

PO Box 501
DICKSON ACT 2602
Australia

13 January 2012

Personal Submission – Comment on 2011 Draft Internal Control—Integrated Framework

While much of the content of these documents is valuable, there are two critical (perhaps fatal) weaknesses:

- The documents ignore the substantial development in risk management theory that has taken place since 1992, and
- The documents place emphasis on reporting at the expense of performance (operation or compliance).

The documents make a false dichotomy between risk and opportunity – the true dichotomy is hazard and opportunity – and equate risks with events. These issues are addressed in the detailed submission (Attachment B).

Organisations must address and can influence risks that originate outside them. An internal control framework must, therefore incorporate mechanisms for this. It is also not appropriate to exclude issues such as strategic planning or determination of attitude to risk from consideration – there is no logical difference in scope between risk management and internal control. The framework, as articulated, encourages isolationist thinking; separating internal control from Enterprise Risk Management inhibits the evolution of both.

It is also disappointing to see that the process model of an enterprise that was one of the more powerful ideas in the 1992 documents (providing a taxonomy for process and risk analysis) is not included in the proposed framework. Including this model may have made discussions about scalability and aspects such as Information and Communications Technology (ICT) more easily handled.

I commend the attached submission to your attention



Michael J A Parkinson CIA CRMA CISA CRISC

Encl: Attachment A – General Questionnaire
Attachment B – Detailed Submission
Attachment C – Biographical notes

Attachment A – Solicited Responses to Exposure Draft

General Questions

1. Are you a member of one or more of the COSO organizations?	Yes – Institute of Internal Auditors
2. Are you responding on behalf of yourself or an organization or company?	Myself
3. Where do you reside?	Australia
4. Where within your organization do you apply the COSO Framework?	Not explicitly, but by implication, as follows:
• Compliance activities	<input checked="" type="checkbox"/>
• External financial reporting	<input checked="" type="checkbox"/>
• External non-financial reporting	<input checked="" type="checkbox"/>
• Internal management reporting (financial or non-financial)	<input checked="" type="checkbox"/>
• Internal control reporting	<input checked="" type="checkbox"/>
• Internal audit	<input checked="" type="checkbox"/>
• Operations activities	<input type="checkbox"/>
• Other	<input type="checkbox"/>
• We do not use the Framework at this time	<input type="checkbox"/>

Overall Impressions on the Framework (answered on a scale of 1 [poor] to 5 [good])

5. The updated Framework will help strengthen an entity's systems of internal control	3
6. The updated Framework is internally consistent and logical	2

7. The updated Framework is written in a manner that is understandable and provides ease of use	2
8. The updated Framework is applicable to organizations of varying legal structures and sizes, and operating in various geographies and industries	4
9. The updated Framework will impose additional burdens on entities' reporting on internal control—e.g., reporting on internal control over external financial reporting based on Sarbanes–Oxley Act of 2002 (SOX) requirements	Cannot comment in relation to SOX. In my jurisdiction this seems unlikely.
9.a If you believe that there is an additional burden, is the change appropriate? If not, why not?	

Questions on Specific Areas of Interest (answered on a scale of 1 [poor/no] to 5 [good/yes])

10. Compared to the 1992 framework, the updated Framework creates a higher threshold for attaining effectiveness of internal control	3
11. The 17 principles set out in the updated Framework are a complete set of principles	1
12. The 17 principles with related attributes are helpful in describing important considerations of an effective system of internal control	2
13. There are necessary changes to the principles	5
14. An entity can conclude that it has effective internal control if one or more of the 17 principles are not present and functioning	1 – but neither can it so conclude if all are present as some principles seem to be missing.

<p>15. The updated Framework appropriately expands the reporting objective category (i.e. internal and external reporting, financial and non-financial reporting)</p>	<p>2 – This depends on what is meant by ‘expands’. The analysis is appropriate, but it is still only one category of objectives which seems to have been given more than its share of attention.</p>
<p>16. The expanded reporting objective, and the manner in which this objective category is presented in the Framework, does not diminish our ability to apply the Framework when reporting on internal control over external financial reporting</p>	<p>1 – No, it does not.</p>
<p>17. The updated Framework provides an appropriate balance of reporting, operations, and compliance related approaches and examples</p>	<p>4</p>

Summary

<p>18. Are there any other general comments that you would like to provide</p>	<p>See Attachment B</p>
--	-------------------------

Attachment B – General Response to DRAFT of *Internal Control – Integrated Framework*

1 Strategic Issues

1.1 ***The documents ignore the substantial development in risk management theory that has taken place since 1992.***

The authors have defined risk as “the possibility that an event will occur and adversely affect the achievement of objectives”. This definition ignores the reality that uncertain circumstances can have positive outcomes – it is a 1980s view of the world. This unbalanced start has adverse consequences throughout the framework: it means for example that internal controls are considered as existing solely to eliminate undesirable events¹, whereas internal controls also exist to promote desirable ones. The result of this approach is that para 279 needs to take an inconsistent stand in order to introduce “standards of conduct” as controls.

Risk is thought of as an event, whereas it is in fact a condition associated with an objective. The existence of an objective means the existence of risk. A risk cannot “occur”; events “occur”. A potential event has a risk profile – there is a range of possible consequences of an event and each has its own likelihood – controls exist to skew this profile to a desirable form.

Hence the statement in para 9 of the Executive Summary that “confidence” is obtained “by mitigating risks to acceptable levels” starts the document on the wrong foot – “confidence” is obtained by “maintaining risk within acceptable levels”. While this might seem to be quibbling over semantics the distinction is very important.

The desire to preserve as much as possible from 1992 seems to have led to the authors overlooking potential structural improvements. A careful study of ISO 31000:2009 (or any of its predecessor documents) should have led to a minor (but important) reworking of the structure. (See 2.2)

1.2 ***The documents place emphasis on reporting at the expense of performance (operation or compliance).***

It is not the primary purpose of an organisation to produce accurate reports. The purposes implied in the definition of internal control are all important, but, surely, achievement of objectives and compliance with the law are the dominant purposes and only then is accuracy in reporting an issue.

¹ See Executive Summary, para 23: “Control activities are the actions established...to mitigate risks. ... They may be preventive or detective in nature...”

The documents seem to be written from the perspective of an accountant or auditor and not from the perspective of a Board member or owner.

2 Framework

2.1 General Comments

The framework document is extremely long. At 150 or more pages, it is more a discourse on a framework than an exposition of one. A great deal of the material, while of some interest, is not appropriate in a framework document. The summary pages for each component, in which principles and attributes are outlined, help rectify this and, I would suggest, might make a good stand-alone document.

The framework ought to be scalable. It is stated to be applicable across all organisations and at any level, but it does not quite work. The responsibilities assigned to a Board in the framework do not all scale to those charged with governance in a subunit. A little more consideration of the functional governance role as distinct from the organisational governance role may be of value.

2.2 Structure

As will be discussed below, it is my view that the framework has structural faults. I would suggest the alternative in Figure 1. Where the proposed principle corresponds with an existing principle, the current number is indicated.

Figure 1 - Proposed Alternative Framework

Component	Principle	Current #
Context	Identifies internal and external factors – history, values, market and the competitive and regulatory landscape	
	Demonstrates commitment to integrity and ethical values	1
	Exercises oversight responsibility – independence from management and oversight of internal control.	2
	Establishes structure, authority and responsibility	3
	Demonstrates commitment to competence	4
	Enforces accountability – hold individuals accountable for their risk management	5

Figure 1 - Proposed Alternative Framework

Component	Principle	Current #
	responsibilities.	
	Specifies relevant objectives – with sufficient clarity to enable the identification an assessment of risks	6
	Determines attitude to risk – develops criteria for assessing risks and determines the nature and level of risk that may be tolerated	
Risk Assessment	Identifies and analyzes risk – as a basis for determining how they should be addressed	7
	Assesses fraud risk – consider the potential for fraud	8
	Identifies and analyzes significant change – identifies and assesses changes that could impact risk	9
Control Activities	Selects and develops control activities	10
	Deploys through policies and procedures	12
Information and Communication	Uses the best available information	(13)
	Communicates internally	14
	Communicates externally	15
Monitoring Activities	Conducts ongoing and/or separate evaluations	16
	Promotes improved performance	(17)

2.3 **Detailed Commentary against the Draft Framework**

2.3.1 *Control Environment*

On the principle that before one can design good internal control or undertake an audit one needs to understand the organisation, the issue of organisational context needs significantly more than the single paragraph (116) assigned to it. Comments in para 282 reinforce this.

In para 69 the *Framework* document indicates that some aspects of importance (“setting the overall level of acceptable risk ... setting risk tolerance levels”) will not be addressed as part of the framework. This has the potential to lead to these critical aspects of control not being considered by those who follow the framework. Issues like-

- “the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- “key drivers and trends having impact on the objectives of the organization; and
- “relationships with, and perceptions and values of, external stakeholders”²-

all need to be examined before planning, implementing or reviewing and organisational activity. This has long been part of internal and external audit methodology; it is explicit in management texts.

Importantly, the suggestion that internal control stops at the boundary of the organisation has the potential to limit organisational thinking. In a highly interconnected economy the risks in the environment need to be managed just as do the risks in the organisation. Organisations find it appropriate to develop contingency plans in relation to external events (eg failure of a supplier) and frequently believe it appropriate to lobby for changes in the regulatory environment.

The framework should explicitly address the analysis of these external factors (“external context”). Similarly there is a range of internal factors worthy of consideration – many of them are explicitly covered, but others need to be drawn out. Principles 1 to 5 would be regarded as part of “internal context”; their importance in this framework warrants explicit treatment. Para 282 has discussion about context – this is important material and could be included in a new principle.

Para 408 specifically excludes “strategy setting” from the scope of internal control. This is quite clearly an internal process and should be addressed as part of the control environment.

In particular, the organisation’s attitude to risk should be addressed in the framework. This is a necessary pre-requisite for the risk assessment component and is a strategic level activity.

The determination of objectives is also a necessary pre-requisite to risk assessment – it is not a part of the process. The principle is misplaced.

Principle 2

This principle is amenable to misinterpretation. As written it can suggest that management is to be demonstrated as independent. This it must not be: it must remain subordinate. Better wording would be “...board of directors demonstrates independence *from* management...”

² Quoted from ISO 31000:2009.

Principle 5

Organisations ought to hold individuals accountable for their management of risk. Internal control is, admittedly, more than simply following the rules – it is about exercising judgement – but the management of risk does imply the need to be alert to new risks or changes in risk levels. An individual needs to be held accountable for the way they respond to these things as well.

Our colleagues in PricewaterhouseCoopers (and others) discuss “risk-aware organisations”³: organisations where officers and employees go beyond following the rules and are capable and empowered to react to the real world. This concept needs to be embraced.

2.3.2

Risk Assessment

As indicated in the introduction to the framework (para 10), there are advantages in establishing a common set of definitions and concepts. This applies equally in risk management and in internal control. Indeed the *Executive Summary* para 42 states that “to the extent diversity in concepts and terminology is eliminated, all parties benefit”. Since the initial *Internal Controls Integrated Framework* (1992), risk management professionals have, in an international effort, developed a well accepted terminology for risk management concepts. These are outlined in ISO Guide 73:2009 and should be used in preference to other terminology. Perpetuating a common term rather than using a correct one is not appropriate in a framework document.

Principle 6

As indicated, this should be in the first component.

Principle 7

The labelling of risks as occurring at “entity level” or at “transaction level” is a little at odds with the cube (and with the COSO ERM cube). Risks will be associated with processes rather than transactions: while a transaction will have an objective (and therefore have risks) a process is likely to comprise a series of related and similar transactions that would ordinarily be considered as a group. Internal controls are therefore incorporated into processes so that they may affect all incorporated transactions.

There is a need to distinguish between the magnitude (and therefore the significance) of a risk and other factors which may influence the manner in which it is treated. The magnitude will affect the priority with which it will be treated – other factors may affect the controls applied.

Magnitude is expressed solely in terms of consequence and likelihood. “Velocity” and “persistence” – which are not well distinguished in this document – may be of relevance when considering the nature of risk treatment to be applied.

³ See, for example http://www.pwc.com/en_GX/gx/risk-regulation/pdf/get-up-to-speed-3.pdf.

It is also necessary to distinguish between a risk and an event. An event may cause one or a number of consequences. Each consequence has a likelihood and the purpose of risk management is to address the likelihoods of each potential consequence. This *might* mean addressing the likelihood of the event - but this may well be beyond management capability – it *will* mean adjusting the risk profile to the maximum benefit of the organisation. Even if an event is guaranteed, the outcomes may not be – risk remains. It must be remembered that many of the potential consequences of an unpredictable event may be advantageous.

The term inherent risk is interpreted in widely varied manners, as a scan of relevant literature would reveal. Even when the definition in the framework is applied, managers are unlikely to be familiar with the concept. Managers think in terms of current risk and residual risk (risk after proposed treatment). It would be best to remove all reference to “inherent risk” from the framework.

Principle 9

The critical point to make here is that changes should be monitored and assessed to determine whether the risks have changed. The internal controls serve the risks, so the risks are the drivers of any need to amend control processes.

The changing risk profile may include emerging opportunities that require treatment to capitalise or they may, as is suggested, indicate an emerging problem that needs mitigation. The two-sided aspect of risk (ie good and bad) needs to be acknowledged. (para 271)

The extensive discussion at para 274 is consistent with these suggestions although it would be strengthened by the inclusion of some up-side considerations.

2.3.3 *Control Activities*

Principle 10

The organisation selects controls to maintain risk at an acceptable level.

This is completely consistent with the COSO concept of “reasonable assurance” – although quite at variance with the concept of “reasonable assurance” that is used in relation to assurance reviews by independent auditors (cf GAGAS and IAASB standards). The COSO concept of “reasonable assurance” that managers want in relation to their processes has been hijacked by auditors and assurers for use in a technical sense in relation to the reliability of their opinions. It may be time for COSO to consider dropping the term.

We could eliminate the phrase to avoid this double use: “reasonable assurance of achievement of objectives” would become “maintain risks at acceptable levels” or, more strictly, “maintains risk within levels determined by the organisation”.

This superficially minor change conceptually also permits that outcomes can be positive.

The information processing objectives (para 287-287) need to be aligned with the quality of information characteristics (para 346). The types of control do not seem to have a place for transaction counts, lodgement times, completion times, customer satisfaction reports and other performance related information.

Principle 11

The inclusion of this is unnecessary. There is nothing conceptually different about information technology risks and information technology controls. The differences are technical and will be covered by the principle of commitment to competence (Principle 4). It is true that ICT is pervasive: but so is finance; so is HR management; so is employee safety.

ICT is a process component of the organisation. If the enterprise model had been retained, this would have been recognised. Principle 11 is a discussion about a process component and might form the basis for a supplementary document but it does not deserve inclusion in the framework.

2.3.4 *Information and Communication*

Principle 13

The information should be the “best available” rather than simply “relevant”.

This recognises that information is expensive to obtain and may be indicative rather than definitive. An organisation cannot necessarily wait or afford to have full knowledge but ought to take reasonable effort to get the information necessary before making decisions.

The quality of information characteristics (para 346) need to be aligned with the information processing objectives (para 287-287).

Principle 15

Inbound communication should also include the monitoring of markets, economic trends, the performance stability of key suppliers and customers, and of political and social stability. Similarly, outbound communication would include political lobbying.

2.3.5 *Monitoring Activities*

The component should specifically address the role of supervision. It would be easy to read supervision out of the monitoring component, yet it is an intrinsic component of ongoing evaluation.

Missing from this component is the concept that review has an objective of improving performance; this could be incorporated into existing Principle 17. Given the tendency of this document to draw out those matter related to fraudulent reporting, it may be more appropriate to introduce this as an additional concept.

Principle 17

“Deficiencies” exist when the current risk is unacceptable (cf para 81). An auditor may, however, recommend improvements in process that, for

example, make the controls more efficient or modify an acceptable risk in a cost-effective manner.

2.3.6 *Limitations of Internal Control*

As described in this section “Management Override” (para 412) and “Collusion” (para 414) are nothing more or less than fraud. They should be addressed at Principle 8.

Attachment C – Biographical Notes

Michael Parkinson CIA CRMA CISA CRISC is an internal auditor of more than 25 years experience. After 10 years in Information Technology and Government Finance he became an IT internal auditor in the early 1980s. He has worked as a government internal auditor for the last 25 years; the last 15 years as a service provider. Whilst working as a government employee he was the Chief Audit Executive of three different government agencies. Michael is currently a Director in the government services practice of KPMG Canberra.

Michael joined the Board of the Institute of Internal Auditors - Australia (IIA-Australia) in 1996, was elected Vice-President in 1998 and became National President of IIA-Australia in 1999, serving until 2001. He continued to serve on the Board of IIA-Australia until 2005. From 2001 until 2004, Michael worked as the Host Committee chair for the IIA International Conference held in Sydney in 2004 and served on the International Conference Committee during that period.

In 2005, Michael joined the IIA Global International Relations Committee and was appointed its chair in May 2007. Michael was the Australian nominee Director on the Board of IIA Global for the period 2008-2009, International Secretary 2009-10 and Vice Chair (Professional Services) 2010-11.

During 1994-97 and 2000-01 Michael represented Australia and New Zealand as the International Vice-President of the Information Systems Audit and Control Association (ISACA). During 2003-2006 he also served as the Chair of the ISACA International Education Board.

Michael currently serves as chair of the Standards Australia OB-007 Risk Management Committee. This committee participates in the development of international (ISO) standards and guides on risk management. Michael is a delegate to the ISO committee. OB-007 also prepares guides published within Australia and New Zealand: HB 158 *Delivering Assurance based on ISO Standard 31000 Risk Management-Principles and guidelines* was one of these.

In 2007 he was presented with the Bob McDonald Award for contribution to the profession.

He served as the Honorary Secretary of the Asian Confederation of Institutes of Internal Auditors (ACIIA) for 2006-07 and as President of ACIIA from September 2007 to November 2008.

Michael has been extensively involved in technical publications issued by IIA Australia and, in 2006-07, worked with the Global Vision Taskforce to revise the Professional Practices Framework. He currently serves on the International Internal Auditing Standards Board.