INSTITUTE FOR RISK RESEARCH

EXECUTIVE WORKSHOP:

IMPLEMENTING RISK MANAGEMENT IN 2008

Friday May 9, 2008
Toronto, Ontario

Editor: John Shortreed

Broadleaf

TABLE OF CONTENTS

'Implementing Risk Management in 2008"; Notes on workshop discussions

By John Shortreed with contributions from note takers Diana Del Bel Belluz, and John Lark as well as comments from speakers and participants.

The May 9 workshop was attended by those listed and the presentations followed the order shown in Table of Contents.

This section of the workshop report contains, in point form, the discussion and comments during the workshop, prior to the workshop and after the workshop. The content of the slides is included elsewhere. The points tend to follow the workshop program unless assigned for convenience to other sections than where they happened.

1) **Nature of the Participants and their issues** - The workshop attendees included 11 consultants and 5 risk management practitioners from the City of Ottawa, Department of National Defense, Hydro One, and the Government of Ontario). The participants indicated that they were most interested in seeing how to;
   a) achieve consistency in applying ERM (Enterprise Risk Management, or ISO 31000 being the same thing in terms of application to the whole of the organization), particularly for organizations with many Business Sub Units,
   b) integrate risk management into business processes using a holistic, organization specific framework,
   c) start risk management as soon as possible, often by first helping people understand their risks in a consistent and reliable way
   d) gain commitment from the organization to risk management by energizing and engaging people, in a way that is sustainable even for mature ERM frameworks,
   e) make sure key decisions on risk are taken by the organization's senior management and not delegated to consultants, or others
   f) accommodate "front page" events that may happen as ERM is implemented,

2) **Overview of ISO 31000** - John Shortreed
   a) The standard represents an international consensus on best practices
   b) Each organization must develop a risk management program that fits its unique management culture, goals, objectives, and business environment. Therefore, by design, the standard does not propose a process for risk management that is certifiable.
   c) Because risk is about uncertainty, a key practice is to review assumptions and analyses. Particularly as circumstances change over time. Risk indicators are key to performance improvement,
   d) The idea of "positive" risk in 31000 was illustrated by the US democratic nomination race where the objectives of more votes and more money and the associated uncertainty, or risk, has seen innovative risk treatments by Barack Obama using the internet, facebook, intergenerational pressures and other risk treatments to increase positive outcomes as well as treatments such as "looking and acting presidential" to deal with traditional negative political risks. It was noted that you will not "get what you want" (sing song please) if risk is thought of as only negative.
   e) Activity to set objectives can be valuable since organizations often recast themselves from say "a distribution company to a wires company" with an improved view of risks and how to make the most of them.
   f) It is expected that many supplemental standards to 31000 will be developed to provide more detailed guidelines for risk assessment methods (e.g., ISO 31010), internal audit, risk communication, legal services, national risk management standards, and so forth.

3) **Implementation of Enterprise Risk Management** - Grant Purdy presented a logical overview of what is needed to operationalize risk management that focused on how to design and introduce a systematic risk management framework. Some key points:

a) The whole is more than the sum of its parts. Risk Management consists of some key elements that must be integrated with key parts of business practices. If you are missing a key element of risk management it won't work. If linkages aren't made to other key management disciplines (e.g., strategic planning, performance management, reporting), risk management won't work. This includes situations where the organization does not have established processes and skills in essential management elements such as strategic planning, performance management, etc.
b) the 'principles' and 'attributes' given in 31000 can be used to conduct a gap analysis of what you have and what you need in terms of those essential risk management components and how well they are integrated with your general management processes.
c) Maturity is when risk management just becomes something you do as an integrated or embedded part of management. For example, the Risk Management Process (Figure 3 in clause 6 if 31000) does not have a separate decision box since it is not really a flow diagram but a relational block diagram of integrated decision making – there are decisions in many of the process activities.
d) The separation of tasks such as setting priorities, implementing controls, and auditing performance, will follow normal management structures, roles and responsibilities in the organization and while enhanced by risk management are not dictated by risk management.
e) If you don't have an objective you don't have risk. Think 31000 got the definition of risk right – "effect of uncertainty on objectives" – seems to be a good step forward. Should help with culture change needed to accommodate ERM. Also the move from a hazard approach to one of looking at events (or a set of or change in circumstance) is facilitated by 31000 since event defines the thing that effects objectives (and should eliminate issues of what is a driver, etc.). Just want to magnify the upside and reduce the downside consequences.
f) Tendency to not accurately estimate likelihoods, particularly in the health and safety field. In general people have trouble with appreciating likelihood (and thus risk) and may tend to wish it away or even lean on advice such as "reasonably practical" to have others make risk treatment decisions for them.
g) The monitor and review step includes root cause analysis - of both successes and failures.
h) "Risk response" is the same as "risk treatment" – 31000 had to pick one term, time will tell if the choice was the right one or not – at this point really academic.
i) There is an issue (partly post workshop) of full versus partial implementations of enterprise/integrated risk management. The evidence of many partial implementations of ERM support the assertion that risk management won't work if you don't have all the pieces. Most organizations have built their program incrementally. It is an exceptional organization that has arrived at a mature level where the corporate risk management activity becomes redundant. One such organization is BHP Billiton where for example, there are 80,000 risks in their risk management information system and 50,000 controls. Similarly MARS have a mature system that mirrors 31000, with few if any gaps, but they do not view it as complete but a work in progress. Perhaps the answer is that ERM is a journey not a destination.
j) Grant indicated that in BHP there is no longer any central RM and he thought that most firms would eventually be like this – the champions (6 sigma black belt like people for RM rather than statistical inference in multi-variate data rich situations) may be sufficient to initiate innovations in RM and a community of practice (network) will keep the organization at the forefront of best practice.

4) **Climate Change example of risk management** - Dale Cooper
a) Good example of a ubiquitous risk that almost any organization must manage. It is also a risk with non-linear effects, i.e., small changes can have large impacts, for example small increase in temperature leads to big increase in power demand for air conditioning. Coca Cola is concerned about the availability of water of good quality. How to take a vague big risk and actually deal with it?
b) The discussion after the presentation focused on thinking about positive and negative outcomes instead of concentrating on the downside only. It is amazing how many risk experts, let alone lay people, have trouble with this concept – that some uncertain outcomes will be good things in terms of our objectives.

5) **Canadian Financial industry's implementation of elements of ERM** - Matthew Hilbert.
   a) Nice overview of financial sector's approach to operational risk management. Goldman Sachs is an industry leader. However, so far the norm is individual elements of ERM and not a holistic approach.
   b) The 'calculation of capital' approach works well for credit and market risk because it is possible to build and validate quantitative models for these risks. The quantitative methods are difficult to apply to operational risks because they tend to be dynamic in nature and as a consequence, data is difficult to access or lacking altogether.

6) **Integrated Risk Management Workshops** - John Lark
   a) A solid methodology for conducting risk assessment workshops particularly. Workshops can be a "safe" place to discuss risks, they can help change culture, they can focus and organize teams of 'experts' to gather expert opinion/information in a structured setting. Workshops can focus on risk assessment (identification, analysis, or evaluation) or risk treatment. Many gems in his presentation including:
      i) "Jiminy Cricket" model of reminding people to do risk management.
      ii) The concept of getting 'pitchers' and 'catchers' to understand one another's worlds (slide 3).
      iii) A handy guide to the composition of the workshop participant group (slide 6).
   b) The post-presentation discussion confirmed the value of risk assessment workshops to harness the 'wisdom of the crowd' and to search for "unknown-unknowns" (famous even before Rumsfeld. More importantly these workshops provide a valuable forum for discussion about material risks and about the adequacy (or inadequacy) of existing risk treatment strategies. Discussion is a key value of workshops and may help people usefully confront their assumptions and do reality checks of existing risk management effectiveness. Their outstanding characteristic is that they are simple, easy to understand, and if done carefully can have the appropriate level of rigour and provide important contributions to the Risk Management Process.
   c) The discussion on the relative merits of voting technology was technical and perhaps not very useful in this forum.
   d) While workshops are a good mechanism for getting information they should be used with care. For example, many workshops use a risk matrix perhaps without realizing that if the matrices are based on arbitrary scales then they are qualitative not quantitative and should not be used to calculate "risk."
   e) Use of matrices for risk ranking is common. The point made that the scope of the workshop needs to be crystal clear – is it for identification, evaluation, analysis, rationalization of options, risk ranking, etc.
   f) The need for preparation focused on the objective for risk workshops is paramount, one example had the preparation as a "white paper" where the options provided to the workshop as choices were developed by the managers responsible in consultation with those they report to and those who report to them, so the white paper options were limited and were highly relevant (also perhaps less innovative but that would be handled elsewhere in the system).
   g) If risk matrices are used then there needs to be an understood "scaling" of risk measures as the level in the organization changes. There are different risk tolerance/acceptance ranges at different levels in the organization. This can be the subject of a vertical workshop, preferably with some options presented to the workshop. Usually called the roll up-roll down problem/issue.

7) **Discussion** – all Topics discussed are given below except where they could be integrated with comments above in sections 1 through 6, also there is no differentiation between pre, post or actual workshop comments. (editor).

   a) ISO 31000 is excellent. An ISO standard framework, terminology and process, may provide a mechanism to reduce the discontinuity between technical and people dimensions of risk management – it is necessary but not sufficient. Today there are numerous methods and standards available for risk assessment, risk reporting, etc. yet risk management has yet to take hold in most organizations. At the

end of the day, the shift to systematic risk management requires a change in management culture, an inculcation of the risk discipline into business practices. ISO 31000 also should save time and resources since it will provide for an "instantaneous" framework for ERM.

b) People don't change their behaviour because they receive new information. Rather, they change because of relationships and networks, i.e., because they see other people (e.g., their leaders, their peers, their competitors) are changing. It is time for the risk management community to shift its focus from creating the ultimate framework in the mistaken belief that these tools will inspire proactive risk management. We have plenty of serviceable methods and tools. What we need now is to focus on creating and leveraging networks to precipitate the tipping point for modern risk management. Using Malcolm Gladwell's terminology, we need to identify and activate *mavens, connectors* and *salespeople.* This will require developing social networks that extend beyond the risk management community. That will require developing language and talking points about risk management that resonate with members of the broader business community. It's time to stop thinking like hall monitors who look for weaknesses in risk management and instead act like evangelists who inspire people to change their behaviours! In some settings there is a great deal of skepticism about risk and this makes risk management training difficult. In some instances, this skepticism on the part of senior decision-makers is borne out of a lack of understanding (and a subsequent lack in trust) in risk analytics. In other instances, skepticism is created when the risk analytics produce results that do not align with the decision-maker's gut instincts and perceptions of the significance (or insignificance) of particular decision parameters and risks. And in some cases, what is overtly expressed as skepticism is actually a covert effort to avoid the discipline imposed by the evidence produced in the decision and risk analysis processes.

c) "Black Swans" (17 weeks at top of non fiction list in 2007 – see http://www.fooledbyrandomness.com/ or http://www.forbes.com/2007/05/23/nicholas-taleb-innovation-tech-cz_07rev_nt_0524taleb.html for main argument of author N.N Taleb) "Before the discovery of Australia, Europeans thought that all swans were white, and it would have been considered completely unreasonable to imagine swans of any other color. The first sighting of a black swan in Australia, where black swans are, in fact, rather common, shattered that notion. The moral of this story is that there are exceptions out there, hidden away from our eyes and imagination, waiting to be discovered by complete accident. What I call a "Black Swan" is an exceptional unpredictable event that, unlike the bird, carries a huge impact." – continues. Douglas and Wildowski identified the importance for risk management of the 'robustness' of organizations, which may be improved by ERM has been argued to provide some accommodation of black swans. "But we do know who society's winners will be: those who are prepared to face Black Swans, to be exposed to them, to recognize them when they show up and to rigorously exploit them " (ed. – all new to me, have learned one more thing from the workshop – particularly enjoyed the quote from Taleb from LSE "We don't know what we are talking about when we talk about risks and opportunities"). One participant notes - *As someone who has worked in the risk field for almost 30 years, I found Taleb's arguments to be a jolt from the blue, and a serious warning not to take what we do as risk practitioners too seriously. One can't ignore what he says, because there are too many examples where normal risk assessment and management practice has failed miserably. His two books (noted above) should be required reading for anyone in the risk field. You don't have to agree with him, or even enjoy his style of writing (most don't) but you have to read his books, or at least read "Fooled by Randomness" if you think you only have time for one*

d) Documentation included in clause 6.7 of ISO happens at every step in the Risk Management Process, "as appropriate". With the advent of modern IT systems, documentation is not the problem it used to be and in any event is not something special for risk (except for the special requirements for risk communication due to risk perception) but a regular part of corporate arrangements for liaison, control, command, motivating, etc. within the organization.

e) Size of Risk Management Department for an organization with many regional locations? Suggested that from 1 to 4 people in the "central coordinating/facilitating department" were needed. Pay attention

if the risk management department gets larger than this as this means that the function is being taken away from the individual regional managers and this is not desirable according to 31000. Realize there is a coordinating issue but this should be handled by the coordinating function within the existing organizational structure roles and those who have responsibility to coordinate the regional offices – not a separate function for Risk Management.

f) Quality has to go into organization as a fundamental objective, not real special to RM, even though 31000 has the plan/do/check/act and is often placed into categories of quality standards as in Canada.
g) Regulatory – a general observation that industries that have higher regulation may be risk averse and have a higher interest in risk management.

Items left for another day

i) Software and budget for implementation (perhaps the best approach is to do manual first then once approach is known then and only then look for software).
ii) For large implementations how to keep things organized and monitored? Dissemination of risk information to make sure everybody is on the same page during the high volume of training.
iii) Role of insurance versus other treatment options. While one of the most used risk treatments insurance is only one of many treatments and might be best thought of as a treatment for standard problems and even as a treatment of last resort when the other 3 of the big 4 treatments (avoid/embrace, treat by enhancing or reducing either consequences or likelihood, taking the risk), are not done, leaving risk sharing (also know as transfer, but share is preferred since often some of the positive as well as negatives are shared).
iv) Risk and Regulation (note that the London School of Economics has a good site for this with lots of information, newsletters, etc.) For example, it is interesting that their take on nuclear regulation is like Canada's and is only for public safety and not including positive outcomes like isotopes to save lives in health care.
v) How to implement training – noted that Grant and Dale were on a train the trainer mission to Canada for a Canadian organization to leave them with some 32 trained managers after 2 weeks. These managers were regular managers with other roles, who like the 6 sigma "black belts" in GE would after training have other "attributes" or employees skill sets and might be thought of as facilitators for others and not as some sort of substitute for managers doing their own RM.
vi) Self help for Risk Managers (central office types assumed). The workshop was a sort of self help event but the question was what else could be done for these people (i.e. central Risk Management people who may be seen being in a dead end and generally negative job)
vii) Learning about RM how to structure, encourage – discussed along with quality and implementing training to some extent, but not really discussed in any depth. In some risk situations, like Society for Risk Analysis type "uncertain risks" of cause and effect, there are some standards which show explicitly the learning loops (check think it is the US red book revised??)

Closing Comments – All

Pleased to be here, good feedback, sector to sector interaction is useful. These sorts of forums are useful and valuable, always something new to learn, more than one way to skin a cat. Question is "how to organize user groups?" (know of one which just started inviting people for lunch meetings and rotated hosting). As a visitor this country is quite interesting as it is often seen as similar but really is quite different up close. Some reading lists would be useful. Particularly liked the context part. Last but not least – ISO 31000 seems to be a starting point to build on.

Pre-Workshop interview issues (of possible interest)

The following responses from the participant's interviews suggest the number one issue is how to integrate 31000 into the regular organization structure and processes and then maintain and sustain ERM. Also high on the list are issues of techniques for integrating and linking strategic risk management and operational risk management as well as conducting workshops to elicit expert opinion.

Risk Management Activities done by participants

1. Advising clients or company or ministry on technical risk issues and helping them evaluate and categorize risks, set priorities (evaluation in ISO), and identify mitigation (treatment in ISO) (7 people)
2. Facilitate workshops to assist organization decision makers assemble expert opinion and technical expertise to carry out the risk management process (clause 6 of 31000) (4)
3. Chief risk officer with responsibility for risk management in the organization.(1)
4. Promote a consistent context and approach around the globe and across industry sectors. Technology transfer among offices, bringing our senior people on board with a service platform that complements all our other services.

Current Challenges (combined responses, grouped by issue)

<u>Issue #1</u>

Communicating to clients that the major risk decisions that they face are decisions that must be made at the highest level in the company - even at board level. Typically clients will ask a consultant to make a decision, but a consultant's proper role is to inform the client of the risks inherent in the various options, but the final decision on which course of action to take is often so huge that only the board has the proper authority to make it. An example - a mining company will ask a consultant to decide the slope of a large open pit mine. (steep slope = more revenue but greater risk that the whole thing will fail). This has huge risk/reward implications that affect shareholder interests. Only the board can make such important decisions, informed by the specialist skills of the consultant. Then we (consultants) have to get better at predicting probabilities of failure. And costs of such failures. (Our clients often suffer such setbacks, slope failures, mine collapses, accidents, flooding of mines) and tailing ponds that kill wildlife (April 30 news item). Communications of the results of risk analysis to decision makers is difficult since they may give lip service but that is all. CEO support is critical. Leadership is critical. ERM needs to be entrenched in organization processes including budgeting. How to demonstrate and create value of risk management? How to get upper management to understand the risk analysis done by specialists? Want ERM to stick, it is all about changing culture, too often people are too much analytical (frameworks, tools, techniques) and not enough people oriented when both are needed in balance

<u>Issue #2 – Same as #1?</u>

ERM is not going well since it is not sustainable in the organization due to lack of commitment of senior management. Starts but fizzles out. Does not have staying power. Not sure if this is a top down or bottom up problem? Should there be a soft approach or strong approach to integrating ERM? Change management needed was too much. How to make RM organic and growing? People do not seem to know what to do to make it work. How to get buy in without taking away rights to make decisions and control of own environment? How to implement 31000 successfully? Many challenges in organizations, as each group think they are special and different and do not talk to each other or look to outside experts for X-fertilization to seek out good ideas from others. For example, banks and health care are struggling yet there is best practise in other areas such as agriculture and process safety. Need more "market" research for methods and solutions to the embedding of risk management in culture of organization. Talking in your own echo-chamber.

Issue #3

How to link strategic/organization-wide risks with operating/site-specific risks? How to roll up and roll down risks between them? How to break down strategic risks to operational levels? Balancing tensions between strategic and operational. Tend to wave our hands a lot but not clear what solution is. Difficulties in communication and implementing "corporate" risk management programs at the operations level

Issue #4

Classifying risks such as reputation risks due to media coverage. Tendency to mix up types of risk or even the nature of risk itself (e.g. outrage is it a risk or a consequence?) People confuse drivers and consequences.

Issue #5

Facilitating workshops in risk management process. Technical people tend to lead the debate may shut out others. Communications is critical. Used for allocating resources and setting budgets. How to help sort out objectives of organization?

Issue #6

In maintenance mode needs are different from start up of risk management, need fewer staff (typically 2-4 is sufficient), how to keep enthusiasm going, focus on workshop facilitation,

Issue #7

Different practices and terminology in different fields (E.G. eco and human health risk, probabilistic engineering assessment, uncertainty analysis, operational risk, project and enterprise risk etc.) gives rise to confusion around risk and its management with a resulting tendency for people to "make it up" by addressing risk in their own way as they go.

Needs from the Workshop

1. Keep ahead of the curve on innovations and trends in risk management. Find out what Australians are doing and thinking (several responses!). What is best practise?
2. How to approach issues #1 and #2. 31000 has the objectives, framework, but how to make it work?
3. How to benchmark ERM against other companies?
4. How to get a working understanding of “positive” risk in 31000?
5. Techniques of communication/education with senior management.
6. How to judge the Quality of risk assessments and what level of quality is sufficient?

Other

1. Risk management is really a proxy for good management.
2. Theory to practise issues.
3. The definition of risk Guide 73 which broadens the concept from Guide 51 but linking the definition just too uncertainly creates more confusion. One of the attached notes should be used as the definition and uncertainty moved to a note (as per other standards). The uncertainty definition also does not flow with Figure 1 or the remaining terminology.

Risk management best practice is ISO 31000

John Shortreed
Director, Institute for Risk Research
University of Waterloo

IMPLEMENTING RISK MANAGEMENT IN 2008

Toronto May 9, 2008

ISO 31000 is a must have for Organizations

- International standards allow for easy interchange of ideas, contractual arrangements, and innovation
- Standards can also be check lists, meaningless exercises in futility and a boon to consultants
- 31000 is non certifiable which makes it a good standard
- Now 10 years since ISO Guide 73 and 20 years since AUS/NZ 4360 and CSA Q850 – well discussed, tested, and validated
- *Why did the Canadian cross the road?*

31000 is high level but comprehensive

- 30 countries have met for some 40 + days
- NO significant GAPS and COVERS almost ALL POSSIBILITIES
- Translation may be needed, for example, Canada will have a supplementary standard
- Implementation is not trivial, large companies will have 100+ existing risk management activities with different terminology, processes, etc. – JUNGLE OUT THERE

Short History of Risk Management

- 3000 BC – right or wrong Captain is right and goes down with the ship
- Darwin "survival of the fit" – get fit
- "if you have an enemy, kill them" – The Prince
- Safety in numbers (insurance) – Loyd's coffee house
- Britannia rules the seas – good set of controls for internal (Billy Budd) and external risks (North America)
- 1960 Zurich Re Blue book (heat map, teams, risk criteria, identification, the works), or Boeing first?
- 1965 Drucker – "risk in every decision"
- Against the Gods - Peter Bernstein – foundation
- Risk ManagementBooks - 1 per week
- 2009 ISO 31000 – positive risk and best practice

One view of an Organization

- Directed, non-equilibrium, SYSTEM of AGENTS
- “No optimal system configuration”- Mike Batty
- Norm is constant change at the top, think Loblaw, Stern
- Agents independent within corporate context
- Management games like scenarios, what if?, to understand the chaotic, teeming, caldron of risks
- Rules/accountability to protect society, public, employees, and to guide management
- 31000 is needed particularly with globalization

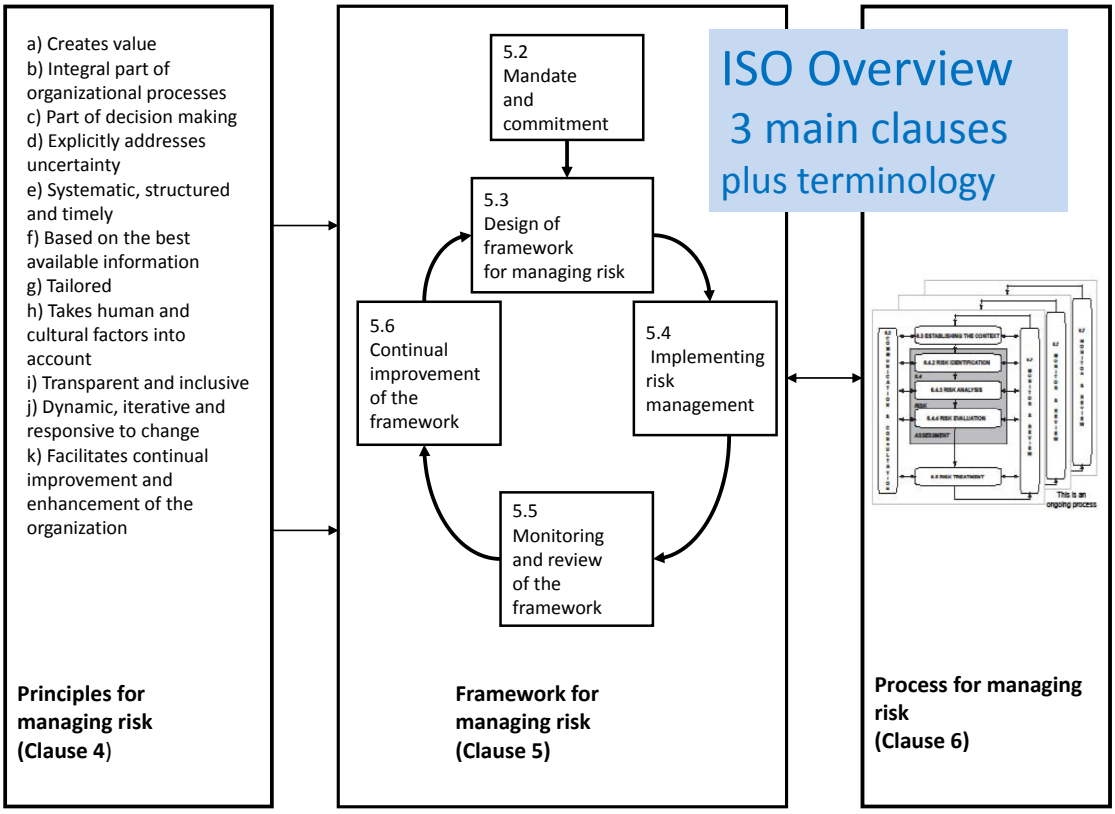
What is ISO 31000?

- Principles and Guidelines on Implementing Risk Management

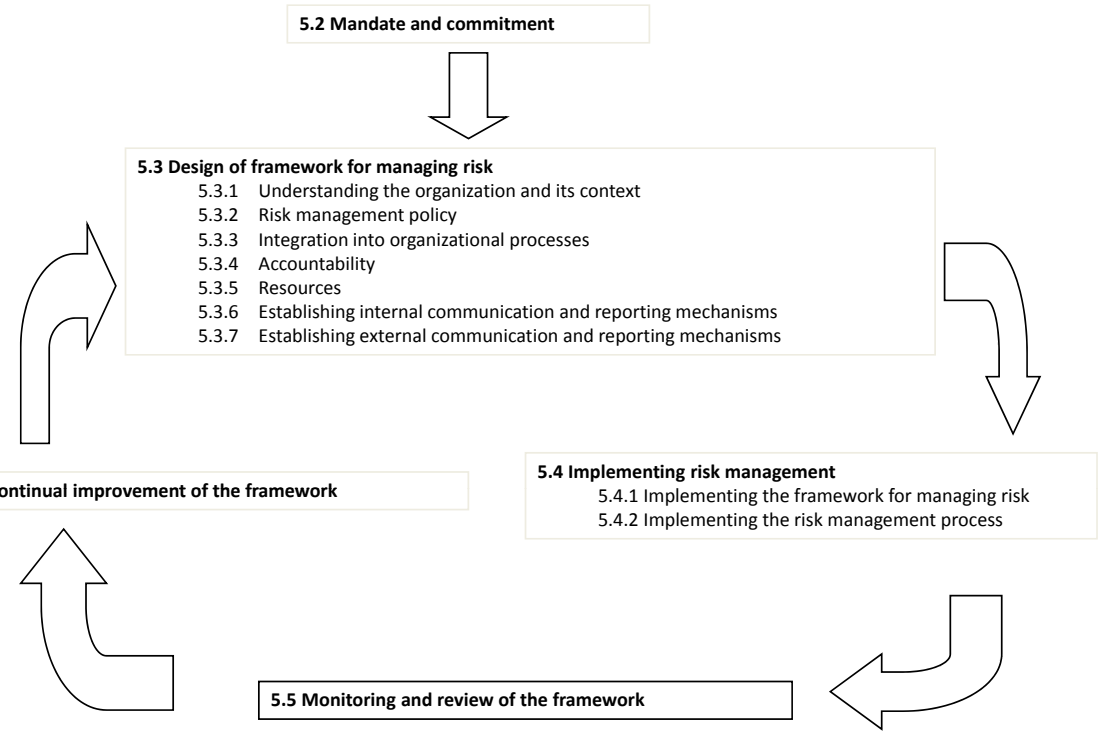
- 11 principles and 5 attributes of excellence

- OBJECTIVES driven within Context by Risk Criteria
- ACCOUNTABILITY
- Organization-wide FRAMEWORK
- Individual decision-maker Risk Management PROCESS

- Design, implementation, monitor and review, KPI, documentation, CONTINUOUS IMPROVEMENT



ISO Overview
3 main clauses
plus terminology



ISO 31000 Framework for Risk Management

Terminology (Guide 73)

risk management-coordinated activities to direct and control an **organization** with regard to risk

risk management policy **external context** **internal context** **risk profile**
risk management framework **risk management plan** **risk appetite** **risk attitude**
risk owner **risk management audit** **exposure** **resilience**

risk – effect of uncertainty on objectives

event

consequence

likelihood

uncertainty

probability

frequency

level of risk

risk source

hazard

vulnerability

risk evaluation-process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable **(part of risk management process)**

risk criteria **risk tolerance** **risk aversion**
risk matrix **risk aggregation**

stakeholder those people and organizations who can affect, be affected by, or perceive themselves to be affected by a decision or activity

communication and consultation
risk perception **risk reporting**

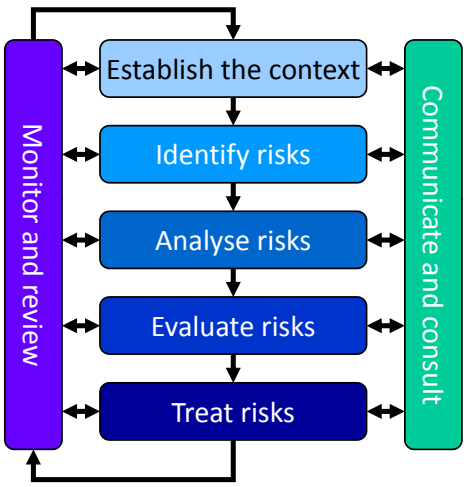
risk management process-systematic application of management policies, procedures and practices to the tasks of communicating, consultation, establishing the context, identifying, analysing, **evaluating, treating**, monitoring and reviewing risk

risk assessment **risk identification** **risk analysis** **monitoring** **review**
risk register

risk treatment–process of developing, selecting, and implementing measures to modify risk **(part of risk management process)**

control **risk sharing** **risk financing** **risk retention**
risk acceptance **risk avoidance** **residual risk** **risk mitigation**

The risk management process

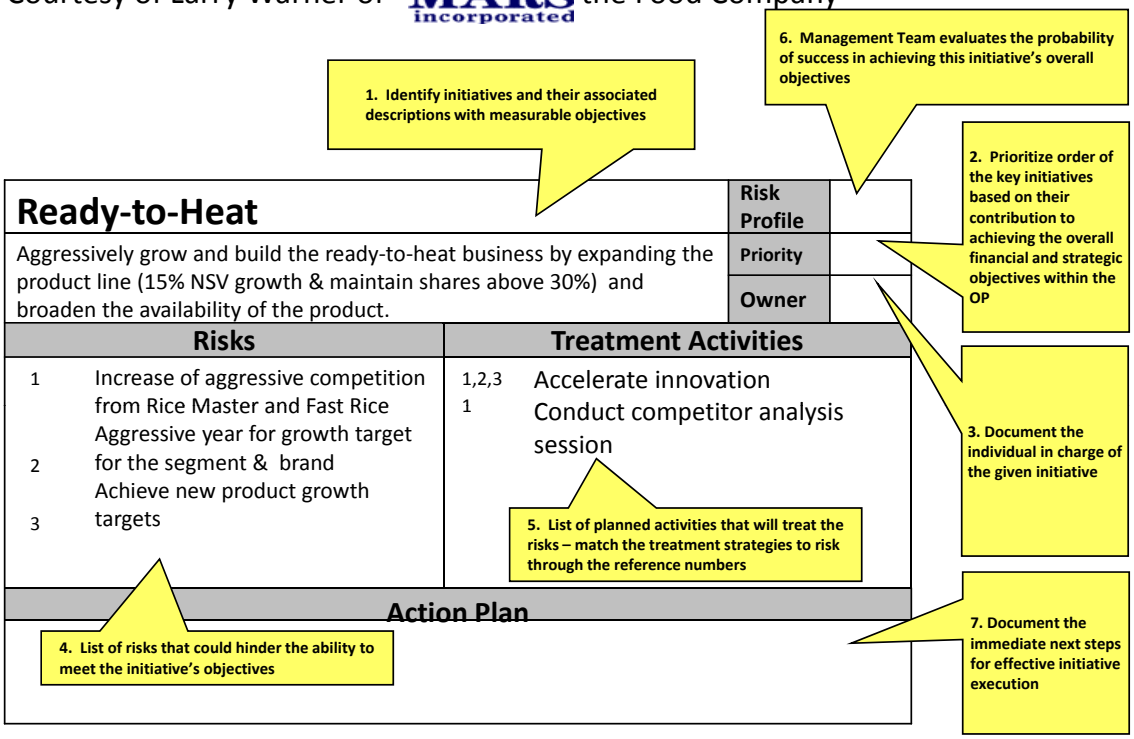


RM Information System
Risk Registers
Treatment Plan
Assurance Plan
Reporting templates

Advantages of 31000

- Strategic, operations, processes, projects, products, assets, governance, everything
- Proactively create value by treating uncertainty, while respecting regulations, laws, organization
- Expect better profits, moral, trust, controls, initiatives, reporting, and corporate culture
- Designed to integrate with existing management–
- Build on existing management systems, add commitment, alignment, IT, stakeholders, ownership of risk, etc.
- Communication and Consultation as appropriate – consider the values and perceptions of stakeholders
- Risk in every decision is set in context, assessed, treated, documented
- Review, review, and review, then act, act, act

Example risk register for a specific Objective – illustration only
Courtesy of Larry Warner of MARS incorporated the Food Company



MARS incorporated

Business units are required to review and update a dashboard on a quarterly basis which allows tracking of performance over time

Initiative	Risk Profile				Trend	Comments
	Q3 '05	Q4 '05	Q1 '06	Q2 '06		
Re-launch of Pedigree Effectively execute the re-launch of Pedigree to achieve the growth targets (10%)	Yellow	Green			Improving	Shipments started in P2 to meet advertising schedule. Advertising on air (P2W3). Massive presentation to all customers was executed during P1 with excellent customer participation.
Direct-to-store (DTS) Increase DTS operations by 10% and add 500 points of sale per cell	Green	Green			Stable	DTS operation is improving however there are still some areas that need to improve further. We will expand when we have a holistic strategy.
Associate engagement Increase associate engagement score from 85% to 90% within the factory	Blue	Green			Improving	Shift managers have been provided associate engagement training. All managers have held meetings with their team members.
Bring Pet Dry plant online Make the Dry plant fully operational by P13	Red	Blue			Stable	On track, construction permit granted. Plant will be ready by P13
Launch of Dove Successfully launch Dove into the mass market and achieve 65% distribution	Blue	Yellow			Stable	Increased risk due to current demand exceeding supply. We have re-phased the roll-out for the mass market to ensure current supply is adequate.

Let's check
what ISO 31000 is, and
what it expects of an organization

then

Discussion, Comments, Questions and useful arguments

Broadleaf

INSTITUTE FOR RISK RESEARCH

Broadleaf

Implementing Risk Management in 2008

9th April 2008

Implementing ISO 31000

…but how do you do it?

Grant Purdy

Associate Director, Broadleaf Capital International

Chair, Standards Australia and New Zealand Risk Management Committee

Nominated Expert - ISO WG on Risk Management

Broadleaf

IRR, Toronto 2008

Copyright

BROADLEAF CAPITAL INTERNATIONAL PTY LTD

ABN 24 054 021 117

23 Bettowynd Road Pymble NSW 2073

Tel: +61 2 9488 8477 Fax: +61 2 9488 9685

Cooper@Broadleaf.com.au

www.Broadleaf.com.au

Broadleaf

IRR, Toronto 2008

The Pivotal Definition

Risk

effect of uncertainty on objectives

NOTE 1 An effect may be positive, negative, or a deviation from the expected.

NOTE 2 An objective may be financial, related to health and safety, or defined in other terms.

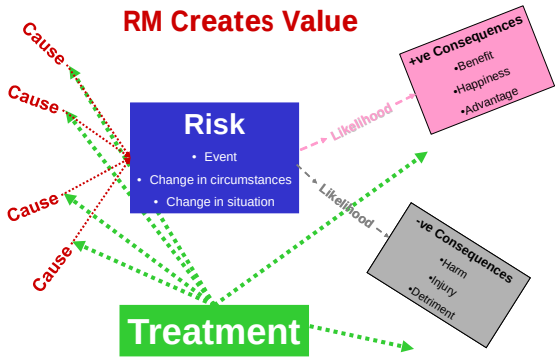
NOTE 3 Risk is often described by an event, a change in circumstances, a consequence, or a combination of these and how they may affect the achievement of objectives.

NOTE 4 Risk can be expressed in terms of a combination of the consequences of an event or a change in circumstances, and their likelihood.

Broadleaf

IRR, Toronto 2008

RM Creates Value



Broadleaf

IRR, Toronto 2008

Is this a car?

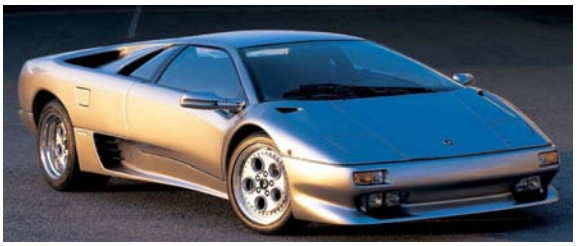
Broadleaf

IRR, Toronto 2008

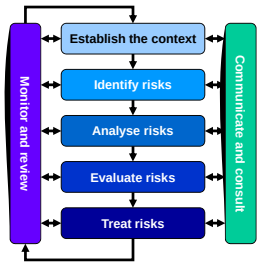
Spot the difference? Between this….

www.broadleaf.com.au

And this.....

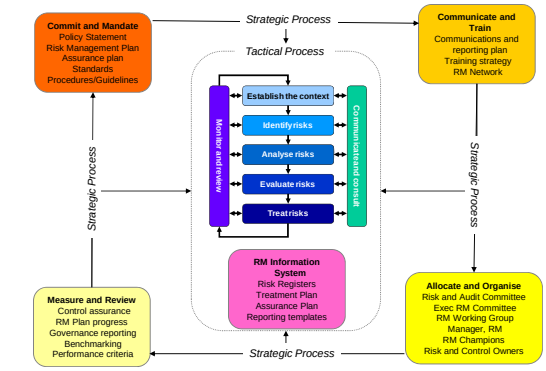


Risk Management Components - The risk management process

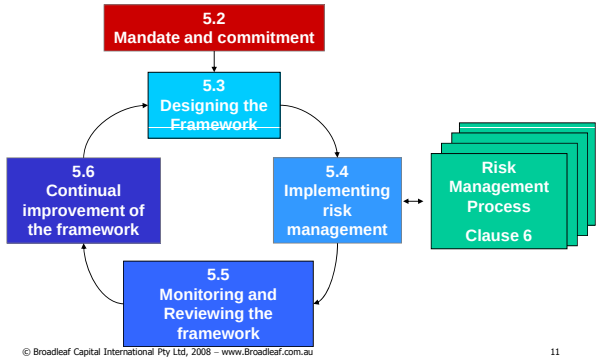


RM Information System
Risk Registers
Treatment Plan
Assurance Plan
Reporting templates

Risk Management Components - The (often missing) organisational context



ISO 31000 Framework for Risk Management



 11

Simple summary

"it aint what you do ...

Its the way that you do it"

Principles (Clause 4)

risk management should….

1. Create value
2. An integral part of organisational processes
3. Part of decision making
4. Explicitly address uncertainty
5. Be systematic and structured
6. Be based on the best available information
7. Be tailored
8. Take into account human factors
9. Be transparent and inclusive
10. Be dynamic, iterative and responsive to change
11. Be capable of continual improvement and enhancement

Annex A – Attributes of excellence in risk management

1. A pronounced emphasis on continuous improvement
2. Comprehensive, fully defined and fully accepted accountability for risks, controls and treatment tasks.
3. All decision making within the organization involves the explicit consideration of risks and the application of the risk management process to some appropriate degree.
4. Continual communications and highly visible, comprehensive and frequent reporting.
5. Risk management is always viewed as a core organizational process.

So how do you start? 1 - the "cunning plan"

1. Conduct a gap analysis – take stock
2. Set a realistic timetable (years)
3. Get a budget
4. Get some help
5. Bleed in the processes (one a year?)
6. Decide when you will be ready to roll (down)
7. Decide on the 'early adopters' with credibility and start with them
8. Decide on the 'blockers' and take them on later
9. Look out for opportunity to 'showcase'

So how do you start? - 2 - receiving the blessing

1. Get a sponsor (CEO/CFO/Co Sec)
2. Write a motivational policy statement and get the CEO to own it and sign
3. Tell the risk/audit committee or Board what you are doing and when you will report to them on progress
4. Set up a W/G with all departments involved – especially the 'difficult ones'
5. Get consultation going on Standards and Guidelines
6. Agree a timetable for engagement of each department/chunk
7. Get Champions nominated
8. Make friends with the Internal Auditors

So how do you start? - 3 - tricks of the trade

- Don't do a pilot study or call it an initiative
- Set 'Standards' and write Guidelines (not Policy and Procedures manuals!!)
- Don't outsource it
- Don't try to force people to do it – you need to make your case
- Don't ever do it for them – after the first time
- Don't start until you're ready
- Never agree to just do it "for reporting purposes"
- Don't over simplify (simple = yes, simplistic = no)
- Don't start at the bottom of the organisation

Roll down or Roll-up?

- Answer – both!
- You roll-down risk management, getting buy-in and ownership
- You roll-up risk profiles to produce consolidated profiles

The roll-down

1. "Engage" the management team at that level
   - Change their vocabulary and make your case
   - Get them to discuss what they perceive as the major risks – and compare across the team!
2. Facilitate a self-evaluation of their current approaches to risk management using a structured maturity evaluation
3. Facilitate a strategic risk assessment – what are those things that might prevent or enhance us achieving our strategic objectives

Risk Management Maturity Measurement System

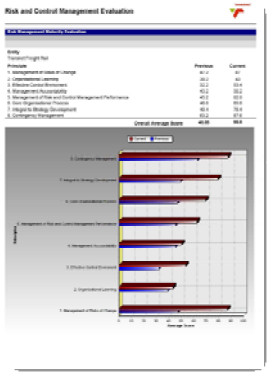
	"None"	"Very little"	"Some"	"Good"	"Complete"
Intent – total of 30%	Management do not recognise the need for the requirement.	Management support the intent for the requirement	Management agree with the intent for the requirement	Management completely subscribe to the intent of the requirement.	Management enthusiastically advocate the requirement.
	0	***3***	***7***	***15***	***30***
Practice – total of 70%	Very little or no compliance with the requirement in any way	Poor compliance with the requirement in practice	Patchy and limited compliance with the requirement	Partial compliance with the requirement in practice.	Absolute compliance with the requirement in practice – at all times and in all places.
	0	***8***	***17***	***35***	***70***

Evaluation Protocol - for example

#	Principle	#	Requirement	Guidance on evaluation
	Management of the Risks of Change			
1	All risks created by both internal and external changes and events are effectively and efficiently managed.	1.1	The Business has and uses a documented system or approach for the management of changes.	Normally this would be a change management system or procedure. The form of risk assessment should be specified within it. The changes covered will be all those which we propose to undertake internally together with those changes which might occur externally which would be significant for our business.
		1.2	A risk assessment that considers all types of risk is conducted whenever an internally created change occurs or is planned.	This means a properly conducted systematic risk assessment with the rigour of the assessment in keeping with the severity of the potential consequences. The risk assessment covers all types of risks and is not, for example, just for Health and Safety risks.
		1.3	Risk assessments that consider all types of risk are conducted whenever significant external changes and events are detected.	Normally, the risk assessments would cover all types of risks. Just a risk assessment that deals with health safety risks is not adequate.
		1.4	Risk Assessments that consider all types of risks are conducted every time an important or critical process or procedure is changed.	Normally, the risk assessments would cover all types of risks. Just a risk assessment that deals with health and safety risks is not adequate. This may include Procedural HAZOP or the use of detailed techniques in keeping with the process concerned. For example, if the change is to a work instruction.
		1.5	Risk Assessments that consider all types of risk are conducted every time before a structural or organisational change occurs.	Organisational changes may involve just one or a small number of people (for example the restructure of a department) or may affect the whole Business (for example a re-structure). This may include Organisational HAZOP.

Maturity evaluation

- Compare the current year to the past – 'footprinting'
- Generate a numerical score that links to KPIs and performance management
- Link to insurance premium distribution and create an incentive
- Validate through Internal Audit – it gives them a protocol to follow
- Refocus on what matters for yoru organisation
- Raise the bar after a few years



The RMIS manages the outputs

Baseline Risk Assessment

Risk Register
- Risks
- Causes
- Controls
- Risk ratings etc.
- Risk owners
- Control owners

Risk Treatment Plan
- Tasks
- Task owners
- Timelines
- Budgets?

Maturity Evaluation

Risk Management Plan
- Tasks
  - for embedding
  - for rolling out further
  - Training
  - Special risk treatment (eg BCP)
  - Measurement
  - KPIs
- Task owners
- Timelines

Conclusions

1. ISO 31000 Risk Management is not just about risk assessment for reporting
2. It is a continuous process that 'infects' an organisation
3. It will not happen by accident
4. It should be carefully planned, managed and resourced
5. The benefits (in time) are remarkable and valuable

www.broadleaf.com.au

Uncertainty is the human paradox:

we fear it, but we need it!

Contact details

For more information about the material discussed here, please contact:

Dr Dale F Cooper	Cooper@Broadleaf.com.au
Grant Purdy	Purdy@Broadleaf.com.au
Dr Stephen Grey	Grey@Broadleaf.com.au
Geoff Raymond	Raymond@Broadleaf.com.au
Mike Wood	Wood@Broadleaf.co.nz
Phil Walker	Walker@Broadleaf.com.au

Visit our web site: www.Broadleaf.com.au

BROADLEAF CAPITAL INTERNATIONAL PTY LTD

ABN 24 054 021 117

23 Bettowynd Road
Pymble
NSW 2073
Australia

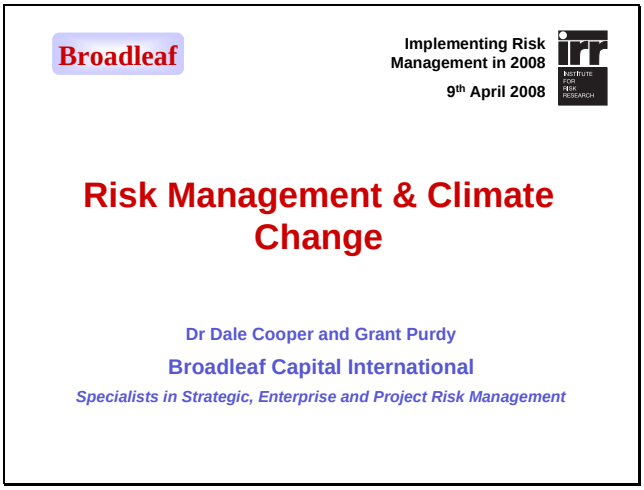
Tel: +61 2 9488 8477
Mobile: +61 4 1943 3184
Fax: + 61 2 9488 9685
www.Broadleaf.com.au
Cooper@Broadleaf.com.au

Specialists in Strategic, Enterprise and Project Risk Management

RISK MANAGEMENT AND CLIMATE CHANGE

Dr Dale F Cooper, Director, Broadleaf Capital International

Supporting material for a paper presented at an Executive Workshop organised by the Institute for Risk Research at the University of Waterloo, PricewaterhouseCoopers LLP and Broadleaf Capital International, Toronto, Canada, 9 May 2008



The Intergovernmental Panel on Climate Change (IPCC), the most authoritative analysis of information on climate change, has concluded that:

- Global temperatures increased by 0.7^{o} C in the 20th century (a further 0.15^{o} C since turn of century).
- 1990-1999 was the warmest decade in the last 1000 years
- Most of the warming in the last 50 years is attributable to human activities
- Climate change will continue for decades or even centuries to come even if large scale action to reduce emissions is taken in the near future.
- A recent report for the Lowy Institute by Dr Alan Dupont (international security analyst) and Dr Graeme Pearman (former Chief of CSIRO atmospheric research) argues that climate change represents a major security threat globally and to Australia and that far from exaggerating the threat of climate change scientists may have understated it.

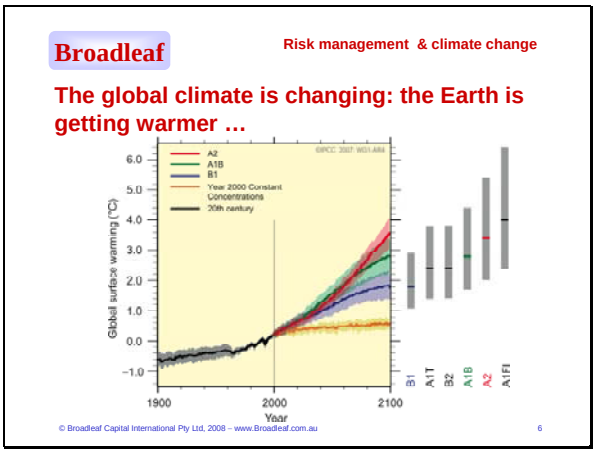
1 The climate is changing, and will continue to change

Climate change will have big impacts on Canada, particularly in Arctic and littoral areas.

1.1 Temperatures are increasing

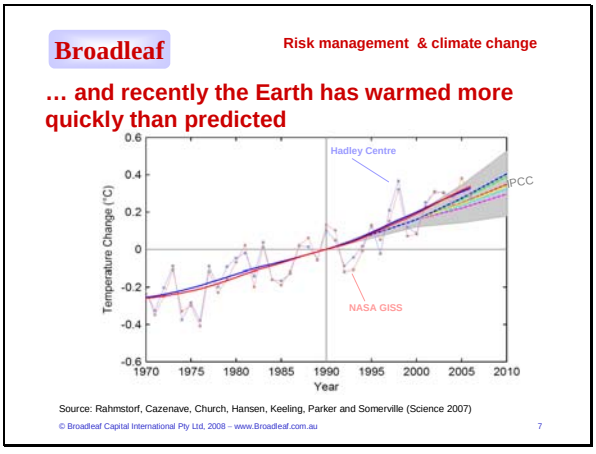
The big picture:

- The global climate is changing: the Earth is getting warmer
- Recently the Earth has warmed more quickly than predicted
- Canada seems to be getting warmer
- Winter temperatures have risen
- Permafrost temperature records show substantial recent warming
- Temperatures across Canada are forecast to increase substantially



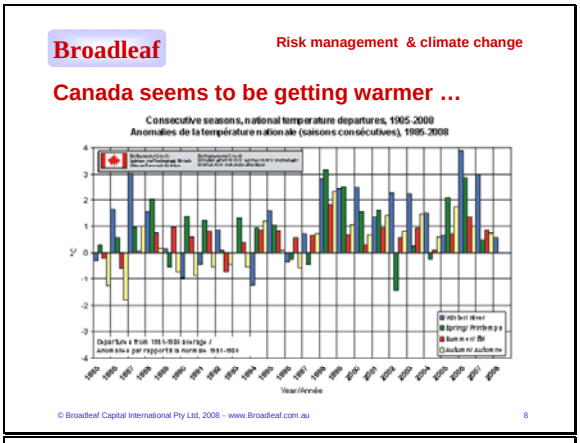
http://www.ipcc.ch/graphics/graphics/ar4-wg1/ppt/spm.ppt#263,6,Figure SPM.5

Figure SPM.5. Solid lines are multi-model global averages of surface warming (relative to 1980–1999) for the scenarios A2, A1B and B1, shown as continuations of the 20th century simulations. Shading denotes the ±1 standard deviation range of individual model annual averages. The orange line is for the experiment where concentrations were held constant at year 2000 values. The grey bars at right indicate the best estimate (solid line within each bar) and the **likely** range assessed for the six SRES marker scenarios. The assessment of the best estimate and **likely** ranges in the grey bars includes the AOGCMs in the left part of the figure, as well as results from a hierarchy of independent models and observational constraints. {Figures 10.4 and 10.29}

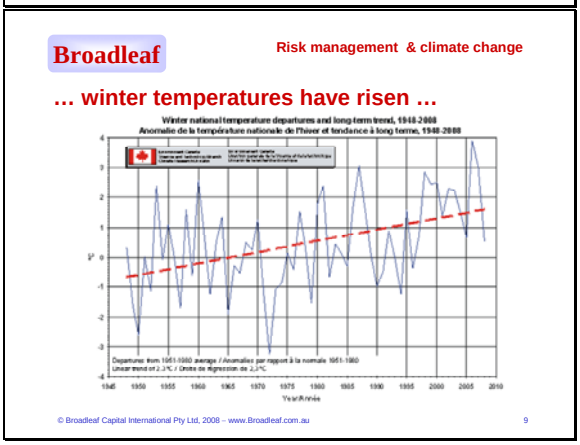


Source: Stefan Rahmstorf, Amy Cazanave, John A Church, James E Hansen, Ralph F Keeling, David E Parker and Richard CJ Somerville, 'Recent Cliamte Projections Compared to Projections', Science, Vol 316, 4 May 2007, p 709.
http://www.pik-potsdam.de/~stefan/Publications/Nature/rahmstorf_etal_science_2007.pdf

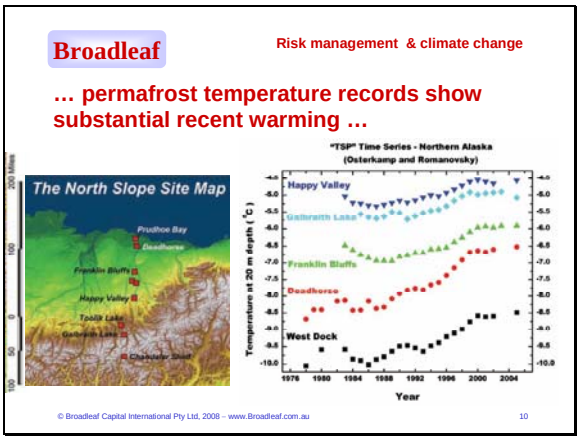
"Given the relatively short 16-year time period considered, it will be difficult to establish the reasons for this relatively rapid warming, although there are only a few likely possibilities. The first candidate reason is intrinsic variability within the climate system. A second candidate is climate forcings other than CO2: Although the concentration of other greenhouse gases has risen more slowly than assumed in the IPCC scenarios, an aerosol cooling smaller than expected is a possible cause of the extra warming. A third candidate is an underestimation of the climate sensitivity to CO2 (i.e., model error). The dashed scenarios shown are for a medium climate sensitivity of 3°C for a doubling of CO2 concentration, whereas the gray band surrounding the scenarios shows the effect of uncertainty in climate sensitivity spanning a range from 1.7° to 4.2°C."



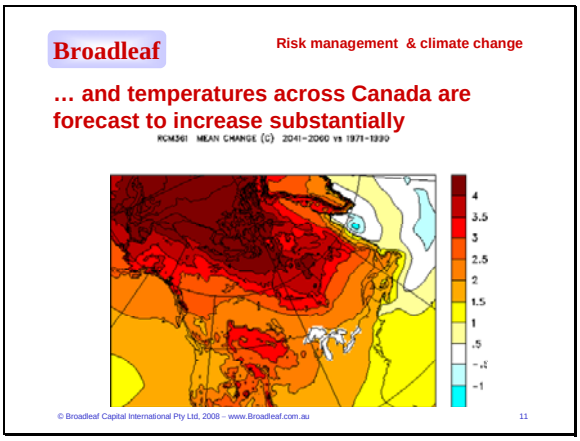
With the exception of the springs of 2002 and 2004, seasonal temperatures have remained above or near normal for almost 11 years, as shown in the consecutive seasons graph.
http://www.msc-smc.ec.gc.ca/ccrm/bulletin/national_e.cfm
http://www.msc-smc.ec.gc.ca/ccrm/bulletin/figseasont_e.html?season=Winter&date=2008



The graph shows that winter temperatures have generally been increasing nationally, with temperatures remaining above normal since 1997. The red dashed line represents a warming trend of 2.3°C over the last 61 years.
http://www.msc-smc.ec.gc.ca/ccrm/bulletin/national_e.cfm
http://www.msc-smc.ec.gc.ca/ccrm/bulletin/figchartt_e.html?season=Winter&date=2008



State of the Arctic, October 2006
Figure 22: Top: Locations of long-term University of Alaska permafrost observatories in northern Alaska. Bottom: Changes in permafrost temperatures at a depth of 20 m over the last 20-25 years. (Updated from Osterkamp, 2003.)
http://www.pmel.noaa.gov/pubs/PDF/rich2952/rich2952.pdf

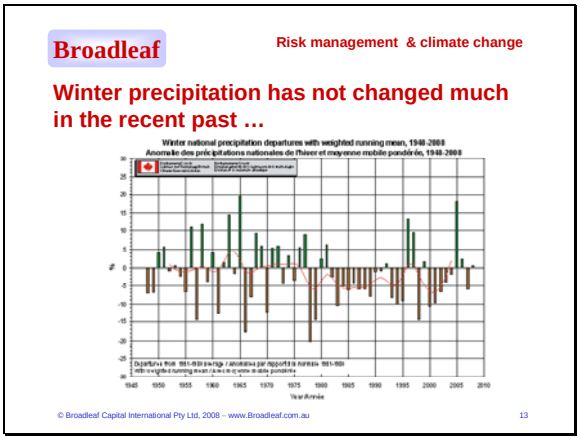


Diagnostic Plots from CRCM3.6
Change in annual mean screen (2m) temperature (°C) in 2041-2060 relative to 1971-1990 simulated by CRCM3.6.1
http://www.cccma.ec.gc.ca/diagnostics/crcm36/crcm36_st_ano.shtml

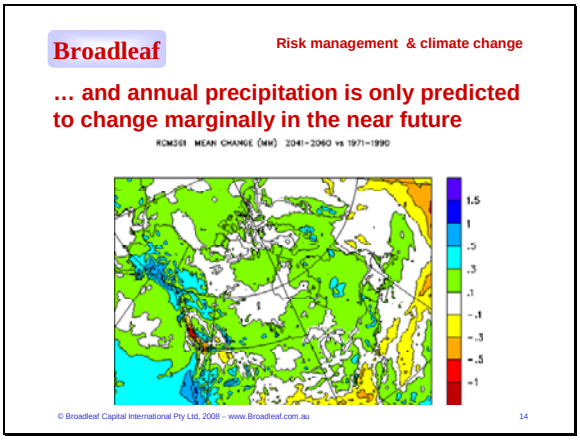
1.2 Precipitation across Canada may not change much in the short term

The big picture:

– Winter precipitation has not changed much in the recent past
– Annual precipitation is only predicted to change marginally in the near future



The graph shows most winters over the last 25 years have had precipitation levels near or below normal.
http://www.msc-smc.ec.gc.ca/ccrm/bulletin/national_e.cfm
http://www.msc-smc.ec.gc.ca/ccrm/bulletin/figchartp_e.html?season=Winter&date=2008



Diagnostic Plots from CRCM3.6 Change in annual mean precipitation rate (mm/day) in 2041-2060 relative to 1971-1990 simulated by CRCM3.6.1
http://www.cccma.ec.gc.ca/diagnostics/crcm36/crcm36_pcp_ano.shtml

1.3 The maritime environment is changing

The big picture:

- There is less sea ice around Canada
- Arctic sea ice is predicted to become thinner
- Its extent is predicted to decline substantially
- Sea levels have risen faster than predicted
- Arctic sea levels are rising
- Rising sea levels, combined with storm surges, will lead to problems in the coastal zone

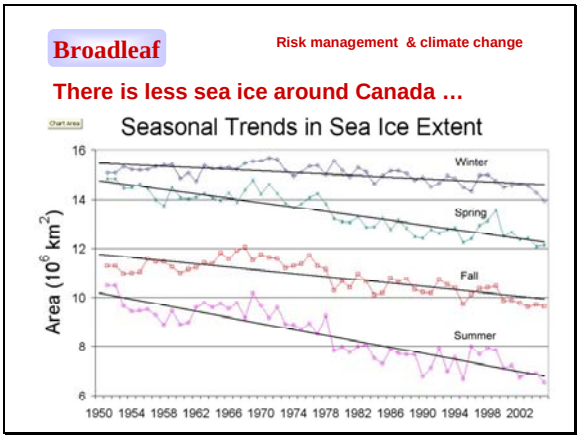
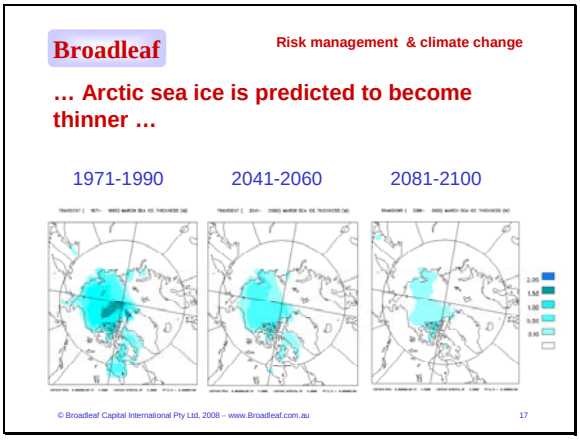
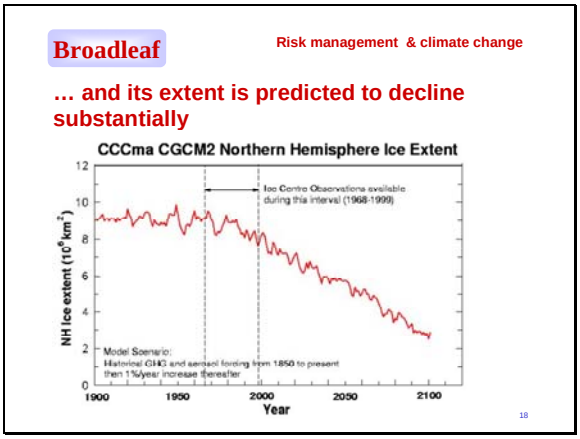


Figure 2: Monthly change in sea ice extent from 1979-1996 as compared to normal for the same period. http://www.socc.ca/seaice/seaice_hist_e.cfm



http://www.socc.ca/seaice/seaice_future_e.cfm

Figure 1: Arctic sea-ice thickness (m) obtained from the CCCma Coupled Global Climate Model for March, averaged over years 1971-1990.
Figure 2: Arctic sea-ice thickness (m) obtained from the CCCma Coupled Global Climate Model for March, averaged over years 2041-2060.
Figure 3: Arctic sea-ice thickness (m) obtained from the CCCma Coupled Global Climate Model for March, averaged over years 2081-2100.
The oceanic and sea-ice components of GCMII are highly simplified. An ocean mixed-layer model is used together with an embedded thermodynamic sea-ice model. The oceanic component is simply a 50 m thick slab of quiescent seawater. Ice is allowed to form at the top of the water slab when it cools down to the freezing point of seawater.

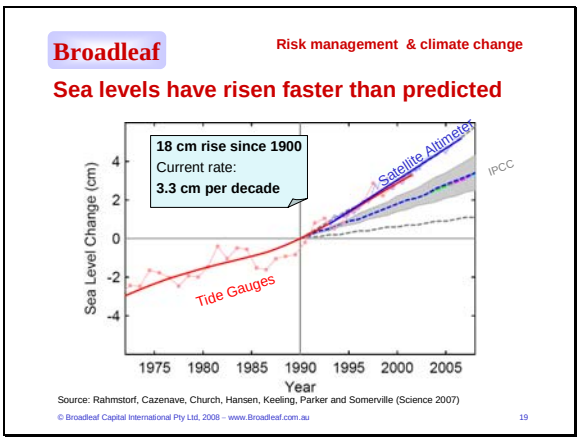


http://www.socc.ca/seaice/seaice_future_e.cfm

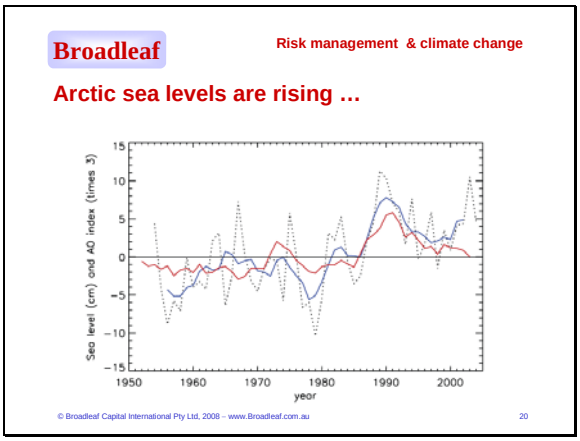
Figure 1: CCCma prediction of sea ice extent during the 21st century.

Figure 1 shows the sea ice extent for the Northern Hemisphere starting in 1900 to 2100. Sea ice extent begins to decrease around the time of the sea ice chart observational record from 1968 to 1999. The decrease is close to the observed decrease of 3% per decade seen in the observational record. Ice extent starts to decrease slightly more rapidly after 2000. By about 2050, summer sea ice cover over the Arctic Ocean has disappeared.

Note that these results are obtained from one particular model using one particular scenario for future greenhouse gas and aerosol forcing. They are provided here as an example of projected changes in the cryosphere which might accompany changing climate.

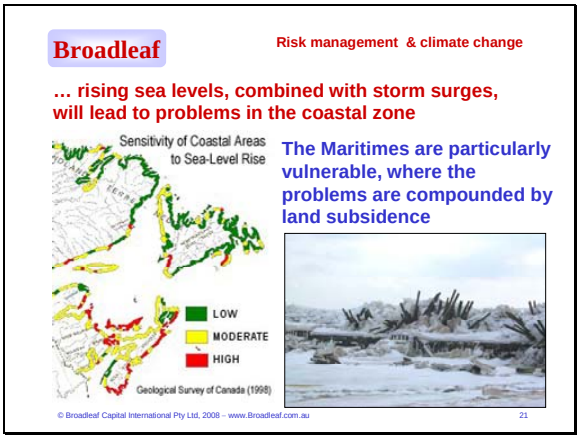


Source: Stefan Rahmstorf, Amy Cazanave, John A Church, James E Hansen, Ralph F Keeling, David E Parker and Richard CJ Somerville, 'Recent Cliamte Projections Compared to Projections', Science, Vol 316, 4 May 2007, p 709.
http://www.pik-potsdam.de/~stefan/Publications/Nature/rahmstorf_etal_science_2007.pdf



State of the Arctic, October 2006

Figure 13: Annual mean relative sea level from nine tide gauge stations in the Siberian seas (dotted line). The blue line is the 5-year running mean sea level. The red line is the 5-year running mean Arctic Oscillation index.
http://www.pmel.noaa.gov/pubs/PDF/rich2952/rich2952.pdf



http://atlantic-web1.ns.ec.gc.ca/slr/default.asp?lang=En&n=61BB75EF-1

Sea-Level Rise

Storm-surge flooding and coastal erosion are problems that are with us today. According to the Geological Survey of Canada, parts of the Gulf of St. Lawrence are some of the most vulnerable areas in Canada to sea-level rise.

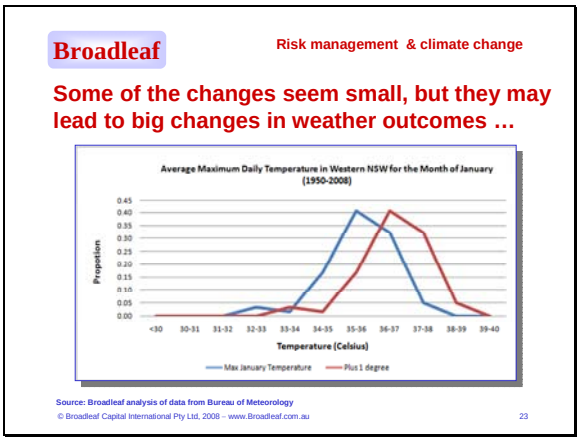
In addition to sea-level rise caused by climate change, land is subsiding in the Maritimes by about 20 cm per century.

In winter, sea ice can protect the shoreline from the impacts of ocean waves, but it can also become a hazard under extreme storm surge conditions—as evidenced by the devastating damage done to the Cap-des-Caissie wharf in January 2000

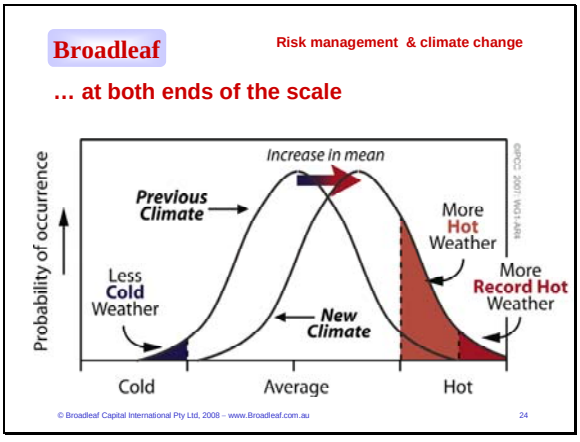
1.4 Small changes in averages can have highly non-linear effects

The big picture:

- Some of the changes in climate seem small, but they may lead to big changes in weather outcomes
- Small changes in weather outcomes can lead to large changes in operational impacts

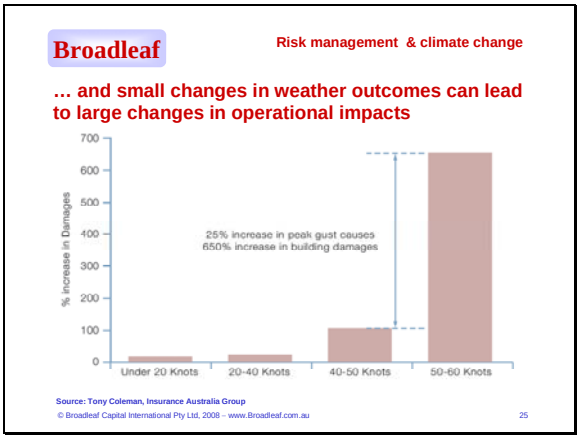


Source: Broadleaf analysis of data from the Australian Bureau of Meteorology, www.BoM.gov.au



IPCC 2007: Box TS.5, Figure 1. Schematic showing the effect on extreme temperatures when the mean temperature increases, for a normal temperature distribution.

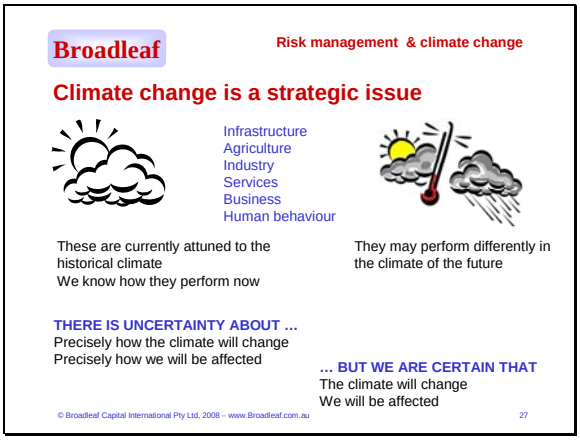
http://www.ipcc.ch/graphics/graphics/ar4-wg1/ppt/technical-summary.ppt#295,35,Box TS.5

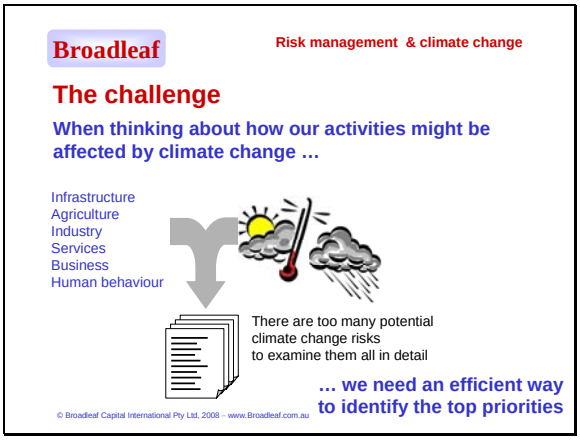


Insurance Australia Group: building claims versus peak wind gust speeds, showing disproportionate increase in claims cost from small increases in peak wind gust speed – that is, a 25% increase in peak gusts causes 650% increase in building damages.
Source: Quoted in CSIRO Climate Change, An Australian Guide to the Science and Potential Impacts

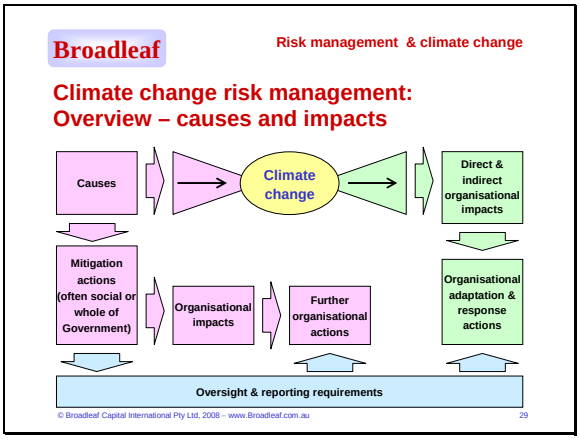
2 Climate change is a strategic issue

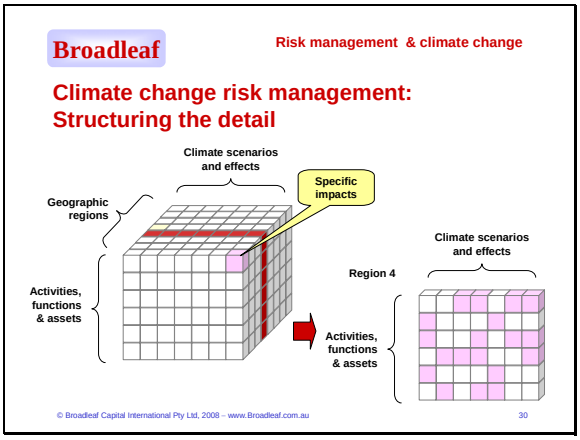
We need effective ways of thinking about climate change and its effects, and of integrating climate change management into our strategic plans

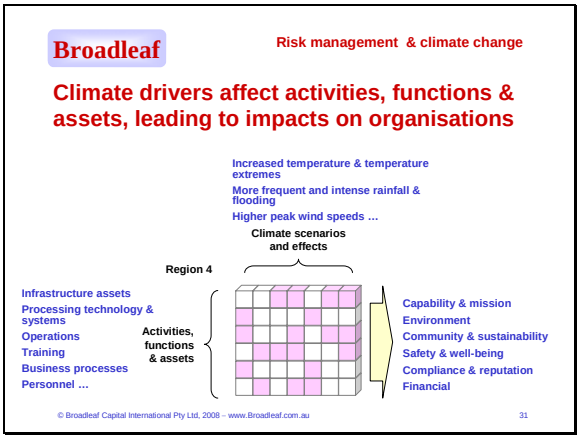


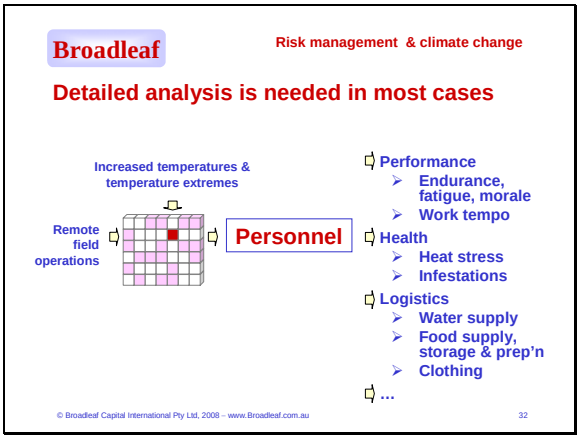


2.1 We must structure our thinking, and get into the detail

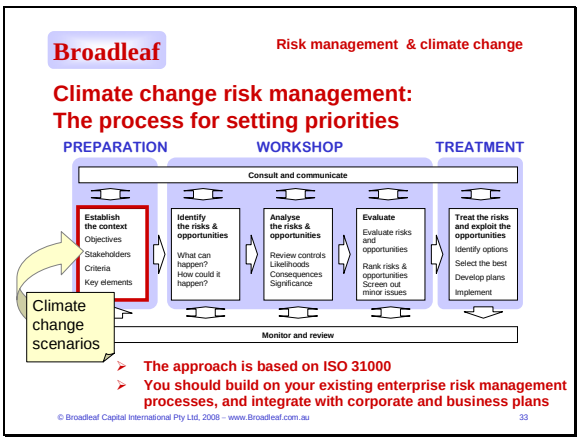






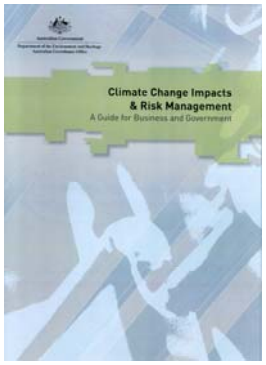


2.2 We must set priorities consistently



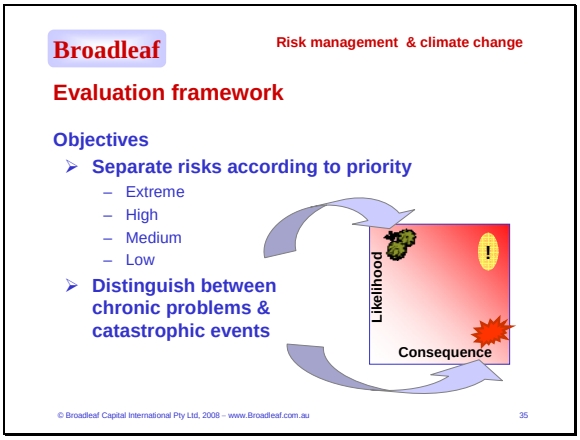
This presentation does not spend much time on the basics of the risk management process – it focuses on how it can be applied to the impacts of climate change.

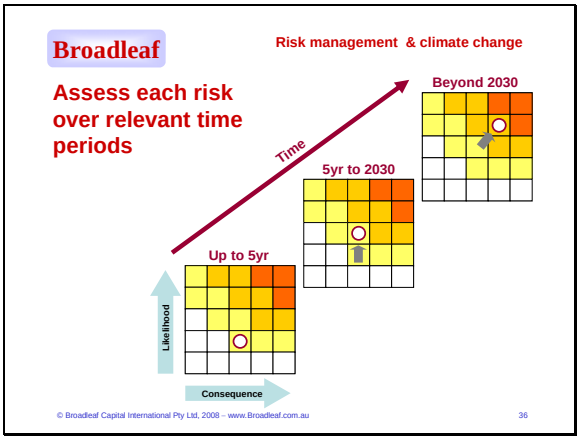
One important point should be noted: the process identifies risks and opportunities. Although many of the impacts of climate change will be negative, some of them will be positive, and it is important to recognise such opportunities and understand how they might be exploited. (For example, the effects of warmer temperatures and higher concentrations of CO_2 may be beneficial in some agricultural areas.)

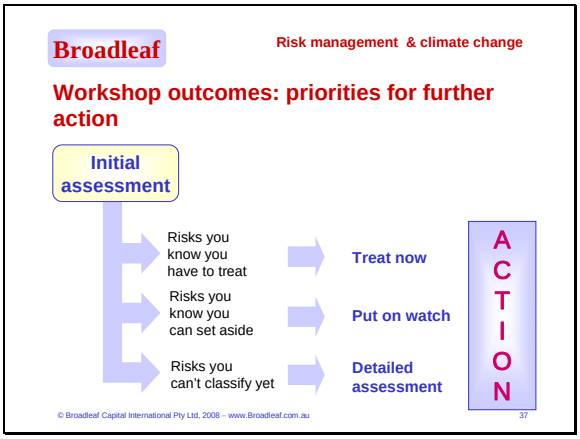


The process is described in detail in 'Climate Change Impacts and Risk Management: A Guide for Business and Government', published by the Australian Greenhouse Office. It is available from http://www.broadleaf.com.au/climate/index.html or http://www.greenhouse.gov.au/impacts/publications/risk-management.html

The guide was co-authored by Broadleaf and tested through a series of case studies – a large private company, a public utility, a State government agency and a local government authority – and we have undertaken many subsequent applications.



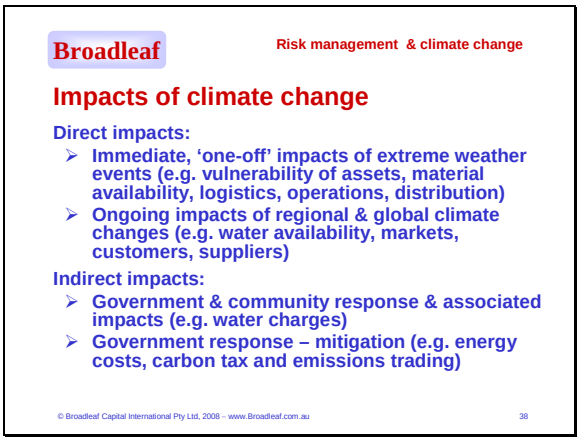




The outcome from the workshop is a triage of the risks and opportunities that have been identified:

- Risks that require action now.
- Those that can be set aside, either because they are genuinely low risks, or because action may not be needed immediately or urgently. Note that these risks are not discarded – they are set aside on a watch list to be reviewed regularly, to determine whether the priority has changed or whether the triggers for more immediate action have arisen.
- Those, risks, generally not many of them, for which we need more information and more detailed assessment before we can make a decision about the need for immediate action.

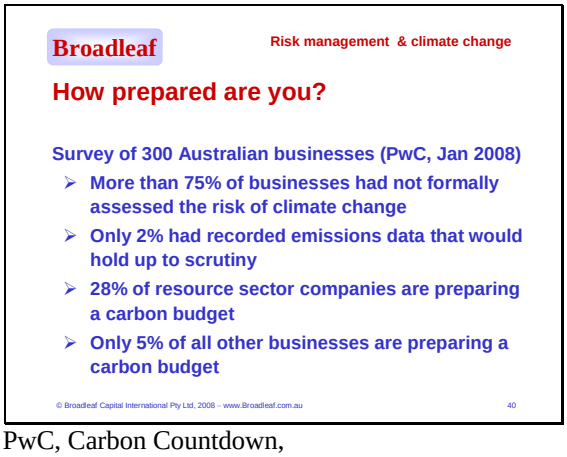
3 Summary and conclusions



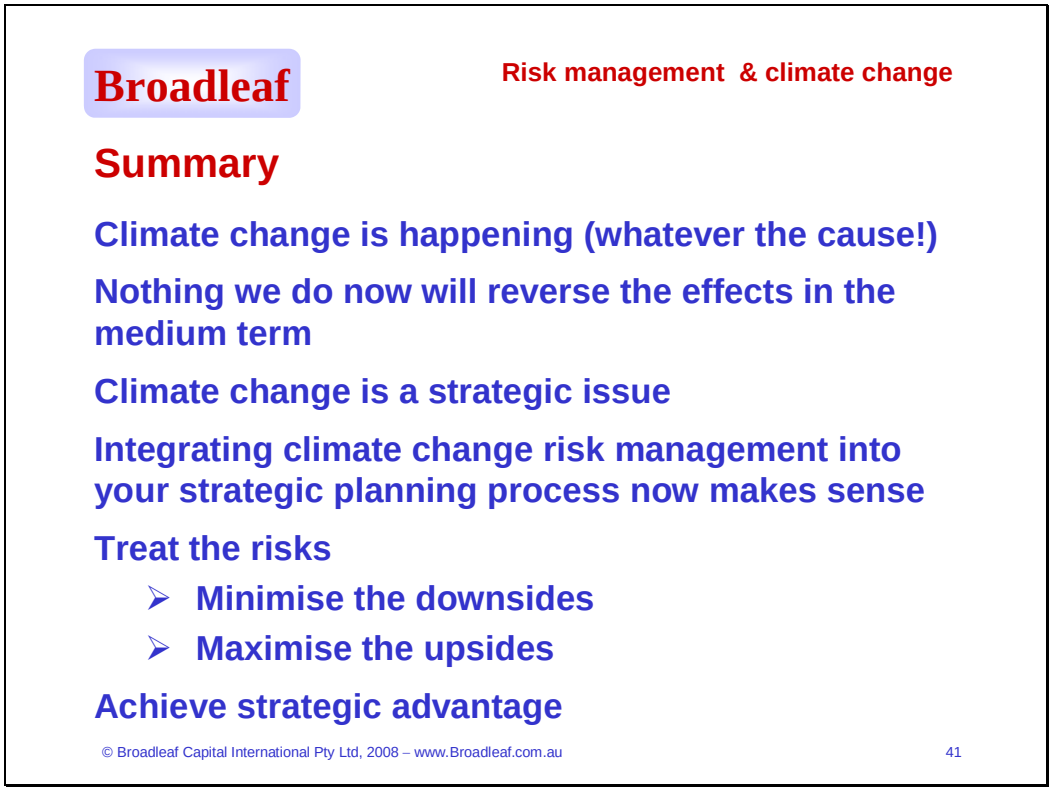
The direct and indirect effects of climate change are likely to generate both risks and opportunities for companies.

Importantly, even if you don't accept the current science of human-induced climate change it is important that you take a strategic approach to the issue. For example:

- considering the risks posed by natural climate variability
- considering the risks (and opportunities) posed by government, community and competitor response to the issue.



PwC, Carbon Countdown, http://www.pwc.com/Extweb/onlineforms.nsf/docid/0EDACFFBA83712AB852573DB000F55FF#



4 Contact us for more information

See the climate change risk pages on our web site: www.broadleaf.com.au/climate/index.html

Implementing Risk Management in 2008: Current Canadian Status of Implementing Risk Management

Matthew Hilbert
Principal

Enterprise Risk Management &
Operational Intelligence Solutions

Risk Consulting

Why Enterprise Risk Management?

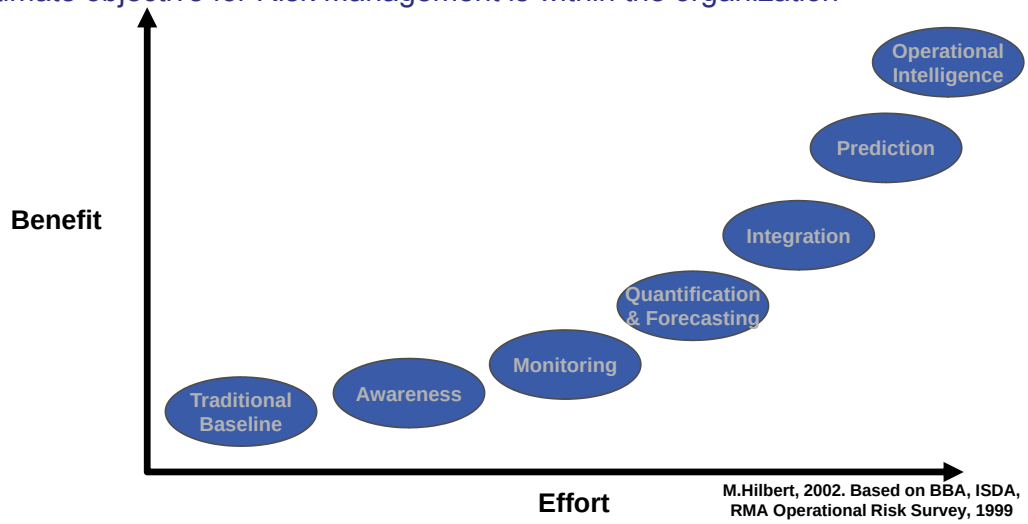
The market place will ultimately drive Enterprise Risk Management forward.

Enterprise Risk Management Drivers

- **Stakeholders, Rating Agencies & Regulators:**
  - Areas where there is a high degree of public exposure/liability
  - financial Institutions (OSFI, CDIC, etc), environmental legislation, etc
- **High Profile Failures & Disasters**
  - Barings, Enron, 9/11 & the WTC
  - Increased Reputational exposures (eg. Andersen)
- **Market Disclosure Requirements:**
  - Increasing pressure for disclosures from investors and analysts
  - Pressure from counter-parties – Climate Change/Carbon Emissions
- **Competitive Pressure & Improved Financial Performance:**
  - Reduce earnings volatility
  - Increase process effectiveness & efficiency

Organization should consider risk management as a spectrum. In deciding what level of maturity is appropriate they must consider a number of factors and the benefits increasing efforts will provide to the organization

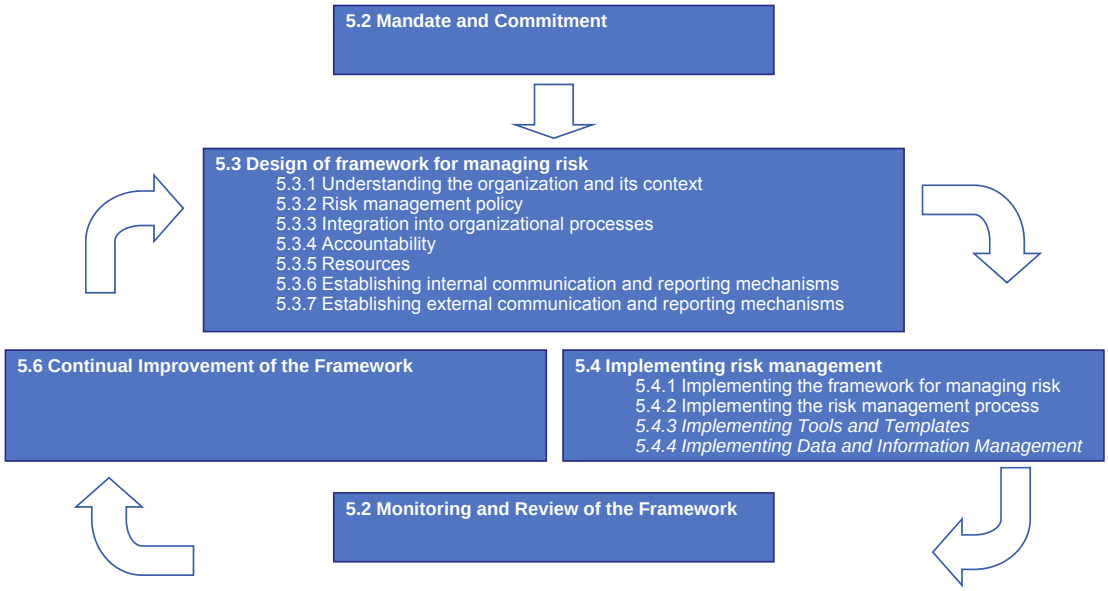
Risk Managers with senior management, including the board, must decide what the ultimate objective for Risk Management is within the organization



The Risk Management Maturity Model

Traditional Baseline	Awareness	Monitoring	Quantification & Forecasting	Integration	Prediction	Operational Intelligence
▪Reliance on Internal Audit ▪Individual Mitigation Plans ▪Reliance on "good" people/staff to make sure things are managed ▪Internal Controls	▪A risk governance structure is in place ▪The organization has some definitions in place ▪Risk management is re-enforced in policies and procedures	▪A clear vision for ERM exists ▪A balanced set of approaches are used (RCSA, event data, KRIs, etc) ▪Dedicated staff exist to support risk management at all levels	▪ Risk is considered on a quantitative basis and risks forecasts are used to understand exposures ▪Quantitative targets and measures are used	▪Linked risk management processes across the firm ▪Losses and indicators are correlated ▪Integration with quality programs ▪Risk assessment processes are integrated ▪Integration inside and outside the firm	▪Exposures and risks can de predicted based on operational metrics ▪Event data captures both magnitude and frequency values ▪Risk predictions drive process modification	▪The use of ERM to realize business opportunity ▪Risk Management is integrated with financial management performance management and operational effectiveness ▪ERM is link with CRM and other major processes

Achieving effective Risk Management requires alignment across a number of dimensions inside and outside the organization



Pulling together the elements of a risk management framework can be a complicated undertaking.

M Hilbert 2008 Based on ISO 3100 Components of the Framework for Managing Risk, (ISO 2008)
Items 5.4.3 and 5.4.4. are not included in ISO 31000

Leading organizations are beginning to take a holistic approach to risk management to promote consistency of risk management across the enterprise. An holistic approach leads to better alignment of risk management processes and fewer surprises

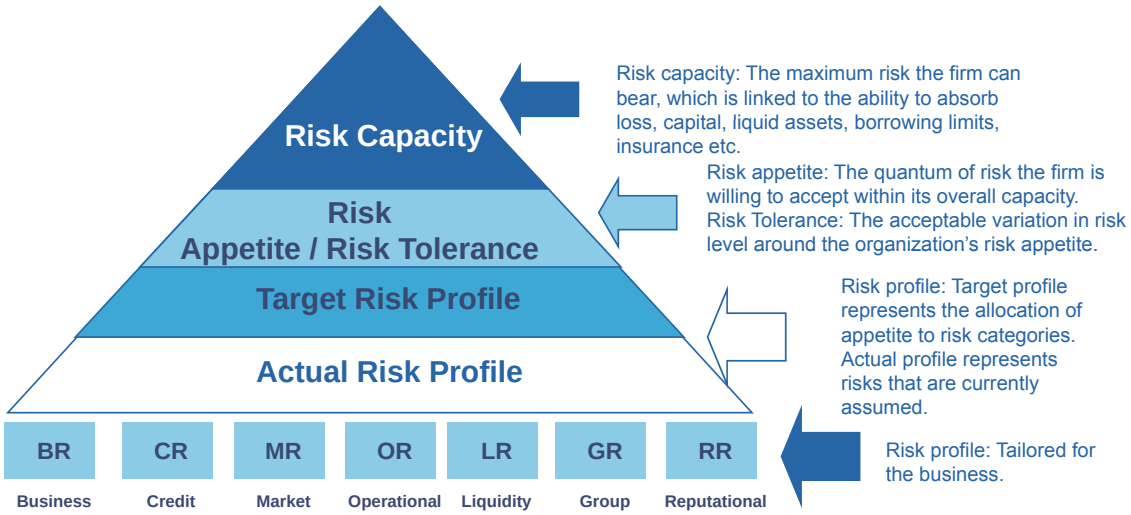
- **Characteristics of Holistic Risk Management**
- **Comprehensive** - considers the full spectrum of risks the organization faces
- **Interconnected** - linkages between risks are considered and reflected in the management approach
- **Integrated with the business** - strategy setting, decision making, execution and monitoring
- **Forward-looking** - innovative mindset to contribute to strategic decision making, in addition to a perspective on historical trends and events
- **Multi-faceted** - all levers to manage risk – process, structure, metrics and culture - are utilized
- **Efficient** - no overlaps in risk management activity, cost effectiveness of activity
- **Collaborative** - line management own risk, close engagement between Risk and the business
- **Value focused** - both a protection and enhancement focus

Best practice is leading to the development of a common ERM framework which is pushed out to the responsibility for risk management to the lines of business but maintains a strong corporate function that ensures alignment, harmonization and exploits synergies.

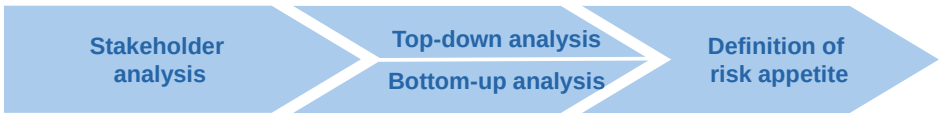
Leading Organizations understand developing a culture of risk awareness in the organization sets the tone and foundation for effect Risk Management

- The Risk Culture model (illustrated at right) identifies eight elements of the culture that have particular importance in a risk context. The model is built on:
  - The realization that an holistic approach to risk management is required, and a focus on controls and processes is not sufficient to drive the right behavior.
  - Values, objectives and practices across the organization must be aligned to achieve a culture of well-managed risk.
- The challenge for organizations is to establish a culture that:
  - Encourages individual accountability for managing risk (and therefore addresses accuracy of individual risk perception);
  - Includes systems to monitor and reinforce desired behaviors; and
  - Takes into consideration differences in the risk environment for different roles, and an individual tolerance for risk.

Leading organization are driving effective Risk Management through setting risk appetite and translating it into a target risk profile for the organization



The most effective firms understand that setting appetite requires that multiple dimensions are considered and integrated to determine a firm's risk appetite



An analysis of external and internal stakeholders and their expectations

A 'top-down' assessment of risk appetite, linked to strategic and business objectives

A 'bottom-up' assessment of the actual risk profile of the firm derived from the underlying business areas

Analysis to ensure that the actual risk profile reflects Board risk appetite, and to make adjustments where necessary

Regulators focus mainly on unexpected losses

Shareholders focus on maximising value in relation to risk

The amount of capital needed per unit of unexpected loss is dependent on the organizations risk appetite

Lead practices in setting risk appetite bring together measures across three dimensions to provide the organization guidance and direction.

Quantitative Measures	▪ Hard measures of risk ▪ Describe the type and quantum of risk the business wants and is willing to take ▪ Relate directly to business plans and risk measurement processes ▪ Example – appetite for earnings volatility
Qualitative Measures	▪ Recognize that not all risk is measurable but can affect business performance ▪ Example – appetite for business activities that are outside of core competencies
Zero Tolerance Risks	▪ A subset of the above which identifies the categories of risks to be avoided ▪ Example – appetite for regulatory mis-compliance

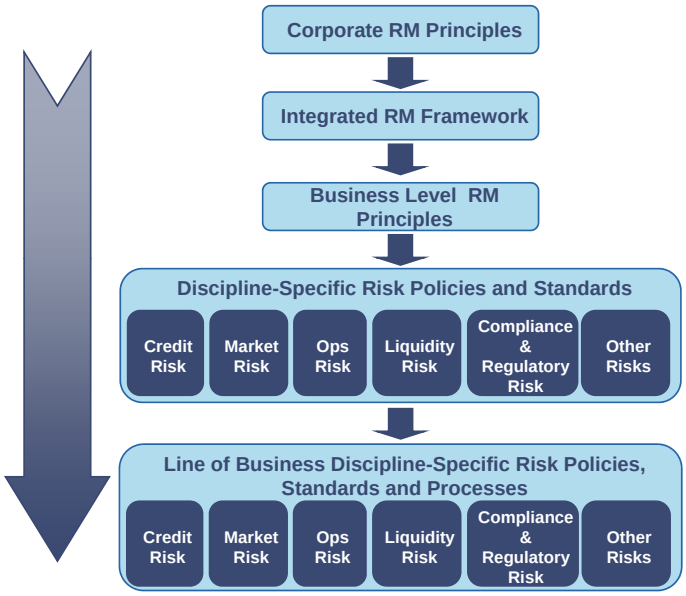
The practices for managing risk appetite are continuing to evolve as firms gain experience with risk management and as approaches take root in firms

- **Established Practices**
- Risk appetite is managed "bottom-up" to some extent - via ongoing monitoring and Senior Management involvement.
- The determination and/or management of risk appetite includes some form of consideration of: the firm's capacity to bear catastrophic losses; the firm's strategic objectives; the firm's relative competencies; the risk-reward trade-off; and the economic environment.
- A framework exists for all risks (including, increasingly, business/commercial type risks).
- Appetite is described in quantitative / absolute terms, and related to clear financial / strategic objectives (as opposed to 'medium'; 'conservative'; 'risk averse' etc.)

- **Emerging Practices**
- Much stronger and explicit link between the organizational objectives (more than maintaining a desired credit rating) and the specification of its risk appetite.
- Risk appetite is expressed at more than one confidence level and/or time horizon.
- Analysis of the risk-reward trade-off is becoming more sophisticated, recognizing that different forms of risk carry different costs (i.e. require different returns).
- Definition of risk appetite extended beyond tolerance (i.e. how much risk) to include which risks and why (i.e. what are the right/wrong risks, having regard for stakeholder expectations, view on credit cycle, relative competencies etc).

Leading firms are driving Risk Management through corporate principles, aligning the focus of Risk Management to objectives, outcomes and setting the expectation for how they will be achieved

Corporate RM principles are applied on an integrated basis consistently through the organization

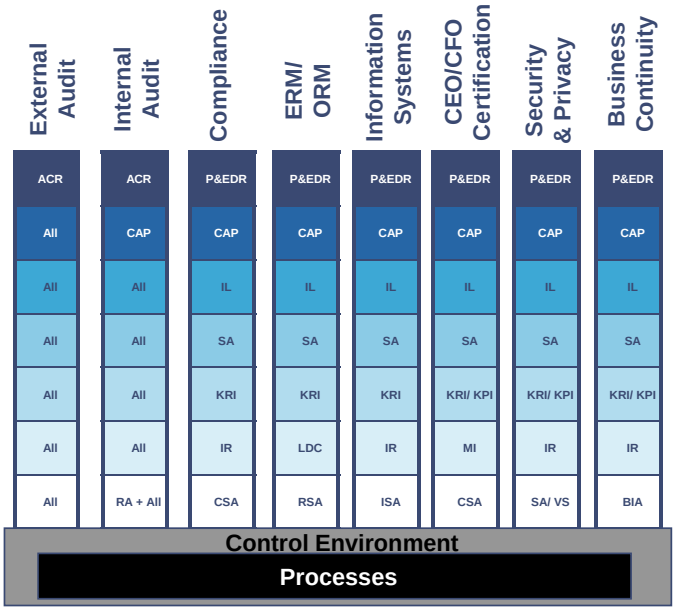


Anchoring risk management through corporate principles provides a framework for the consistent delivery of risk management across disciplines and lines of business.

In moving forward with an integrated approach to Enterprise Risk Management organizations typically have to deal with siloed, replicated and disconnected processes and systems

ACR	Audit Committee Report
All	Utilizes information from all groups
P&EDR	Periodic and Event Driven Reporting
CAP	Corrective Action Plan
IL	Issues Log
SA	Scenario Analysis
KRI	Key Risk Indicator
KRP	Key Performance Indicator
IR	Incident Report
LDC	Loss Data Collection
MI	Major Incident Report
RA	Risk Assessment
CSA	Control Self Assessment
RSA	Risk Self Assessment
ISA	Information Systems Assessment
SA/VS	Security Assessment/ Vulnerability Scan
BIA	Business Impact Assessment

Reporting
Adjustments
Issues
Scenarios
Indicators
Incidents
Assessment

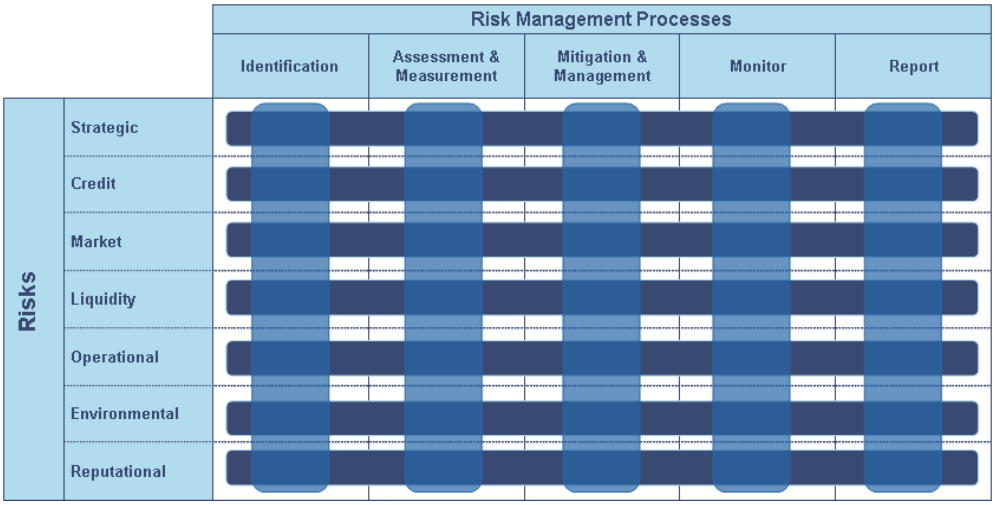


Current Challenges (large) organization

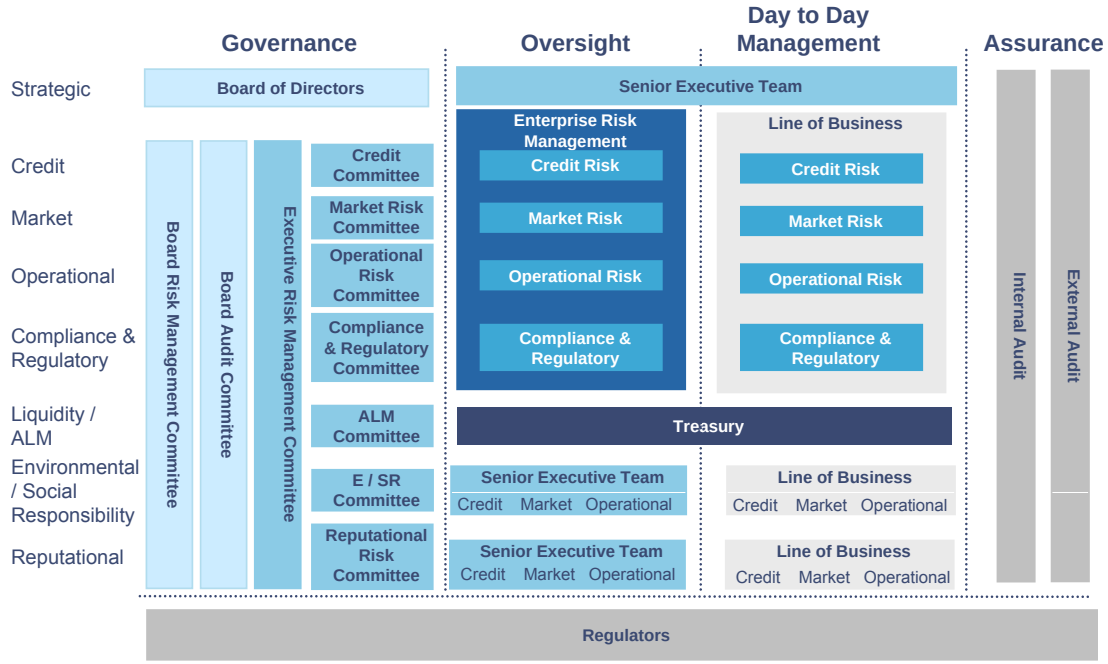
- Multiple initiatives
- No coordinating systems backbone
- Need for a common language
- Non-standard processes
- Lack of common/shared definitions
- Limited transparency
- Assessment fatigue
- Ad-hoc investments in technology
- Duplicate efforts
- Manual process using spreadsheets
- Roles and responsibilities unclear

The integration of Risk Management processes increases transparency and supports the simplification of the processes while improving the effectiveness of Risk Management

To provide a complete picture of risks across the enterprise, risk management processes need to be integrated across risk disciplines.



Effective ERM in today's increasing complex and connected business environment requires operational alignment as well



Managing risk is an integrated process that relies upon multiple groups within an organization

Within financial institutions the finance and risk management disciplines are now merging in a way that necessitates the integrated management of risk, return and growth

Finance

- CFOs are increasingly required to evaluate financial performance and strategic plans in the context of earnings sustainability and risk-based capital requirements.

Risk Management

- CROs are required not only to demonstrate loss avoidance benefits but also prove ERM strategic management applications by maximizing the risk-reward balance in all decision making.

Integrated Risk-Adjusted Performance Measures

Key Elements

- Integrated management approach of risk and performance towards capital optimization and value creation
- Analytics and data required to perform enterprise wide aggregation and integration of risk and return information
- Integrated risk and performance measurement forms an essential part of strategic planning and risk appetite definition processes
- Tactical applications such as pricing, investment allocations, product design and portfolio management can be leveraged.

Emerging Risk Management Organizational Practices

	Theme	Outcome
	Strengthen **risk management rigor** by engaging the business	Strong **senior management commitment**, Risk management becomes **embedded in the business** and the tone at the top pervades the organization
	Clarity of roles, responsibilities, rewards and consequences (board, business lines, risk management, I/A)	Strong central risk group, **aligned performance measures, incentives and rewards**. Unambiguous accountability and escalation requirements
	Bring a **strategic risk perspective** to risk management and look beyond traditional financial risks. Embed risk in the strategic planning process	Timely **valuable independent risk insight** and effective discussion about inherent business risks Improved **performance balancing risk and reward**
	Define risk capacity, tolerance and appetite to improve our understanding of the risks we are assuming	**Strengthen analytical capability**, improve risk judgments and clarify the communication about the risks we are assuming
	Improve the **formality and effectiveness of the risk management processes**. Integrate credit, market and operational risk management practices	Improved **data and process quality** to deliver comprehensive transparent reporting. Improve operational excellence across the business **(no surprises)** Improve the formality of **operational controls, models, metrics, limits, valuation**
	Improve **relationships with stakeholders**	Restore **regulatory goodwill** and relationships

Summary of the Canadian Bank's approach to Risk Management - findings from Annual Reports*

- Each bank has a risk management framework that includes credit, market, liquidity, operational, environmental and strategic risks.

  Responsibility for managing credit, market, liquidity and operational risk generally belongs with the LOBs.

  Environmental risk is typically incorporated in credit risk.

  Strategic risk is the responsibility of the Senior Executive Teams.
- Each bank has a risk management committee at the board level. Typical responsibilities are reviewing and approving risk management strategies, policies, standards and limits.
- Each bank has executive level risk management committees. Generally, the committees either directly or through sub-committees, have responsibility for credit, market and operational risk.
- Oversight for risk management activities is performed by a central risk management function.
- Risk management is performed by independent risk professionals within the business units.
- Internal audit is not involved in day to day risk management activities, but performs periodic reviews of the effectiveness of the risk management framework.
- Market risk is responsible for trading risk. Non-trading risk and liquidity risk is managed by Treasury with oversight from the ALCO or its equivalent.
- Where Canadian banks differentiate themselves in credit risk is their discipline and enforcement of risk policy to meet corporate objectives.
- Compliance risk is managed differently across the banks. RBC has a Global Compliance Group which is part of Enterprise Risk Management. Compliance risk is managed by Operational Risk at Scotiabank.

* Annual reports reviewed for BMO, CIBC, TD, Scotiabank, RBC and NBC.

Overall Risk Management Framework in the Canadian Banks

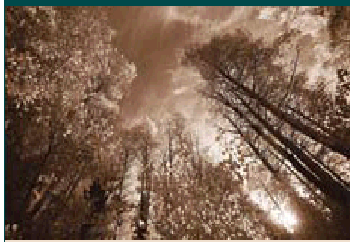
Category	Industry Practice	Observations
Enterprise Risk Management Framework	▪ Leading industry practice is to have an Enterprise Risk Management Framework that clearly defines key roles and responsibilities: – Business units responsible for taking and managing risk – Independent risk and compliance functions responsible for setting standards, providing tools and objectively monitoring risk – Internal Audit responsible for providing independent validation and assurance that the risk management system is designed and operating effectively – Board and senior management both responsible for overseeing effective and efficient enterprise risk management. ▪ Leading industry practice is to have an integrated Risk Management Framework that drives cross-functional effectiveness and efficiency with respect to people, processes, technology and information. ▪ Consistency in corporate and business unit organizational structures helps achieve framework integration, effectiveness and efficiency objectives.	▪ Each of the major Canadian banks have Enterprise Risk Management Frameworks that include Credit, Market, Liquidity, Operational, Environmental and Strategic risk. Within each bank, responsibility for managing risks generally belongs within the business units for Credit, Market, Liquidity and Operational risk. Environmental risk (lending related) is generally managed through credit risk. Two banks (TD and RBC) have Corporate Environmental Affairs groups for the oversight of Environment risk (non-lending related) management. Strategic risk is the responsibility of the Senior Executive team. Oversight for liquidity management is generally the responsibility of Treasury. ▪ While each bank has a risk management framework, only the Royal Bank of Canada provides a description of their risk appetite framework and the risk management principles that guide their risk management activities (see Appendix II).

Matthew A. Hilbert, ***B.A., B.E.Sc., M.E.Sc., P.Eng***
Principal

MAH Risk Consulting
87 Hemingway Crescent
Markham, ON
Canada, L3R 2S4

mobile **416.919.8008**
office **905.943.9608**
email **mah_risk@rogers.com**

Stratos
strategies to sustainability



ONE APPROACH TO HOLDING SUCCESSFUL INTEGRATED RISK MANAGEMENT WORKSHOPS

EXECUTIVE WORKSHOP:
IMPLEMENTING RISK MANAGEMENT IN 2008
Friday May 9th,

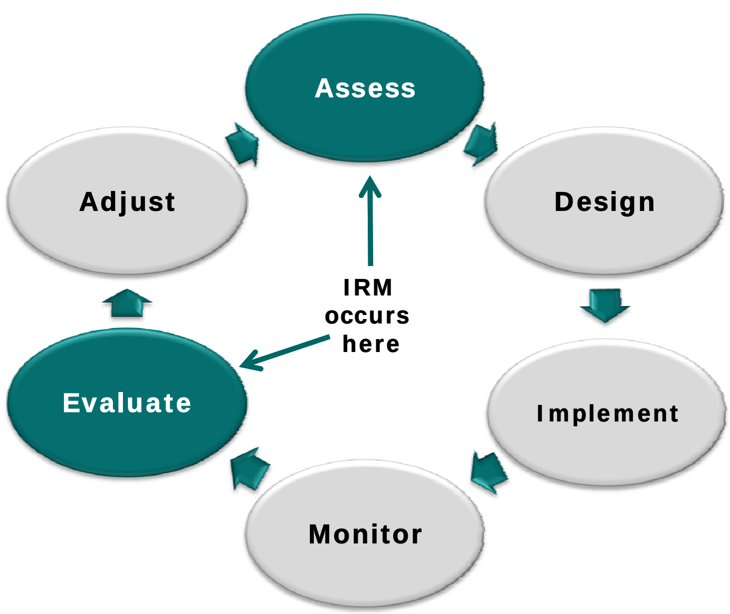
John Lark
Risk Practice Manager
Stratos Inc.
jlark@stratos-sts.com
613 241 1001

Imagine Caring Company Une entreprise généreuse

CO_2 A Carbon Neutral Company®

Stratos
strategies to sustainability

Where Integrated Risk Management Fits In



Stratos
strategies to sustainability

Risk Workshops

What they are

- An “expert Committee”
- “The Wisdom of Crowds”
- Self Assessment
- Ask the people who know
- Reality Check
- First things First
- Looking across the organization
- The end of “the best PowerPoint”

What they accomplish

- Engagement of working staff in the process and in the results of the process
- Get managers and “deliverers” and policy makers to talk
- Get “pitchers” and “catchers” to understand one another's worlds
- And their actual tolerance for risk
- They produce reliable and repeatable results that the participants understand and support

Stratos
strategies to sustainability

Workshops

How do they work?

- Prepare, prepare, prepare
- Use anonymous voting technology
- Open with validation and engagement
- Confirm
  - Objective
    - Of their work
    - Of the workshop
- Activities Universe
- Risk Universe
- Timing (arrival, departure, meals)

Before the workshop

- Always provide as much background as you can
  - Risk Profiles
  - Activity Universe
  - Objective of the workshop
  - A contact for participants to get clarification from
  - Identify who “authorized” establishing the workshop
  - “placemats” of information needed for the workshop

Stratos
strategies to sustainability

Workshops

Details

- Duration
  - Between 1 and 2 days
- Size
  - No less than 6
  - No more than 18
- Composition
  - Staff from all levels, including those who:
    - Deliver the work (Pitchers)
    - Direct the work
    - Plan the work
    - Rely on the results of the work (may include the public) (Catchers)

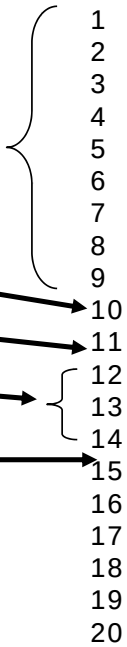
Keeping Focussed

- With activities, risks, likelihood and impact all sloshing around at the same time, people can easily get confused
- You need an excellent facilitator
- Other Strategies
  - Place Mats
    - Red are criteria, Blue is program elements
  - Two Data Projectors
    - One for votes, one for whatever is being discussed

Stratos
strategies to sustainability

Who Should Attend

- 10 to 20 people
- At least half “deliver”
- The line manager
- The client for the work
- One or two key “enablers”
- The line manager’s manager
  - For the opening and closing of the workshop



Stratos
strategies to sustainability

Sample Risk Information Sheet

There is a risk that . . .

Statement of the risk event that, if it materializes, can negatively affect the achievement of enterprise objectives

Risk Drivers

- Identifies possible sources of the risk event, such as environmental factors or management framework weaknesses

Current Risk Mitigation

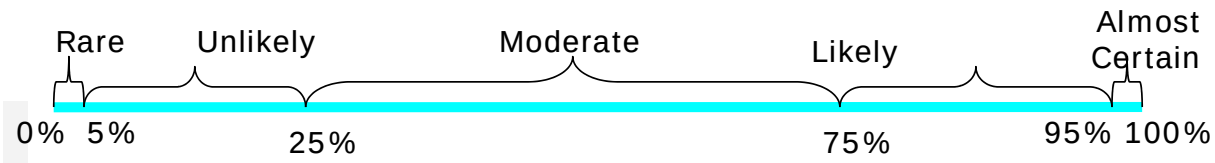
- Identifies examples of current actions, processes, controls, etc., that reduce likelihood of risk occurring, or severity if it were to occur

Possible Consequences

- Describes possible impacts if the risk were to fully express

Stratos
strategies to sustainability

Choose Criteria For Rating Risk Likelihood



Likelihood	% Probability	Experience/Observed Frequency
5. Almost Certain	More than 95%	Occurs regularly here.
4. Likely	76 – 95%	Has occurred here more than once, or is occurring to others in similar circumstances.
3. Moderate	25 – 75%	Has occurred here before, or has been observed in similar circumstances.
2. Unlikely	5 – 24%	Has occurred infrequently before to others in similar circumstances, but not here.
1. Rare	Less than 5%	Almost never observed - may occur only in exceptional circumstances.

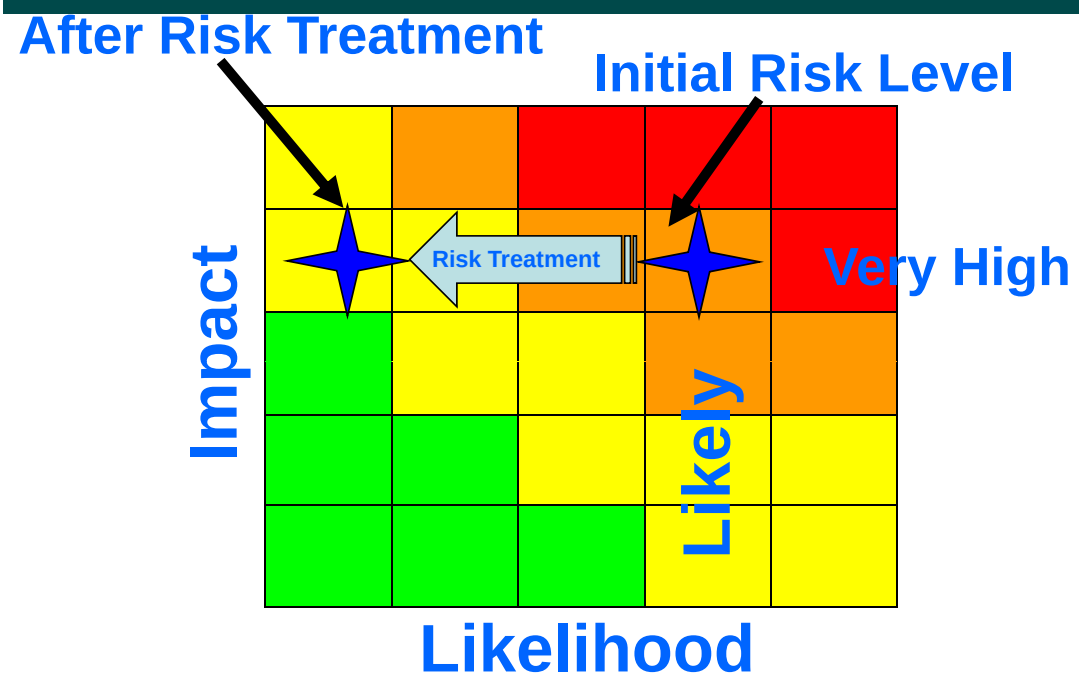
Stratos
strategies to sustainability

Choose Impact Criteria

Impact Level	Definition
5 Critical	A critical event having an intolerable impact on the entity and that will require the entity to make a large scale, long term realignment of its operations, objectives or finances.
4 Major	A major event having significant impact on the entity, the consequences of which can be absorbed, but with proper management can be addressed by the entity.
3 Moderate	An event having a significant impact that can be managed by the entity. The consequences could mean that an activity could be subject to review or changed ways of operation.
2 Minor	An event having an impact, the consequences of which can be absorbed but management effort is required to minimize the impact.
1 Low	An event, the consequences of which can be absorbed through normal activity.

Stratos
strategies to sustainability

Risk Treatment



IMPLEMENTING RISK MANAGEMENT IN 2008

PARTICIPANTS

Ertugrul Alp
Alp & Associates

David Bleiker
Amec

Richard K. Brummer
Itasca Consulting Canada Inc.

Dale Cooper
Broadleaf Capital International

Diana Del Bel Belluz
Risk Wise

Serge Deschenes
National Defence

Brian Griffin
Golder Associates

Matthew Hilbert
Consultant

Roger Humphries
Nuclear Safety Solutions Ltd.

Kim Hunton
City of Ottawa

John Lark
Stratos Inc.

Michael Moskau
National Defence

Michael Murphy
Ontario Internal Audit Division

Marcello Oliverio
Nuclear Safety Solutions

Grant Purdy
Broadleaf Capital International

Rob Quail
Hydro One Inc.

John Shortreed
Institute for Risk Research