The Evolution of Risk Management: Just do it !" -- do ISO 31000 !

. Summary of talk by John Shortreed at 2008 International Risk Management Conference Toronto, Tuesday January 29 with repeated material etc., edited out

NOTE a survey of progress in each of the 5 Olympic Risk Circles (scored as 2 for 'have risk ring' 1 for implementing ring and 0 for no ring, total 10) indicated about 35 % of the 140 people there, that their organizations scored 5 –10, 40% scored 3-4.

Organization-wide risk management is now "ready for take off", the 50 year evolution to maturity is complete, Not only is the evolution mature but a take off platform is being constructed – that platform is ISO 31000 a risk management standard, - 31000 is now essentially finalized and to be published in early 2009. ISO 31000 will be invaluable to ensure your ERM program adds value to your organization by helping with implementation of the latest and best global risk management practices.

This talk will focus on the near future of risk management - defined as the implementation of ISO 31000 in your organization and others throughout the world – I will talk about what is 31000?, how to implement 31000?, and most importantly WHY YOU WILL HAVE TO IMPLEMENT 31000!. ISO 31000 is very similar in some respects to ISO 9000 and 14,000 and other broad based international standards, except it is not, not certifiable and hopefully more practical. It is a concise and comprehensive statement of good ERM practice.

Participation in a round of golf at St. Andrews, running the Boston marathon, representing your country at the Olympics, playing on the local hockey team, are all activities that provide value to the individual participant, not just the winners. All participants have increased confidence, more comfort in the ability to achieve objectives, noticeable gains in learning and experience in playing the game, improved resilience, higher reliability, more respect from others, and better health and fitness.

These **participation** benefits are also available from implementing ISO 31000, Risk Management - Principles and Guidelines on Implementation, in your organization. You also can have increased confidence in making reliable decisions, managing risk, dealing with threats, opportunities and crisis, improved safety, financial and corporate governance and all other benefits of fully integrated enterprise wide risk management.

Like the famous Olympic logo of 5 intertwined rings, ISO 31000 has 5 intertwined themes as shown in **Figure 1**; The bottom two rings or the foundation for ISO 31000 is **firstly a common set of risk Terminology and secondly the Risk Management Process.** The process in not new, you all use it now to manage risk in your organization today.

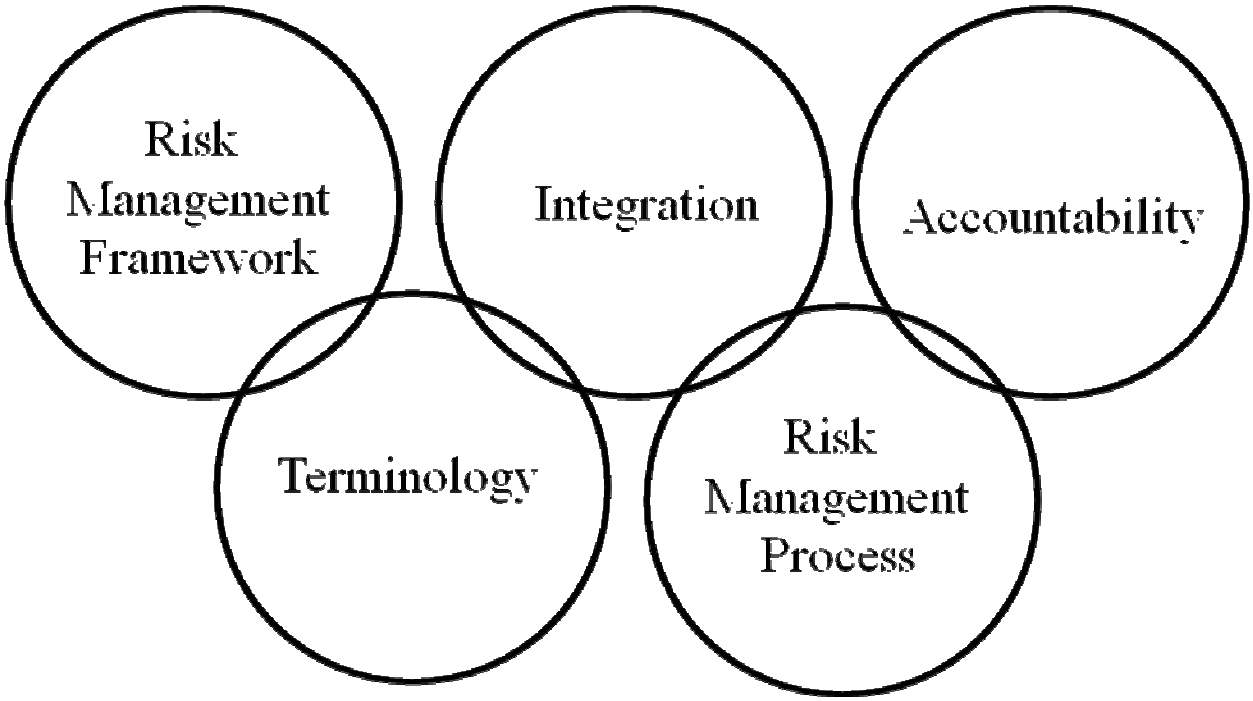

Figure 1: The Risk Olympic Rings

The top three *Risk Olympic Ring*s are **Risk Management Framework, Integration, and, Accountability** .

ISO 31000 Risk Management – Principles and Guidelines for Implementation, is now more or less finished given the decisions made by the working group in China last month. To obtain a draft copy for review and comment just contact me or Jan Mattingly or Awad Loubani, after April 1 when the latest draft goes out for a 5 month comment period and vote.

Also in 2009, Canada and other countries will reissue existing risk standards such as CSA Q850 (1997) in compatible form. So the time is opportune to look at what is new in 31000 and what your organization must do to implement it – assuming you believe me when I state that risk management is finally ready for take off for a world wide consistent, comprehensive, and universally understandable application of risk management.

Like training for the Olympics, hard work is needed, new techniques must be looked at and changes made – but the results are worth it. The 5 *Risk Olympic Ring*s are shown in **Figure 1**.

The **Terminology** *Risk Olympic Ring* is a key change – while ISO Guide 73: introduced in 2002 common risk terminology, ISO Guide 73 will be reissued with ISO 31000 in 2009 and will have more general, more generic, and much higher profile definitions. One arrangement of the currently defined terms in Guide 73 is shown in **Figure 2**.

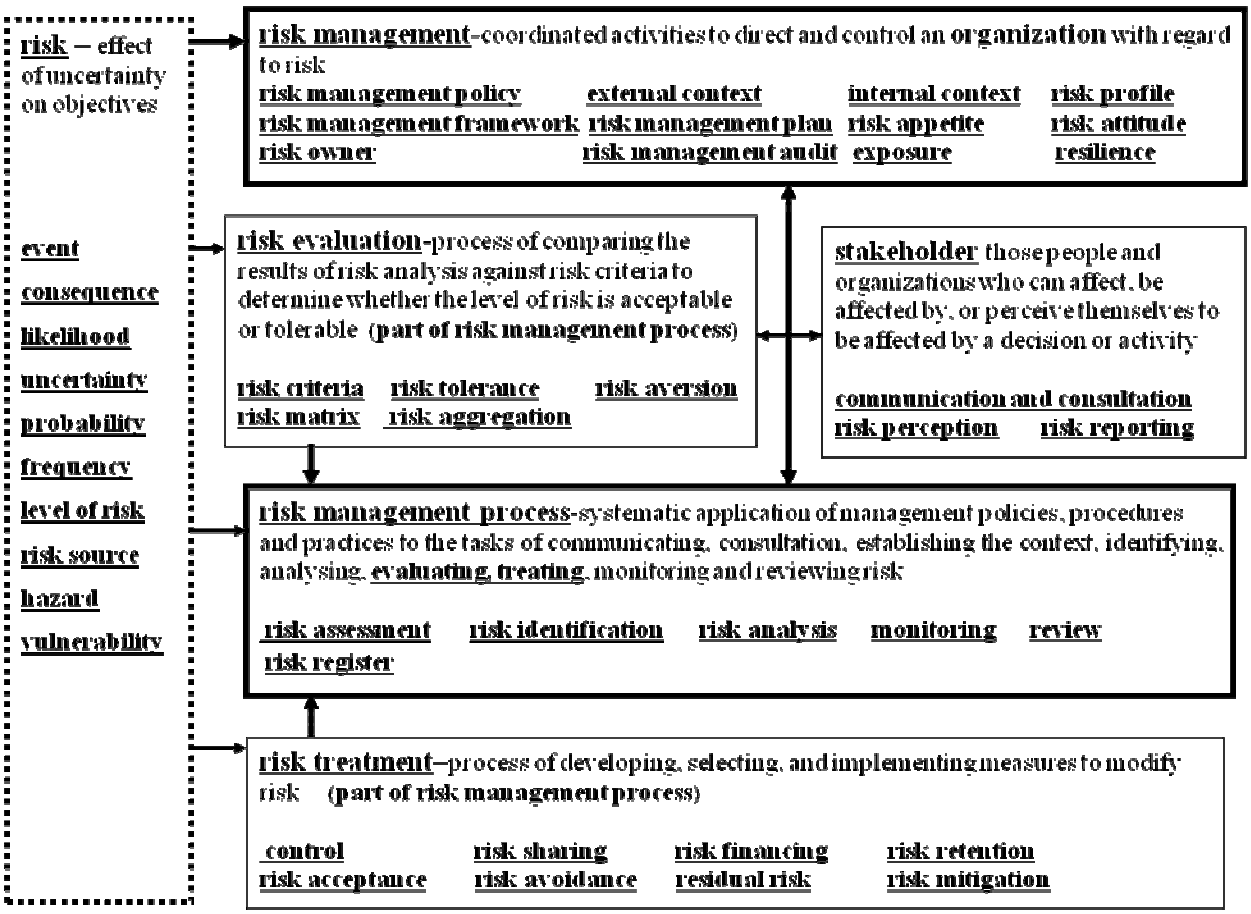

Figure 2: Relationship between **terms** for risk management in an organization. (Note: Risk management process includes risk evaluation and risk treatment).

For example, **risk is defined as "effect of uncertainty on objectives"** not as some technical statement about events, consequences, likelihood, perceptions, etc. The new definition is much closer to the needs of modern organization-wide risk management frameworks. This high level generic organization-wide application, is ERM that is also designed to incorporate existing risk management techniques for credit risk, for workplace health and safety, for currency fluctuations, for hiring and firing risks, or any other detailed technical risk management, not just for ERM.

Risk –*"effect of uncertainty on objectives"* is supported by a new concept, for risk standards; **Risk Management Framework; *"set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization"*** As the definition states, these are the components, in an organization, of policy, accountability, implementation, and continuous improvement of risk management. The **Risk Management Framework** is one of the 5 *Risk Olympic ring*s and we will return to it in a moment.

Other key terminology for a key concepts is **Risk Treatment**; ***"process of developing, selecting, and implementing measures to modify risk"***. **Risk Treatment** results in **Control** – ***"measures to modify risk"*.** Users of COSO will immediately recognize that the terminology is more business and

general organization-wide risk management friendly Unlike COSO the risk management process that incorporates risk treatment is a process that is also simple, practical and feasible.

The control for a risk belongs to the **risk owner; *"person or entity with the accountability and authority"***. Firms like BHP Billiton, Mars (bars people-see excellent talk by Larry Warner), and Hydro One, that have fully integrated and accountable risk management frameworks, enjoy savings of 10's of millions a year on lower insurance rates and cost to borrow money due to good risk management practices. BHP for example has lists of risks and risk owners, with more than 80,000 entries as well as libraries of tens of thousands of risk registers filed by these risk owners in order to meet performance expectations for annual bonuses.

New also is the explicit definition of **context; *"external or internal environment in which the organization seeks to achieve its objectives",*** as well as informative lists of context elements. The context drives the objectives of the organization as well as driving **risk evaluation; *"process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable".***

ISO 31000 is not certifiable – in the same way that management of an organization can not be certified against some standard, risk management is designed in terms of principles and guidelines for implementation but not for certification – how each organization does risk management is up to them.

The **Risk Management Process** in **Figure 3** has five activities;

1. Communication and Consultation,
2. Establishing the Context,
3. Risk Assessment, where risk is identified, analysed, and evaluated
4. Risk Treatment, and
5. Monitor and Review,

This process has been more or less consistent over the 50 years of evolution of 'modern" risk management. This is standard stuff found in CSA Q850, the Australian/New Zealand risk management standard 4360 (2004), COSO, RIMS, European Space Agency, etc.

The **Risk Management Process** is used by individual decision makers in an organization to help them make decisions according to the protocols and procedures in their particular organization as established by the organization's own **Risk Management Framework**. It is different for each organization but also immediately recognizable as a standard process.

After the **Terminology** *Risk Olympic Ring* and the **Risk Management Process** *Risk Olympic Ring* let's look at the **Risk Management Framework** the third *Risk Olympic Ring*.

The **Risk Management Framework** is new to ISO 31000 and a central concept, as shown in **Figure 4**. **Risk Management Framework** is continuously improved with a Design-Implement-Monitor and Review-Improve cycle which is the same as the more traditional Plan-Do-Check-Act from Total Quality Management.

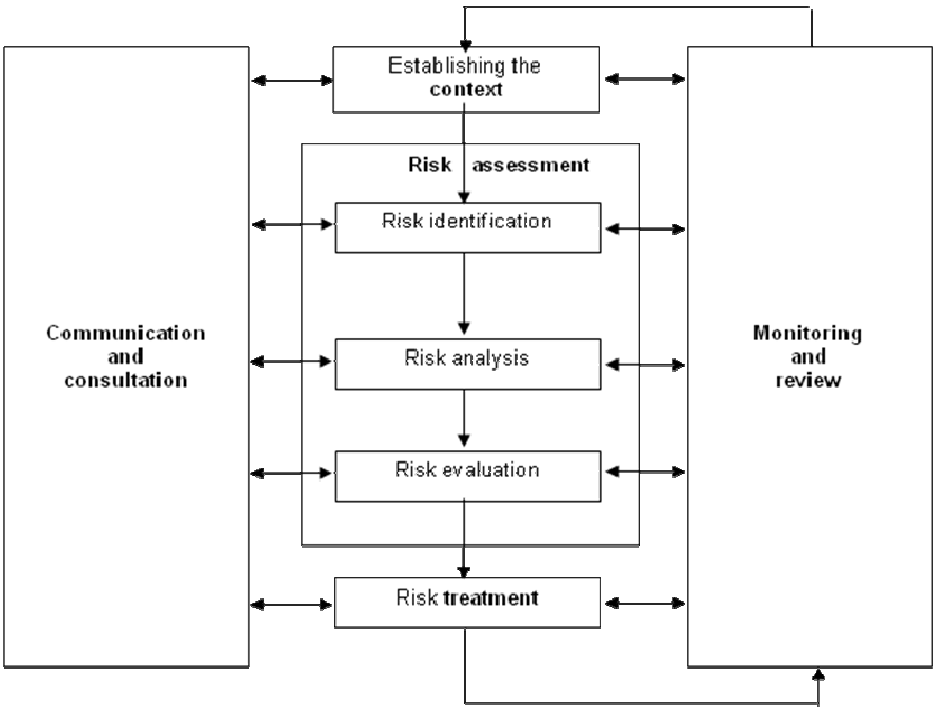

Figure 3: Risk Management Process (Traditional).

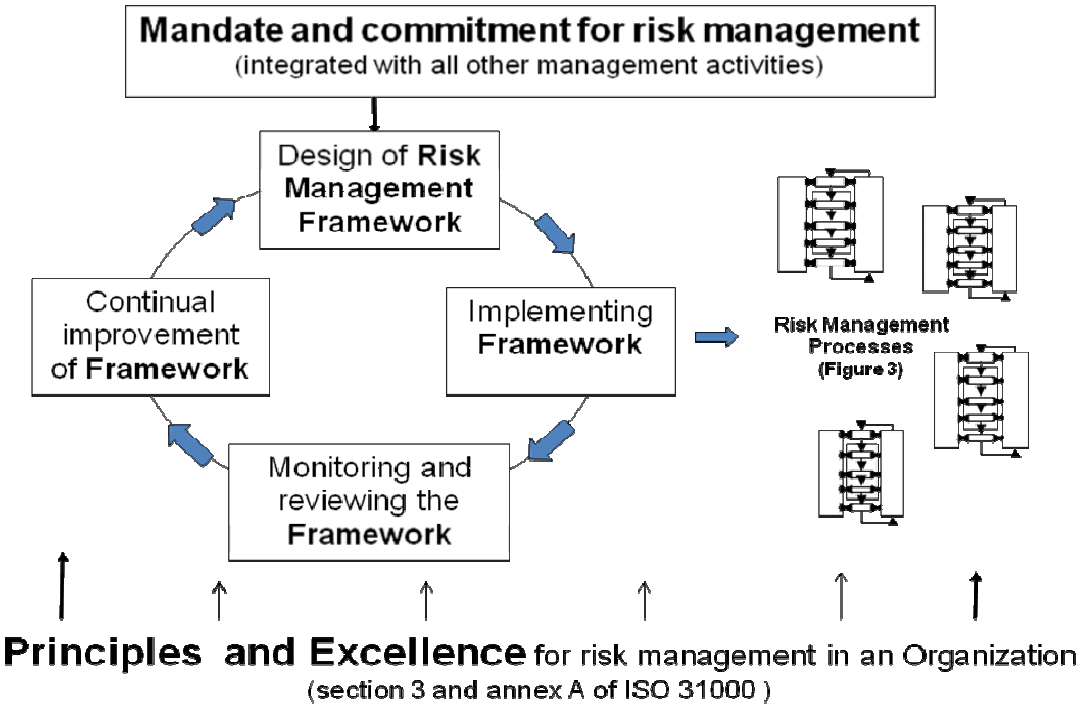

Figure 4: Risk Management Framework in an Organization.

The **framework** concept is supported by an annex of excellence or risk maturity indicators as well as 10 principles in the text of 31000 The principles are about creating value, integrating risk management into the organization, using systematic methods, explicit consideration of uncertainty, up to date inputs, accounting for human behaviour, being dynamic, etc. .

There are 5 excellence criteria and associated measures given in 31000 for the **Risk Management Framework**.

- Excellence One, the **Risk Management Framework** must be continually improved using the well known quality improvement cycle of Design, Implement, Monitor and Review, and Improve, also know as Plan-Do-Check-Act cycle.

- Excellence Two, the **framework** must be comprehensive with accountability for all risks– you can go to anyone in the organization, anyone in the organization, and they will be able to tell you, what risks they own, what controls they are responsible for, and the current status of those controls, trends and current status of the risks, and the expected effects on the objectives concerned. That simple –everyone will know all about the risks they own.

- Excellence Three, all decision making in the organization has explicit consideration of risk, as evidenced by documentation of decisions. This expectation of evidence is embedded in the **framework**.

- Excellence Four, continuous communications and reporting that is highly visible covers internal and external stakeholders as appropriate and talks about performance indicators for risk management is part of the **framework**.

- Excellence Five, risk management is a core element of the organization's management processes including governance. Risk management is regarded as essential by the organization's culture.

The forth *Risk Olympic Ring* – **Integration**. There was a debate, long and heated, among the working group members to say embedding of risk management in overall management of the organization or integration of risk management, so far embedding is winning out, even though Webster's has embedding as a knife stuck into a block of wood while integration is taking two parts and making them one whole. I prefer integration but you can't win them all.

Integration is central to "modern" risk management, the days of add on, after the decision, buy a little insurance, application of risk management should be over forever. For starters the treatment of uncertainty for positive consequences such as revenue targets, customer satisfaction, market share, product life, and reputation are best dealt with when decision options are being identified and selected.

Integration was particularly difficult for the ISO working group since many of the "safety" folks think that safety is absolute and quite different and separate from other risks. There were debates for example about FAR, Fatal Accident Rates that pointed out that safety is never absolute (FAR is

never zero). Other 'traditional safety" issues were also hard going for the ISO working group such as – what about reputation and the possibility to improve the organization's reputation through protection of the environment?

In the end the integration of safety and risk management is achieved by risk being the "effect on objectives" and having safety objectives. This "objective" basis for risk provides a common approach to any risk. This is stressed throughout 31000. As well 31000 addresses the similar issue of how to integrate existing risk management techniques and procedures into the overall framework for risk management in the organization.

The idea is that existing procedures for safe driving, for environmental protection, for workplace health and safety must be fully integrated into the risk management framework. This can be done even though many of the existing risks and their controls are mandated by regulations, by exposure to torts, or by high level policies of the organization.

The second dimension to **Integration** is integration of risk management into the core processes of the organization. The idea is that risk management is just one of many considerations in any decision. Risk is neither more important nor less important but just takes its place with the other inputs to be considered when the decision options are framed, evaluated and selected, not after the decision is made.

While easy to state: "the **Integration** *Risk Olympic Ring* is really change management writ large" this is a real stumbling block to effective and efficient risk management. The issue is how to get senior management's attention and tell them that achieving **Integrated** risk management is a key issue requiring major change. I personally believe in the direct and simple approach - make sure they know that **Integrated** risk management is practical and feasible and will help to achieve their objectives - the rest is up to them

The fifth *Risk Olympic Ring* after, **Terminology, Risk Management Process, Framework, and Integration is Accountability**. **Accountability** is the glue that holds everything together. Typically, **Accountability** is introduced in a formal way – there is a published risk policy, there is a formal risk framework, and there is a list of risks and their owners.

In BHP Billiton, with 200,000 employees, any managers can go on line and see who owns each of the 80,000 risks that are identified. Those owned by the CEO are the only ones missing. Managers know that when their performance review comes around they will have to demonstrate that they really do own the risks, they own the controls, they monitor the controls and the risks and when necessary they took action to ensure continuous improvement.

BHP has a head office of 4 full time risk people, supported by 1 in 200 to 1 in 500 "interested" employees, depending on the nature of the processes, who are "knowledgeable in risk management". These employees are similar to GE employees who have a black belt in six sigma – a special training in cause-and-effect analysis using advanced statistical tools for data rich situations – GE encourages people to get qualifications in 6 sigma even though it is outside of their required skill set – sort of a bonus performance indicator. This support network is there to assist managers who are fully responsible for the risks they own.

Accountability, being a key requirement for success, leads to the requirement that the **Risk Management Framework** and the **Risk Management Process** component of that **framework** have to be "sweet and simple" – the old KISS principle rears its difficult head. Fortunately, there is a feedback loop since managers will complain if their performance bonus depends on an unworkable and unfeasible **framework** and **process**.

The talk then walked through the 4 Figures to reinforce the 5 Olympic Risk Rings – only a few excerpts are given here.

The First *Risk Olympic ring* of **Terminology** is shown by the arrangement of definitions in Guide 73, which will be issued with ISO 31000. These definitions are organized by me in **Figure 2**, time will tell which figure will be in the Guide – (I was not even close on this one, others are ok).

1. terms about risk,
2. terms about organization wide risk management,
3. risk evaluation terms,
4. stakeholder terms,
5. risk management process terms and
6. risk treatment terms, where the rubber actually meets the road.

Consider, risk evaluation. Many organizations use risk management to make strategic decisions utilizing a risk matrix and representing risk consequence, by 5 levels for reputation, 5 levels for profits, 5 for environmental protection, 5 for regulatory compliance, etc. These levels are judged equivalent on a 5 point scale. This approach is often referred to as "establishing tolerability limits" – they are really establishing consequence criteria. Organizations should be sure they actually attach likelihoods to these consequences before they do the risk evaluation of strategic decisions.

The **Risk Management Process** is shown in **Figure 3**. It is instantly recognizable as the standard risk process used by every decision maker who owns a particular risk. This is the well known Australian/New Zealand 3460 (2004) standard and is also conceptually the same as the 1997 Canadian Q850 standard and others such as the 1960 standard for US defence spending and the Zurich insurance companies "blue book" from the 70s. Note that the **Risk Management Process** takes up a full 50% of the text of 31000, so it is rather important.

The *Risk Olympic Ring* of **Integration** is everywhere in the document, from the notion of risk as uncertainty for both positive and negative objectives, to the notion of ownership of risks by decision makers, to the ideas of integration of existing risk management policies and procedures, to the incorporation of continuous improvement through continuous communication and consultation as well as continuous monitor and review processes.

Reflect for a moment what might have happened if risk management had been fully integrated into an organization. Sarbanes-Oxley would not have been a huge add-on process but a minor revision of existing risk management regulatory compliance processes. Improved governance after Enron would not have been a major new review and change situation but a smaller continuous improvement of monitor and review processes for the organization, where appropriate.

ABCP the current ‘threat” to most organizations, but an “opportunity” for Warren Buffet would be a simple matter of review of existing control practices based on experience. As exemplified by some financial institutions such as TD that dodged the bullet, any reasonable understandable and ‘best practice’ control of uncertainty in capital markets would have kept organizations out of the deep water in the first place.

END OF TALK – Please see end notes and example of how to implement ERM?

End Notes (or “if I more time” wish list)

1. Once ERM is implemented everywhere, over the next 5 years, according to ISO 31000 there is a need to revisit the existing risk assessment techniques and bring them into harmonization or alignment with the framework implemented in each organization – this is a big task.

2. In implementing 31000 it is important to have an "architectural" design for risk management in the organization. The concept is similar to construction of buildings where on behalf of the client, the design is done by an architect quite separately from the construction or implementation This gets around the problems of consultants selling you something they know how to do and organizations thinking they can off-load all the heavy lifting to consultants. The following describes one such approach used in Australia, the “original source” of ISO 31000.

Application of the “Architect” Approach in Implementing and Sustaining Effective ERM
(example courtesy of Grant Purdy of Broadleaf Capital, **Purdy@broadleaf.com.au**)

Rather than use a “design build” contractor with a pre-packaged approach to ERM it is preferred to have a consultant who partners with the organization in developing a customized framework, tools and methods that reflect the organization’s needs, risk profile, and organization structure. Risk management champions are found within the organization and trained to implement and roll out the framework in a top-down engagement process. This seems to achieve the most rapid take-up and long term ownership of risk management in the organization, by working with the organisation’s line managers and risk management specialists, and building on their skills and experience risk management processes are more relevant to business needs and this also creates early and visible risk management benefits.

The Broadleaf approach involves a 10 step process (modified slightly by JHS);

1. Achieve an unequivocal Executive and Board mandate for the program with a full appreciation of the implications of the changes required at all levels of the organisation.
2. Undertake a gap analysis and maturity evaluation against recognised standards.
3. Develop a carefully tailored framework, based on ISO 31000 risk management framework, principles, and process as well as the organisation’s context and structure necessary for ERM to be implemented and sustained.
4. Workshop and develop a strategic risk management plan to implement the framework utilizing practical tools and best practice methods

5. Develop and gain senior management agreement on a set of performance-base standards that codify the framework and its implementation plan.
6. Create a risk management information system, tailored to the framework and organisation, that enforces accountability for risks, controls and tasks, supports control assurance and enables risk management performance management and reporting.
7. Cause Champions to be appointed within the organisation and trained to create the confidence, skills and local management support needed to roll-out the framework.
8. Help Champions engage local management and implement the framework and risk management plan, generating risk registers and other information systems.
9. Establish a process and structure for RM performance management and reporting, including committees and review groups, reporting templates, KPIs and performance measures.
10. Periodically, review, benchmark with external best practice, and revise the framework.