our ability to manage this risk?
- Will questions be raised about senior personnel and their competencies?
- Will we be less believable?
- Will our credit ratings suffer?
- Will our long term capacity to manage suffer?
- Will we damage our capacity to secure further support or funding for future projects?
- Will we lose the control we need?
- Will we be subject to intense media scrutiny that will damage our good name?

Evaluate reality.

The organization must objectively evaluate its ability to meet the performance expectations of stakeholders. Gauging the organization's true character is difficult for three reasons: First, managers have a natural tendency to overestimate their organizations' and their own capabilities. Second, executives tend to believe that their organization has a good reputation if there is no indication that it is bad. This might be called the overly generous interpretation of silence. Finally, expectations get managed: Sometimes they are set low in order to ensure that performance objectives will be achieved, and other times they are set optimistically high in an attempt to impress

superiors or the market.

As is the case in assessing reputation, the more contextual, objective, and quantitative the approach to evaluating character, the better. Just as the reputation of a organization must be assessed relative to context, so must its reality. It pays to be part of comparative performance systems with similar organizations, as just one example. It also is important to have performance reporting that clearly articulates gaps in performances as well as achievements.

Part of the IRM process should focus on whether the organization has either created unrealistic expectations or had them imposed upon them. This can articulate itself very clearly in the gap between targeted results and resources. It can also identifying underlying demand or market changes that may cause the organization to under perform. IRM plays a key role in challenging these gaps.

Close Gaps.

There are no easy answers to closing reputational gaps. Part of the recognition of reputation as a high risk area for organizations is that many of the gaps are perceptual and therefore take time and consistency of effort to overcome. Here are some of the many areas that can be addressed in closing such gaps:

- Ensuring that targeted results and resources align,
- Ensuring that targeted deliverables and results align,
- Using governing bodies and external advisors for senior management on steps to take in building strong reputations
- Developing tools to measure not just results but trust and confidence in the organization's brand and competence (surveys, focus groups),
- Making sure that the organization does foist itself on its own petard with excessively optimistic projections, promises or inflated meaning to results,
- Developing a long-term and consistent plan for explaining your organization's objective, strengths, weaknesses and challenges to a variety of audiences through spokespersons, leadership and good presentational material,
- Putting the organization into the broader context of its mission through involvement with other organizations and the broader community,
- Testing your messages in a ground-truthing process, i.e. does this stuff really make any sense or are we just pleasing ourselves?

Monitor What Is Happening to Your Reputation

Understanding exactly how beliefs and expectations are evolving is not easy, but there are ways to develop a picture over time. Reputations can be damaged by single events, but are more likely slowly destroyed through long-term problems. For instance, regular surveys of employees, customers, and other stakeholders can reveal whether their priorities are changing. While most well-run organizations conduct such surveys, few

take the additional step of considering whether the data suggest that a gap between reputation and reality is materializing or widening. This is where integrating such surveys into the risk assessment process makes such good sense. Similarly, periodic surveys of experts in different fields can identify political, demographic, and social trends that could affect the reputation-reality gap. “Open response” questions can be used to elicit new issues of importance—and thus new expectations—that other questions might miss. It is generally useful to supplement these surveys with focus groups and in-depth interviews to develop a deeper understanding of the causes and possible consequences of trends.

Finally, organizations need to understand how the media shape the public’s beliefs and expectations. Dramatic changes in the amount of coverage influence how fast and to what extent beliefs and expectations change.

Find an Organizational Locus for Reputation

Assessing reputation, evaluating reality, identifying and closing gaps, and monitoring changing beliefs and expectations will not happen automatically. If integrated into IRM, much can be done to see this as an important underpinning of a resilient organization. However, depending on the size and nature of the organization, it would be wise to vest the “reputation file” with an executive. Working with communications support, but not depending on it entirely, the executive should work to look at reputation as if it were one of the key inputs to organizational success and see his or her role not as a reactive one but as a stewardship one. This means that reputation would be treated as a valuable organizational resource to which all the skills of management need to be applied, not simply an issue of having the best communications tools.

The chosen executive should periodically report to senior management on what the key reputational risks are and how they are being managed. It is up to senior management to decide whether the risks are acceptable and, if not, what actions should be taken.

Managing reputational risk is not an expensive undertaking that will require years to implement. In fact, many will argue, as they do with most risks, that they are already on the case. Maybe, maybe not. But IRM will make it clear whether this is really the truth. At most well-managed organizations, many of the elements are already in place in disparate parts of the organization. The key to successful reputation risk management is to recognize that it is not a communications or recovery exercise. It is about organizational character building that reflects out and instills confidence in those you most need to achieve your objectives.

Planning Your Communications Approach

No one says that you have to have a documented plan for everything. However, it helps to know what you need to do to effectively manage the reputational and communications elements of your IRM. Therefore, even if you do not intend to lay down

a specific plan, the following chart outlines some of the elements of a plan or planning process that you need to take into account.

Components of an IRM Communications Plan

For IRM, communications is a continuous process of both intake and output. Therefore, it is less event driven than crisis communications, although there are similarities as certain key stakeholders, the media and the public may interpret your identification of risks and your mitigation strategies as inadequate or cause for a strong reaction. Therefore, a plan will help your organization see if it can prepare itself well. Here are the key components of such a plan:

- Organizational audit/ appreciation of its current communications environment
 - *Addresses relationship building, trust & credibility, transparency & openness*
 - *Assessing your reputational strengths and weaknesses*
 - *Develop monitoring tools such as media scans, regular consultations*
- Risk Communication team with responsibilities defined
 - *Equal emphasis on planning & response*
 - *Must cross functional lines to include senior management*
 - *Not delegated to spokesperson alone*
- Key audiences
 - *Strategies to “listen” to audience*
 - *Building trust and credibility – reputation management*
 - *Factors in response to both input and output*
 - *Defining non-business elements of concerns, e.g. emotional response, safety concerns, security concerns.*
- Risk communication goals
 - *Pre- and post- event goals as well as emergency response goals*
- Media relations
 - *Working relationship with the press prior to an event*
- Emergency response
 - *Be first, right & credible*
- Recovery & evaluation

Section 8: Risk Resources and Information Sources

Websites

Bank for International Settlements: (for Basel 2) (www.bis.org)

Committee of Chief Risk Officers: for energy trading companies (www.ccro.org)

COSO (Committee of the Sponsoring Organizations of the Treadway Commission): (www.erm.coso.org)

Emergency Preparedness Canada: (www.epc-pcc.gc.ca/)

ERisk: extensive data, daily news, links (finance) (www.Erisk.com)

Federal Emergency Management Agency (US): (www.fema.gov/)

Geneva Association: insurance (www.genevaassociation.org)

Nonprofit Risk Management Center: nonprofit focus (www.nonprofitrisk.org)

PRMIA: try its search engine (ROSE: Risk Online Search Engine) but you must become a member (<http://prmiamembers.c.tcl.net/maabqfPaa0jXca5qCd0e/>)

Public Entity Risk Institute: nonprofits and governments (www.riskinstitute.org)

Protiviti Inc: this is a private firm that provides lots of free and useful material on risk. There is also an e-newsletter. www.protivit.com

Queensland Education: a site filled with practical applications from Australia (<http://education.qld.gov.au/strategic/policy/guidelines/risk/>)

Risk Center: finance-focus (www.riskcenter.com)

RiskInfo: broad RM subjects (www.riskinfo.com)

Risk Management Reports (www.riskreports.com)

RiskWorld.com: public policy (www.riskworld.com)

Standards Australia: special risk management site; information on ANZ4360 (www.riskmanagement.com.au)

Reputation Risk: Deon Binnemon on Managing Reputation: <http://deonbinneman.wordpress.com/>

Books

Alexander, Carol, **Operational Risk: Regulation, Analysis & Management** (2003)

Bernstein, Peter **Against the Gods: The Remarkable Story of Risk, (1997):**
(1995)

Grose, Vernon, , **Managing Risk: Systematic Loss Prevention for Executives,**
(1986)

Head and Herman, **Enlightened Risk Taking,** (2002)

Hoffman, Douglas, **Managing Operational Risk,** (2002)

Daniels, Kettl & Kunreuther, **On Risk and Disaster,** (2002), University of Pennsylvania

Drennan and McConnell, **Risk and Crisis Management in the Public Sector,** 2007,
Routledge

Lam, James, **Enterprise Risk Management,** (2003)

Leiss, William, **In the Chamber of Risks: Understanding Risk Controversies**
(2001)

Molak, Vlasta, Editor, **Fundamentals of Risk Analysis and Risk Management,**
(1997)

McNamee and Selim, **Risk Management: Changing the Internal Auditor's
Paradigm,** (1998)

Powell,D. and Liess,W: . **Mad cows and mother's milk: The perils of poor risk
communication.** Montreal: McGill-Queen's University Press.

Schwartz, Peter **The Art of the Long View,** (1991)

Shrader-Frechette, Kristin, **Risk and Rationality: Philosophical Foundations for
Populist Reform** (2000)

Skipper, Harold, Editor, **International Risk and Insurance,** (1998)

Schiller, Robert, **The New Financial Order: Risk in the 21st Century** (2003)

Tenner, Edward, **Why Things Bite Back: Technology and the Revenge of
Unintended Consequences,** (1996)

Articles

This is a list of important articles, papers and monographs on the integration of risk management within organizations. It is by no means exhaustive.

1. *A Conceptual Framework for Integrated Risk Management*, by Lucy Nottingham, Conference Board of Canada (4 pages) Contact: pubsales@conferenceboard.ca. It is brief, to the point and well-written.
2. "Enterprise Risk Management," by Jerry Miccolis and Robert Schneier, in *Strategy & Leadership*, March/April 1998, Vol. 26, No. 2 (6 pages). Contact: miccolj@towers.com.
3. "Integrated Risk Assessment: Current Views of Risk Management," by H. Felix Kloman, *Risk Management Bulletin*, London, February 1999 (drawn from article in May 1998 *Risk Management Reports*) Contact: fklooman@aol.com
4. *Leaving Nothing to Chance*, by Melanie Herman and Leslie White, Nonprofit Risk Management Center, Washington, November 1998 (30 pages). This is a Board primer on risk management, for nonprofits. Well written and succinct. See info@nonprofitrisk.org
5. *Enterprise Risk Management: An Analytic Approach*, Jerry Miccolis and Samir Shah, Parsippany, New Jersey, 2000 (36 pages) Contact: miccolj@towers.com
6. *Learning About Risk: Choices, Connections and Competencies*, by William Bradshaw and Alan Willis, Canadian Institute of Chartered Accountants (CICA), Toronto, 1998 (134 pages). A well-written description of risk management initiatives, describing the COCO (Criteria of Control) process. Contact: janice.turner@cica.ca
7. *Managing Business Risks in the Information Age*, Economist Intelligence Unit and Arthur Andersen, 1998 (98 pages). A current survey of global RM practices. Contact: newyork@eiu.com
8. *Financial Reporting of Risk*, Institute of Chartered Accountants of England & Wales, London, 1998 (51 pages) Guidelines for reporting; good definitions.
9. *Internal Controls - Integrated Framework*, Council of Supporting Organizations of the Treadway Commission, AICPA, New York, 1997 (157 pages) The US counterpart to the Canadian COCO (see CICA above). Contact: MRothchild@aicpa.org
10. "A Framework for Risk Management," *Harvard Business Review*, Nov-Dec 1994, by Kenneth A Froot, David S. Scharfstein, and Jeremy C. Stein. A guideline for financial risk management, especially hedging. Contact: custserv@cchbspub.harvard.edu
11. "Enterprise Risk Management - Pulling It Together," Andrew Berry and Julian Phillips, *Risk Management*, September 1998. Brief but over-focused on shareholders. Contact: phillij@towers.com
12. "Realizing the Rewards in Risk," Kimberley Birkbeck, Conference Board of Canada Members' Briefing No. 236-98 (June 1998). Report on the 1998 International Conference on Risk Management. A concise four page summary of papers. Contact: pubsales@conferenceboard.ca

13. "A Shoppers' Guide to Risk Management Systems," *The Risk Professional*, March 1999. Listing of software systems, primarily for financial risk. Contact: riskpro@llplimited.com
14. *Forewarned is Forearmed: Identification and Measurement in Integrated Risk Management*, Kimberley Birkbeck, Conference Board of Canada, Report 249-99, (January 1999). A well-written focus on risk categories, frameworks and measurement tools. Contact: pubsales@conferenceboard.ca
15. *Risk Financing Strategies: The Impact on Shareholder Value*, Deborah J. Pretty, Risk & Insurance Research Group, London, 1999. A challenging contrarian view on the utility of risk financing. Contact: rirg@rirg.co.uk
16. *A Guide to Integrated Risk Management*, Tom Cannon, AIRMIC, London, 1999 (24 pages), A concise description. Contact: enquiries@airmic.co.uk
17. "The New Religion of Risk Management," Peter L. Bernstein, *Harvard Business Review*, March-April 1996. A challenging view of the use of risk management, with three "dangers:" exposure to discontinuity, the arrogance of trying to quantify the unquantifiable, and the threat of increasing risk instead of managing it. Email: custserv@hbsp.harvard.edu
18. "How Risky is Your Company?" Robert Simons, *Harvard Business Review*, May-June 1999. A focus on growth, corporate culture and information management pressures and how they affect risk. Email: custserv@hbsp.harvard.edu
19. *Business Risk Assessment*, David McNamee, Institute of Internal Auditors, Altamonte Springs, Florida 1998. (107 pages) One of the best practical guides to integrated risk management. Contact: research@theiia.org
20. Don't Gamble with Goodwill, by Karen Thiessen, Report No. 284-00, Conference Board of Canada, Ottawa, March 2000 (14 pages). An excellent guide to communication risk information with key stakeholder groups. Contact: pubsales@conferenceboard.ca
21. Peters, R. G., V. T. Covello and D. B. McCallum. 1997. The determinants of trust and credibility in environmental risk communication: An empirical study. *Risk Analysis* 17: 43–54.
22. *Audit Committees: A Practical Guide*, The National Association of Corporate Directors, Washington, DC, 2000 (59 pages) Focus on the role of risk and risk management at the board level. Contact: info@nacdonline.org
23. *Risk Management: Changing the Internal Auditor's Paradigm*, by David McNamee and Georges Selim, Institute of Internal Auditors Research Foundation, Altamonte Springs, FL 1998 (219 pages). A thoroughly researched and current review of risk management literature. Contact: research@theiia.org
24. "Creating a Business Risk Inventory," *Internal Auditor*, February 2000. A description and useful graphic of Allstate Insurance Company's "Business Risk Inventory." Contact: cbarber@allstate.com
25. Jungerman, H. 1997. When you can't do it right: Ethical dilemmas of informing people about risks. *Risk Decision and Policy* 2 (2): 131–45.
26. *Operational Risk*, a special monograph published by Risk Professional, March 2000 (108 pages) that includes a series of well-written articles on operational risk. Contact: riskprof@llplimited.com

27. Fischhoff, B. 1995. Risk perception and communication unplugged: Twenty years of process. *Risk Analysis* 15 (2): 137–45.

Risk Management Standards

Both private firms and public organizations have an array of standard-setting bodies, depending on the kind of work they do. Certainly, the most pervasive are accounting standards. Standards do not have the force of law, but are close. Therefore, in the realm of risk management, it is good to know what is out there and how it might relate to your organization. In addition, these Standards can provide useful guidance in the design of your IRM. They can also be powerful tools in selling IRM in your organization or in explaining the reasons for implementing it to stakeholders. Finally, adhering to or effectively using Standards can be used as a sort of good housekeeping seal, one that validates what you are doing and as a means of assuring stakeholders that you are pursuing desired outcomes through IRM, ones that national or international organizations endorse.

The following, therefore, is a useful list of Standards in integrated risk management.

<p>A Risk Management Standard – Institute of Risk Management (UK), available at http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf</p>
<p>AS/NZS 4360:2004, Risk Management Standard, available through purchase at http://www.riskmanagement.com.au/Default.aspx?tabid=148 Note: As already mentioned in the history section, this is the grandmother of all risk management standards in the world. It remains a powerful and robust thought leader for both public and private organizations.</p>
<p>Project Management Risk Management Standard, British Columbia Ministry of Sustainable Resource Management, available at http://srmwww.gov.bc.ca/imb/3star/sdlc/8manage/risks/risk_std.html#VERSION%20CONTROL Note: There are many standards like this available at what some might call a more micro level. Project management is a sub-set of management. However, this particular one is well written, straightforward and concise.</p>
<p>Risk Management Policy of the Government of Canada: http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/siglist_e.asp</p>
<p>Risk Management: Guideline for Decision-Makers, CAN/CSA-Q850-97 (R2002), available at http://alert.scc.ca/openstandardsalert/search_form.cgi?stdnumber=&title=risk+management&all_fields=&sdo=998&language_1=1&language_2=1&L=E&find=Search+for+standard%28s%29&first=1&last=15&lan1=true&lan2=true&session_ID=</p>
<p>COSO, Committee of Supporting Organizations of the Treadway Commission, Enterprise Risk Management – Integrated Framework, 2004 an Executive Summary is available at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. It has international influence and is seen as a standard setter and leader in</p>

implementation sound financial and governance practice. The Treadway Commission is otherwise known as the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

Canadian Standards Association: CAN/CSA-Q850-97 (October 1997), "Risk Management: Guideline for Decision-Makers, A National Standard for Canada."

Section 9: Questions and Answers

Why is risk assessment important?

Managing risks puts you in control since it leaves your organization less open to chance. A risk assessment helps to prevent accidents and ill health to you, your workers and members of the public. Accidents and ill health can ruin lives and harm your business too if output is lost, equipment is damaged, insurance costs increase or you have to go to court.

How do I do a risk assessment?

Most risk assessment processes follow a similar format:

- Identify the hazards
- Decide who might be harmed and how
- Evaluate the risks and decide on precautions
- Record your findings and implement them
- Review your risk assessment.

What's the use of a risk matrix?

It's a tool, pure and simple, for working out a risk level by categorizing the likelihood of the harm and the potential severity of harm and then plotting these two risk determining factors against each other in a risk matrix (see below). The risk level determines which risks should be tackled first. As with any other method of risk assessment you should not overcomplicate the process e.g. by having too many categories.

		Potential severity of harm		
		Slightly Harmful 1	Harmful 2	Extremely Harmful 3
Likelihood of harm occurring	Highly unlikely 1	Trivial 1	Tolerable 2	Moderate 3
	Unlikely 2	Tolerable 2	Moderate 4	Substantial 6
	Likely 3	Moderate 3	Substantial 6	Intolerable 9

Using a matrix can be very helpful for prioritizing actions. It is suitable for very many assessments but particularly lends itself to more complex situations. However, it does require a fair degree of expertise and experience to judge the likelihood of harm accurately. Getting this wrong could result in applying unnecessary controls or failing to take important ones.

When do I need to do a risk assessment?

Risk assessments at the organizational level should be part of your planning process. You should carry out an assessment before you do the work that gives rise to the risk, and review it as necessary. Also, when the risk level is unknown. A robust risk assessment process, that is one that is sustained within the organization, will also want to regularly review existing risk assessment, because circumstances and the risk drivers will inevitably change.

When should I review my risk assessments?

Few organizations stay the same. Sooner or later, you will bring in new equipment, substances and procedures, and that could lead to new hazards. Therefore, you will need to review where you are every year or so, to make sure you are still improving, or at least not sliding back.

During the year, if there is a significant change, don't wait: check your risk assessment and where necessary, amend it. If possible, it is best to think about the risk assessment when you're planning your change - that way you leave yourself more flexibility.

Do I need to get consultants in to do my risk assessment?

This will depend. The bottom line is that most organizations benefit from consultant help in the policy setting and design phase, but that implementation needs to part of the organizational capacity. Risk assessment is a straightforward process that most people can do, given a little time and effort. You will probably need help if you have particularly hazardous or complex processes, but for the majority of organizations, you or a competent member of staff should be able to complete a satisfactory assessment. Once you have the policy, procedures and training to back it up.

Do I have to record the findings of the risk assessment? If so, why? Isn't that just bureaucracy?

It makes sense to keep a record of the assessment so that when you come to review it, you can check back to see if anything has changed. It is also useful to keep a record so that you can share the findings with your staff, stakeholders and governing bodies. Finally, it proves that you have carried out the process if a health and safety inspector asks about it.

Is there a specific form/format that I have to use to record a risk assessment?

No. But there are plenty of examples around. The key is for the organization to adopt one and use it consistently.

Isn't risk assessment nonsense? Everybody is grown-up in my organization and can look after themselves. Aren't we all risk managers on a daily basis?

Everyone hopes so but what does that have to do with the organization and its objectives. IRM is built on the assumption that the people in the organization are trying to do the job they understand they are there to do with the tools they are given. Risk management, on an organizational level, is part of ensuring that happens. Its also a way for everyone who is pulling their weight to signal to the organization that things are changing, that adjustments are needed and maybe, must maybe, they need some back-up.

Doesn't risk assessment just lead to more and more rules safety measures - most of which aren't necessary?

There's a real danger that people will confuse policies, processes, reports and more paper with action. Risk management is not at fault here. The organizational culture is.

Is our organization just risk averse.

The answer you want to hear is: We don't think so. The approach is to seek a balance between the unachievable aim of absolute safety and the kind of poor management of risks that damages the organization and people associated with it. In a nutshell: risk management, not risk elimination.

What is the precautionary principle?

The precautionary principle should be applied only in very particular circumstances. It is highly unlikely to be relevant to your work. The precautionary principle says that where you have good reason to believe that something might cause harm but there isn't enough scientific knowledge to carry out a full risk assessment, you should not take the course of action until there is evidence that it is safe. This should not be used as an excuse to do nothing to prevent harm. The precautionary principle is therefore applied to a few new hazards until enough is learned about the risks they present. It should not be applied to well-known hazards where the broad level of risk has been established. If you applied it universally, you would have a complete stoppage of most activity including crossing the road. It is, in many ways, the antithesis of risk management.

What is the difference between risk appetite and risk tolerance?

Both risk appetite and risk tolerance set boundaries of how much risk an organization is prepared to accept. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable and necessary to meet its objectives. Risk tolerances are narrower and set the acceptable level of variation or error around objectives and targets. For instance, an organization that says that it does not accept risks that could result in a significant loss of its revenue base is expressing appetite. When the same organization says that it does not wish to accept risks that would cause revenue from its top-10 customers to decline by more than 10% it is expressing tolerance. Operating within risk tolerances provides management greater assurance that the organization remains within its risk appetite, which, in turn, provides a higher degree of comfort that the organization will achieve its objectives.

How does an organization determine the right amount of risk for the value it is trying to create for stakeholders and how should it communicate its risk policy to stakeholders?

The level of risk that an organization is willing to accept is a management decision – and there is no right answer to this question. One management group will pursue a higher-risk strategy while another will pursue a lower risk strategy. The shareholder should understand the risk chosen by management and invest in accordance with his/her own tolerances for potential variation in stock performance. Governments need to do the same. Organizations communicate the levels of risk accepted through the Management Discussion and Analysis portion of their financial reporting, quarterly and annual performance reports, press releases, investor calls, public statements etc.

What is the relationship between effective integrated risk management and improved financial reporting and transparency?

There are natural linkages between IRM, improved financial reporting and transparency. An IRM requires that organizations establish a risk appetite, measure actions and decisions against that risk appetite and communicate results. Communication of enterprise risk management to users of financial information clearly enhances transparency.

Is this intended only for private organizations? Is there any organization this is not intended for?

IRM is a process that organizations of all sizes and degrees of sophistication should consider. The framework is scalable, enabling organizations to be able to match the process to their complexity. There is an intrinsic expectation that all organizations be they for profit, not-for-profit, government organizations, etc, each work to manage risk. A good IRM will facilitate the process.

Does this mean replacing an Internal Control Framework with an Integrated Risk Management Framework?

No. An Internal Control Framework is conceptually sound and has stood the test of time. It is an inherent part of an overall risk management strategy. An Integrated Risk Management Framework is a broader framework that incorporates the internal control framework within it. In other words, one approach to risk is to develop controls to mitigate the risks. The frameworks are compatible and are based on the same conceptual foundation.

What is the relationship between technology controls and effective integrated risk management?

Any IRM process requires feedback of information from throughout the organization. This information must be current and accurate and must be robust enough to support the analysis of different risk responses. Therefore, the technology that provides this data must have the highest levels of integrity and controls. IRM cannot be effective if the technology that provides the data used to manage risk is flawed.

If you have good internal control, isn't that a way of managing risk?

Of course it is. A strong system of internal control supports the achievement of the organization's business objectives and therefore good internal control is a way of managing risk. However, integrated risk management is much broader than internal control. In addition to supporting management's efforts to achieve its objectives, it aligns risk management with strategy setting and aids an organization's ability to assess whether the organization is accepting risk appropriately.

What is the role of the board in IRM? For that matter, what is the role of a City Council or Minister of a Department? How does this framework help them?

These entities provide oversight of IRM. They will be asked to understand key elements of IRM, inquire of management about risks, and concur on certain management decisions. However, they are not in the position of making choices on behalf of management and do not alleviate management's role in enterprise risk management. They will expect that management is undertaking an appropriate level of risk management, regardless of what they call it. Having in place a systematic approach like IRM gives governing bodies and leaders a greater level of assurance.

What is the role of the CFO and others in the financial management organization in IRM.

The CFO and the financial organization play a key role in providing the needed disciplines and procedures to establish risk management as an integral part of the business strategy setting process. The CFO provides the organization with analytical

tools to help determine risk appetite and risk tolerance. The CFO is well positioned to look across the businesses and functions within organization to develop and implement the portfolio view of risk. He/she has the experience and knowledge to establish controls necessary to assure that the evaluation of risk is a continuing and integral part of the management process and is consistent with the risk management philosophy agreed to with the board.

What is the role of internal auditors in enterprise risk management?

Governing entities and audit committees have an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective. Internal auditors can assist both management and the audit committee by examining, evaluating, reporting, and recommending improvements on the adequacy and effectiveness of management's risk management processes. Using an IRM process that is standard driven provides a benchmark for internal auditors to use in the evaluation of their organization's risk management efforts.

Who are the potential implementers of an IRM?

The framework is robust. It works best when an organization develops an integrated process to address risk throughout the organization, and further, that risk approach is led from the top of the organization. The right IRM framework can be used in all functional areas, including information technology, finance, accounting, internal audit and risk specialists within any organization. However, a good IRM framework is designed to promote entity-wide capabilities for identifying, documenting, and dealing with risk on a consistent basis.