1. Which risk management framework is used in your practice and why?
How do you see the comparative strengths and weaknesses of COSO ERM
and ISO 31000:2009?

[Fraser] Our ERM framework was derived from the AS/NZ 4360 in 2000 with input from Towers Perrin Tillinghast papers and Conference Board of Canada papers. Not much has changed since then in my opinion. I have not read the COSO document recently. I really tried when it first came out in 2004 and 2005 but gave up due to its length and complexity. There was some good in it but it was more than twice as long as merited. It also has some known flaws (i.e. ignoring black swans, ignoring the upside, confusion over terms like appetite and tolerance, talk of inherent risk, etc). Linking it so closely to the 1992 COSO document sounded logical but was a mistake. I always advise implementers NEVER to show the infamous “cube” to management as it is a complete turn off. The Conference Board of Canada 2007 survey of Canadian CROs showed few in Canada use or like COSO 2004.

ISO 31000 is short, precise and logical. Nothing in it conflicts with 4360 and the earlier writings above or what has worked in practice for ten years. Obviously it cannot contain all the details but neither do the Ten Commandments. Once we can get people agreeing on ISO 31000 we will have a base to work with.

[Parkinson] We have used AS/NZS 4360 since 1995. We have recently "upgraded" to ISO 31000:2009.

The COSO document has its origins in "fraudulent financial reporting" at it shows in its approach. ISO 31000 starts with the organisation (however you wish to define that) and its objectives. It is scalable - so can be simple for small tasks - and can be applied to any form of risk. We (in Australia) are in the process of applying it to disruption risks (so called "business continuity"), health and safety risks, risks to and from the environment, risks in running not-for-profit organisations and many other subject areas.

With 15 years of experience in using the standard, we feel that AS/NZS ISO 31000 works well and is universally applicable. It is true that it lacks detail, but detail is developed as it is applied in particular circumstances. There are current ISO proposals to develop an implementation guide for 31000.

[Schanfield] I prefer to use ISO 31000:2009 or AS/NZS 4360:2004 instead of COSO ERM. Several thoughts that follow are gleaned from discussions as well with Purdy and Fraser.

1. ISO is 10% of the length of COSO ERM: 5-10,000 words versus 150,000 words. COSO ERM takes hundreds of hours of effort to read a number of times, let alone getting your hands around the material. Nobody has this sort of time to invest.

2. The COSO ERM definition of risk management is confusing. It is a 62 word run on paragraph. The ISO definition of risk management is six to seven words and is easy to understand. “Risk Management is a discipline for managing uncertainty.” “Risk is the effect of uncertainty on accomplishment of the business objectives.”

3. Both frameworks are principles based but the COSO ERM consists of 120 principles versus 15 or so in ISO. Many of the 120 principles are redundant overlapping concepts and in the end analysis, what are you supposed to do with 120 principles? How can you expect to review these throughout an assignment and expect to glean value? At least with the 15 ISO principles, you can quickly scan such material throughout any risk management effort to ascertain whether all are being complied with.

4. We are still waiting after six years post issuance of COSO ERM to see an initial completely integrated case from beginning to end. If this material is so good, why does one comprehensive
case not exist? What I have seen in the way of case material is at best a series of PowerPoint slides depicting pieces of the framework or the cube but never an integrated case. The cube is simply confusing. The authors injected into the application book 50 or so examples of implementing COSO ERM but there is no integration of the examples which cross industries and situations. Helpful in some respects but overall not helpful for those individuals that are novices in this area or wish to get their hands around the material.

5. The authorship of COSO ERM was by the public accounting profession- albeit presence of various industry groups to oversee the initiative but basically this is a public accounting document. Several key constituent groups and thought leaders from the risk profession were not represented on the task force- GARP, PRMIA, RIMS and many sole practitioners and thought leaders. The ISO 31000 effort was worked on by hundreds of risk practitioners from around the globe for three years with several drafts having been written. It is a best in class document written by the risk profession for the risk profession.

6. There is minimal discussion in COSO ERM on external stakeholders and their needs/expectations which is quite monumental. COSO ERM seems to be focused primarily on internal stakeholders, yet external stakeholders are critical. Much of the disconnect we witness in companies occurs because we do not take the time to understand external stakeholders and their needs/expectations. All the stakeholders will influence a company’s risk appetite/attitude (how much risk and the type of risk it wishes to take) and the risk criteria (the parameters/guidance by which the significance/likelihood are defined).

7. There is a risk management process and a risk management framework. The framework exists to support the process. This is clearly articulated in ISO 31000. COSO ERM confuses the two and makes no effort to delineate these two concepts. This is in my opinion the primary reason why the COSO ERM framework is so difficult to understand and implement. This confusion just disappears when you pick up and read ISO 31000. The process which should be fixed comprises context, risk assessment (identification, analysis, and evaluation), risk treatment, risk monitoring, and communication. The framework is flexible and needs to be tailored to the specific company.

8. It is impossible to understand in COSO ERM where to begin, whereas this is quite clear in the ISO 31000 guidance and accompanying materials.

9. The COSO ERM guidance indicates that in considering opinions during drafting of the framework, that other risk frameworks were considered including AS/NZS 4360:2004 the precursor to ISO 31000:2009. It was further stated in the COSO ERM document that the team decided it was not necessary to use such a framework. No explanation is given for this decision. Had AS/NZS 4360:2004 and the accompanying application guide of HB 436 been used instead of creating a separate framework, we probably would not be having this discussion since ISO 31000:2009 is built on the DNA of AS/NZS 4360:2004.

10. COSO ERM focuses on the apparent/ fast types of risks and not the slow evolving ones such as for example changing population demographics.

11. COSO ERM does not spend much time focusing on untapped business opportunities or the upside of risk but primarily deals with the downside of risk. It also uses the term of inherent risk which is risk in the absence of any controls which does not make sense. Why not use the term “worst credible risk?”

\[Purdy\] We have used AS/NZS 4360 for the last 15 years. Three members of our team are part of the committee that developed that standard. We also played a major role in the development of ISO 31000 and I am the nominated expert for Australia on the ISO Working Group.
As Manager of Risk Management at BHP Billiton (world's largest resource company), I built the framework for ERM on AS/NZS 4360:2004 and that framework now operates around the globe at all the company's locations.

ISO 31000 is based on over 15 years practical application of AS/NZS 4360 in 1000's of organizations around the world. The AS/NZS was updated through a public consultation process on three occasions. ISO 31000 was developed by an international team of over 30 practicing risk management professionals from many sectors and interests. Their role was to consult with 'mirror' groups in their respective countries and sectors so that 100s, if not 1000's of risk management professionals were involved in its development. ISO 31000:2009 comes with a vocabulary for risk management where the terms used are consistent with one another and with the risk management process.

ISO 31000 is concise at 20 pages, excluding definitions. It contains not just descriptions of the steps of the risk management process, but also practical advice on how risk management can and should be integrated into the decision making processes of an organization. It also contains performance criteria against which an organization can judge if is approach to risk management will be effective and how it can be advanced.

COSO ERM outside of the US has always been regarded as a US standard, inextricably linked to SOX - which is itself mostly considered an ill-informed and ill-focused attempt to deal with poor reporting and poor corporate governance. COSO ERM therefore is more focused on reporting than on treating risks. It lags more advanced governance reporting thinking that reporting should be about the quality of risk management, not just what are the risks.

From the start COSO ERM seemed to embody the 'auditor's view on risk management' not the risk managers' view. While the report is vast, it does not seem to offer much tangible advice on how risk management should be implemented to be effective.

There are many technical weaknesses in the COSO ERM framework, many of which stem from the need to be seen to link the risk management process to the internal control model in the 1992 COSO document - which itself led to that wretched cube.

The major technical weaknesses are that:
1. It is internally focused and the context is not established in terms of both external and internal factors and influences.
2. Stakeholders and their objective are ignored in terms of setting risk criteria.
3. Risks are seen as events, not associated with the effect of uncertainty on objectives.
4. Risk is incorrectly estimated in terms of the likelihood of an event and its consequences. This produces 'phantom risks' and does not lead to effective and appropriate risk treatment.
5. Risks are only seen in a negative light and risk treatment (response) is only about mitigation.
6. "Risk responses", "control activities" and "monitoring" are confused. Control is used as both a verb and a noun.
7. Risks are said to "occur" and likelihood is when risks occur!
8. Inherent risk is used. This is recognised as a highly confusing and flawed concept that is unnecessary.
9. "Risk appetite" and "risk tolerance" are mixed up and confused. They are dealt with in a naive and simplistic way.
10. The description of the risk management process is mixed up with the framework required for the effective implementation of risk management through integration.
ISO 3100 is a relatively easier framework to present and understand compared to COSO. The COSO framework and “cube” is a robust end point but difficult to start with. It strikes management people and directors as too complex and “consultant speak.” The COSO approach also goes quickly into defining risk appetite, which we find in practice is not something that fits early in the ERM process. Organizations and senior people need to move further up their learning curves to deal with risk appetite.

We believe COSO is in the process of trying to produce practical information through their Thought Paper series (we are developing one currently) to make their ERM framework more applicable and user friendly.

I’ve never really fully adopted a specific framework where I have worked, but have taken parts from both AS/NZ 4360 and COSO ERM. I found that people’s eyes glaze over when I discuss COSO ERM, but most folks in the US have been resistant to considering a standard coming from Australia/New Zealand. So I took the good things from both and we never officially adopted a single framework.

Having said that, I recently conducted a gap assessment of our ERM program here at Mirant and used ISO 31000 as the foundation for the assessment. I supplemented the ISO with other relevant practices, for example, from the NACD Blue Ribbon Commission report titled Risk Governance: Balancing Risk and Reward, as well as the Standard & Poor’s ERM review questions. I found this combination of leading practices to be quite useful in my assessment.

Overall, I agree with the others that ISO 31000 is the most intuitive and executive-friendly framework, and believe it should be adopted globally. However, I don’t think we should just throw COSO ERM on the trash heap. I believe it has some good thoughts and guidance that supplement the briefer, more intuitive ISO guidance. I’ll talk later (Question #7) about what my recommendations are re: COSO ERM.
2. **Is there a need for a single, global risk management standard or framework? If so, what should the role of the IIA be?**

**[Fraser]** It seems like a good idea. With globalization and moves to IFRS, ISO 9001, ISO 14001, etc., it makes sense. The challenge is that for many other standards there were well understood country practices and standards and ISO then brought them together. The challenge with ERM is that few countries really understand or practice it well, which makes alignment of the existing confusion more difficult but desperately needed.

IIA’s role should be the same as it is on ISO standards generally (what did it do with ISO 14001? on IFRS? on Sarbanes-Oxley?). Presumably it sent input to help these along. COSO is different in that the IIA has included itself in a group as a de facto standard setter. Its position within COSO could be very powerful; however it needs to bring a broader perspective to bear than what has been done before. Alternatively, the IIA could take a leadership role and publish its own material separately from COSO.

**[Parkinson]** Yes and I believe 31000 provides it. There is also a series of Management System standards (ISO 9000, ISO 14001, ISO 28000) that are not entirely consistent with each other, but ISO has a project to develop (redevelop) the management system meta-standard, so that all of these may eventually become consistent with each other.

I would not make general comments about whether "countries" understand ERM - I would suggest that in all countries some individuals understand it and others do not. Many Governments use the terminology, but whether this means there is general understanding amongst officials is another matter. Even after 15 years, I am not convinced that everyone who should understand risk management in our Government sector really knows what it is about. When ERM is well understood in the management community - local, national, multinational - then it will be applied.

IIA should contribute to the debate and this can be done at multiple levels. Every IIA Institute can participate in their National Standards Organisation (ISO is a federation of such bodies). IIA could become a corresponding member of ISO and contribute directly at a global body to global body level.

COSO being a US body should be able to work with the US NSO - IIA (global) as an international body should be able to work at the summit level, while individual institutes work at a national level.

**[Schanfield]** Sure there is. Let me respond to your question with another question which is “what do you think the implications are because a standard risk management framework does not exist?” Play this out. There are 30 of so organizations in the US all touting expertise in risk management and selling their various products and services. (See listing in appendix). In addition to these organizations are the various consulting firms, both big and small, with their individual version/interpretation of risk management which in many cases consists of various PowerPoint slides “adapted from COSO ERM.” What I maintain we have here in the US anyway is bedlam in terms in risk management because of the myriad of different approaches.

The inconsistent services throughout the US have contributed to waste and inefficiency and I think as well been a catalyst for some of the governance issues we have witnessed over the past ten years. True that we have been mired in Sarbanes-Oxley work, however there was an opportunity in 2004 to leverage up the Sarbanes effort to ERM in issuing the COSO ERM framework but this leveraging never occurred.
The role of the IIA post meeting in August should be in my opinion to recognize the other professional organizations out there and seek to bring them together. In addition, the IIA could perhaps take the lead at venues such as the World Economic Forum in Davos to speak on a unified approach to risk management.

[Purdy] Yes. That was the express purpose of ISO 31000. ISO is now in the process of aligning all its management system standards to ensure a consistent approach and vocabulary.

The roles of standards are to:
- standardize definitions and approaches to management;
- reduce barriers to trade through harmonization;
- drive improvements in safety, environmental protection, business efficiency etc. through setting performance requirements.

It makes a lot of sense therefore that there is just one standard for the management of all forms of risk that uses one approach with one set of terms and vocabulary. It also makes a great deal of sense if management, risk management professionals and assurance providers also use the same approach and terminology. It is highly inefficient if we use the same words to mean different things and go about risk management in quite different ways.

IIA is concerned with assurance, not primarily with risk management. Assurance providers need the results from a risk management process and therefore are concerned that that process is reliable and comprehensive. SA/IIARF Handbook HB 158:2010 (and the 2006 version) shows how that can be achieved.

Assurance providers also need to understand what good and effective risk management looks like so that they can provide assurance to the Board and management. This assurance must focus on both the processes being used and also the 'framework' present for its implementation and continual improvement.

IIA should therefore be closely involved in the development of any global standard for risk management but should not create its own.

As an aside, it is unfortunate that the IIA did not take a more prominent role in the development of ISO 31000. It could have been a major contributor to the working group as other sector based organizations were.

[Frigo/Anderson] No, there is a need for good frameworks, but similar to control frameworks, you could have more than one. This is probably best left with individual countries and their respective standards setters in each respective country.

IIA’s role should be as an advocate, giving input and perspectives to standards setter. In some ways similar to its involvement on COSO, active and at the table.

[Sobel] I think it makes a lot of sense to have globally accepted ERM principles, but I am not convinced there needs to be a single, globally accepted framework. I believe ISO 31000 does the best job of providing Definitions and laying out the Principles of effective ERM. I also believe the Framework and Process make sense, but we don’t need to imply that other ways won’t be effective as well. I believe it should be adopted globally, and the mechanics of how to implement it can be developed from there.

I agree with what others said: It’s not The IIA’s role to promulgate standards or frameworks outside of the IA profession. The IIA should advocate through its role in COSO and find a voice within the ISO.
3. **What should the role of the IIA be with respect to the development and update of risk management (and governance) frameworks and standards? Consider both IIA global and national organizations.**

*Fraser* Does the IIA wish to be a standard setter? Is there an issue with setting standards and then auditing to them? Should the IIA be in bed with AICPA, etc? Is this too cozy? I think it is OK once a firm stance is taken on critical issues and the IIA membership understands where there are disagreements.

*Parkinson* IIA should encourage individual participation on appropriate standards-setting committees. In Australia, at least, committees are established by nominees of organisations (no one represents themselves). Then, if IIA has a number of players on committees around the world, there is the opportunity for the IIA representatives to share ideas and swap notes.

*Schanfield* Nothing substantive for me to add on this point.

*Purdy* As I've stated above, it should contribute to that development to ensure that it can fulfill its assurance role. It should not, however, lead the development of such standards.

Certainly in Australia, the IIA plays a major role in the Standards Australia and Standards New Zealand Risk Management Committee and contributes to all the handbooks and standards that are created. In particular, IIARF and Standards Australia have jointly published a handbook on 'delivering assurance' using ISO 31000:2009.

*Frigo/Anderson* Again, the IIA could be active, at the table with a perspective wherever possible. It should be an advisor but not an actual standards setter. It should stick to the IIA standards as its standards focus. Again, we see this no different than the IIA’s involvement in internal control frameworks or regulation. Be active, provide input, be an advisor to the groups who are setting the standards. Then be proactive in helping the IIA membership understand and apply the standards.

*Sobel* I agree with what’s been previously stated. The IIA must be a strong voice and advisor in risk management and governance discussions, but risk management standards and frameworks extend beyond the IA profession and should be left to others to formally promulgate.
4. Is the role of internal auditing in risk management adequately defined and is IIA guidance sufficient (Standards, Practice Advisories, Practice Guides, Position Papers, etc.)? Consider (a) how internal audit can provide assurance and consulting services related to risk management, (b) how internal audit can make use of the organization’s risk management process, and (c) the role of the CAE in leading risk management functions in addition to internal audit.

[Fraser] IIA guidance on the role of internal auditors with ERM was well done, i.e. the famous fan showing three categories of roles. No need to change that. The IIA published several good research books/papers up to about five years ago and then stopped.

While the paper above is generally adequate, it should emphasize that where the CAE has accountability for ERM (e.g. in smaller organizations), then:
- Staff involved should not be the same, i.e. auditors should not be doing ERM, workshops, etc. and risk staff should not be doing audits.
- The role of ERM should be only of the facilitation type, i.e. the CAE should not be doing deals, approving transactions, etc.

[Parkinson] Yes. There is quite a lot around. There is also a joint IIARF/Standards Australia publication on delivering assurance using ISO 31000. This (will) provide guidance on (a) and (b).

[Schanfield] The role of internal auditing seems to be reasonably well defined.

[Purdy] The 'fan' diagram produced by the IIA in the UK seems to summarize the respective roles of management, IA and risk management professionals. Clear segregation of roles is essential to prevent conflicts of interest and to preserve the integrity of the assurance activities

a) See my comments above and those of Mike aside on HB 158:2010.
b) See my comments above.
c) I have witnessed some very difficult situations that severely compromise the independence of audit if the CAE also leads the risk management function. Also, at a practical level, the risk management function is concerned with supporting management and facilitating the integration of risk management into decision making processes. This conflicts with assurance and often requires skill sets that are not normally required or developed in auditors. Conversely, as risk management professionals are primarily change agents, they cannot fulfill that role if they are required to act as assurance providers or if they respond to a CAE. The best possible solution is if the auditor and the risk manager are good friends; they work together with mutual respect but respond to different leaders in the organization.

[Frigo/Anderson] While the IIA has produced a significant amount of material on the topic, there is still major confusion and uncertainty in many internal auditors about their role relative to risk management.

For example, Dick did a recent webcast for the IIA on this topic and received a significant number of questions, a good number of which dealt with this question of internal audit and its role. We believe the IIA has to hit this issue head-on. The standards are still confusing to people and need more clarification. The IIA should also consider some specific interpretation of application of the standards for situations where the CAE is also the CRO or has the risk function reporting to them on a permanent basis. This is the area we feel the IIA should focus on, not specific risk frameworks.
I am also a fan of the “fan” (pardon the pun), and agree that The IIA and IIARF have published a lot of good theoretical guidance about the “desired state” as it relates to internal auditors. However, I agree with Dick and Mark that the desired structure, both from an organizational and responsibility standpoint, is not always obtained. I think more specific guidance is necessary to help articulate what to do when the CAE and others in the IA function take on management (i.e., risk management) responsibilities.

Toward that end, The IIARF has just approved a project for Kurt Reding (Wichita State) and I to write a book titled *Enterprise Risk Management: Achieving and Sustaining Success*. We plan to cover IA’s role in the implementation of ERM as well as the ongoing assurance role. I know we’ll need to liaise with the Internal Audit Standards Board and the Professional Issues Committee to make sure the book aligns with the current standards and guidance already, as well as anything new to be promulgated by The IIA. I would like to reach out to this group for insights on how it’s working in real life to make sure we don’t get too theoretical in the book.
5. What research should the IIA’s Research Foundation commission relating to risk management?

[Fraser] There is tons of research needed. Whether this should be done by IIA or others (e.g. academics) is debatable. There is a lot to go around and the IIA membership provides fertile ground for access to practitioners.

[Schanfield] How to conduct a proper risk assessment from cradle to grave- with the 20 or things of importance that would go into conducting such a review following the ISO 31000 guidance (identification of events, analysis of such events for their significance, likelihood and timing and evaluation).

The second area is how to conduct an assessment of adequacy of a company’s risk management system. Such guidance does not exist in the context of a comprehensive internal audit program or if it does, I have not seen it.

The third area is in providing stellar training modules to Boards of Directors in risk management practices. These thoughts carry through to education section below.

[Purdy] This should focus only on the assurance role. In other words, how auditors can use the output from the risk management process and how they can audit the process and the framework.

In fact, that is what the joint IIARF/Standards Australia handbook covers.

Most importantly, the IIARF should not attempt to re-invent the wheel on risk management. It must use concepts and terminology that are consistent with international risk management standards and ISO 31000:2009, in particular.

[Frigo/Anderson] This is needed at several levels:
- Practical research on how to do better risk assessments, including assessing and identifying emerging risks.
- Risk management practices; maturity levels, approaches, information that can be used by internal audit to assess the adequacy of their organization’s risk management practices.

Note: Risk Management has been a priority research topic in 2009, and 2010-2011.

[Sobel] As indicated in my answer to the last question, I think the IIARF-sponsored book will help update the thinking on IA’s role relating to ERM. I also reinforce Dick and Mark’s comment that The IIARF has risk management as a priority research topic, although I’m not aware of any substantive research submissions at this time. Finally, I think the Standards Australia Handbook, that’s co-branded by The IIARF, will help get the guidance in that publication out to a wider audience.
6. Does the IIA provide appropriate education services on risk management?

[Fraser] It probably does a basic job given the current level of knowledge, although I suspect that few organizations do a good job currently. I read most of the brochures and there is a lack of depth, e.g. nothing on how to run good risk workshops, how to allocate resources based on risk, how to develop risk tolerances – all prerequisites for ERM. The real challenge is that there are only about ten (or less) people in the world (that I am aware of) who get part or most of ERM right, i.e. Kloman, Beaumont, Purdy, DeLoach, Mikes and a few others if I thought long enough.

[Parkinson] I think John is basically right here - although I would add a few others that I have worked with: Cooper, Cross, Knight. I am sure there is a handful in every country. A handful may be all that is needed, if their skills are leveraged properly.

[Schanfield] See above three key areas where I believe the IIA focus needs to be. If we can do these three things well, we will be providing stellar services.

In addition, the IIA should be establishing contacts/ties with the leading academic institutions where resident risk management gurus reside, such as Anette Mikes from Harvard, Kunreuther from Wharton, Arielly from Duke, Shiller from Yale, Lo from MIT- just some examples.

[Purdy] I and my colleagues in Broadleaf and in Standards Australia/Standards New Zealand try to do as much as we can. However, the risk management profession itself is not very good at this. Also, there are few recognised and broadly based tertiary courses for risk managers. Certainly in this part of the world, risk people learn their trade 'on the job' and as a consequence there are often problems of inconsistency in interpretation and implementation.

As an example, I'm running at 1/2 day workshop for the IIA in relation to the assurance of risk management in government organizations next month. This is well subscribed.

[Frigo/Anderson] Two overall areas:
- Risk management, how is it done, how to run it or audit it, more on how to do it.
- Education on risks and risks assessments. What works, what lessons are to be learned from the recent crisis, etc.

[Sobel] This is a tricky question. I think The IIA needs to provide basic education on ERM concepts and sufficient education on how to provide assurance related to ERM, both of which are important to comply with the Standards of the profession. But anything more advanced is probably best conducted by other organizations (although I’m not sure there are any out there that have the infrastructure and experience to conduct such training). I think this issue is one that’s best addressed further down the road, once the recommendations from this Summit are acted upon and the ERM book I referred to is published. Otherwise, we may see training that doesn’t address the current thinking related to this topic.
7. What advice would you provide the IIA as a member of the COSO organization? Is there a specific direction it should advocate COSO take with respect to any of the COSO frameworks or guidance?

[Fraser] First, update the 1992 COSO internal control framework. Second, retract the 2004 COSO ERM framework and come up with something practical, succinct and relevant based on ISO 31000 concepts. I do not suggest waiting for ISO’s attempt at this as it would likely take too long, will be limited by the need for consensus and there is currently a vacuum on ERM and people are starving for help.

[Parkinson] I would be prepared to state that given its purpose and its date, COSO 2004 was an appropriate document. The world has moved on since 2004 and it is time for a rethink.

[Schanfield] COSO needs to align with the ISO framework and stop producing documents which in the end analysis provide little value. COSO should be represented by a comprehensive team from most professional groups and not just the five groups listed in the framework. The only one of the four COSO documents of value is COSO III – Internal Control Financial Reporting for smaller entities published in 2006. COSO I serves as a good research document but is already stale. COSO II on ERM needs to be tabled. There is too much work to do to rewrite it. COSO IV on monitoring also provides little value. The document could have been written in 20 pages and should have focused on four key aspects of monitoring gleaned from ancillary ISO materials- namely internal audit’s role, the Board’s role, embedded key risk indicators as part of the information management system and lastly line management reviews. There was no need for another several hundred page document.

[Purdy] Disassociate itself from the COSO ERM framework. It is out of date, seriously flawed and leads to poor risk management and poor governance practices.

There is a major danger here if COSO tries to revise the ERM framework in the light of ISO 31000. There is an almost irresistible temptation to produce yet another inconsistent standard with inconsistent definitions and approaches. And why does the US or the world need yet another standard?

Re-inventing the wheel to produce son of COSO ERM will not help anyone in the world and I doubt if COSO can marshal the breadth and depth of experience that ISO was able to.

Undoubtedly IIA must now engage fully with the ISO standard making processes. A new standard to support the implementation of ISO 31000 is about to be discussed by the management board of ISO and IIA must be part of its development. Also, as ISO 31000 will itself be reviewed and revised within 2 years, IIA must play a central role in that process.

[Frigo/Anderson] As indicated, COSO needs to continue to develop practical materials that can be put in use. We don’t see a need for them to try to develop a revised framework, it’s more how to apply the concepts and how can application take advantage of lessons learned and developments since 2004. Again, practical application is needed and developed in a way to help senior people move up their learning curves on risk and risk management. They need to take advantage of what people have learned and are doing, for example our earlier comment on risk appetites; people aren’t starting there.

[Sobel] This is where I diverge a bit from my esteemed colleagues. As I stated in my answer to Question #1, I believe there is some good stuff in COSO ERM, albeit buried among a lot of words in an overly long document. Here are my recommendations for COSO:
1. Start by acknowledging and endorsing the Definitions, Principles, Framework and Process contained in ISO 31000:2009. I’m sure there will be some quibbling with small parts of the standard, but this is not the time to wordsmith. I think ISO 31000 is fundamentally sound enough and everyone can support it for now; let’s get the U.S. broadly aligned with the rest of the world.

2. Commission a project to cull out relevant and useful information from COSO ERM and map it to ISO 31000. Less is probably better here since bifurcating COSO ERM into the ISO Framework and Process areas will probably not be widely embraced. Rather, thoughts and guidance that truly supplement ISO 31000 should be identified and mapped. This project should include people from outside the US, and outside the public accounting profession.

3. Identify gaps where there is currently no good guidance for key ISO 31000 areas. This can be done as part of the project mentioned in #2, but would likely result in new projects to fill those gaps. This step should also consider other meaningful research and publications (e.g., the NACD Blue Ribbon report that I referenced before).

4. Establish a schedule to develop white papers or knowledge briefings that leverage off of #2 to provide focused guidance on key Framework or Process areas. This should be coordinated with ISO, and perhaps even led by ISO to ensure the output is globally accepted.

5. Officially retire COSO ERM as all of the good and relevant stuff will have been culled out and put in the deliverables in #4.

By the way, I may be alone with this opinion but I actually like the cube. I understand the comments and complaints that others have made about it, but it’s the only visual depiction I’ve seen that effectively reinforces that the ERM process must apply across all types of objectives. Maybe there’s a better way of depicting it, but I’ve gotten a lot of traction in presentations or by pulling the cube off my desk and describing the concepts by pointing to one of the key sides (the Objective types on the top of the cube and the eight Components on the front; I don’t spend much time on the Organizational types on the side). Perhaps we can figure out an improvement, but I’d like to make sure we still have something that visually illustrates some of these key concepts.
APPENDIX

Professional Associations and Organizations Promoting Risk

- ACFE (Association of Certified Fraud Examiners): fraud oriented risk
- AICPA (American Institute of Certified Public Accountants): accounting oriented
- AIRMIC
- ALARM
- Canadian Institute of Chartered Accountants
- CAS (Casualty Actuarial Society): insurance oriented
- Conference Board of Canada - Karen Thiessen
- Conference Board of US - Ellen Hexter- Consultant
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
- GARP (Global Association of Risk Professionals): finance-oriented but probably the world's largest
- IIA (Institute of Internal Auditors): an internal audit focus; some governance and some risk
- IRM (Institute of Risk Management): started in insurance, shifting towards RM; in London
- IRMI
- ISO (International Organization for Standardization): creator of ISO 31000
- NORMAC (Nonprofit Risk Management Center: focus on nonprofits
- PERI (Public Entity Risk Institute): focus on governmental bodies
- PRIMA: education area
- PRMIA (Professional Risk Managers International Association): finance-oriented; 2nd largest
- RMA (Risk Management Association): oldest; credit-risk; first name was Robert Morris Associates
- RMIA (The Risk Management Institute of Australasia)
- RIMS (Risk & Insurance Management Society): heavily insurance oriented; prior name was
  American Society of Insurance Management; see also AIRMIC in London and IFRIMA, its
  international counterpart
- SOA (Society of Actuaries): insurance oriented
- SRA (Society for Risk Analysis): public-policy, health & environment oriented; formed 1980
- The New Zealand Society for Risk Management