'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)

Issue #1

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

Issue #2 – Same as #1?

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.