

Notes and Recommendations (at end) on COSO's December 2011 Exposure Draft

Andrew Chambers

The five COSO bodies first got together to sponsor the Treadway Commission which in 1987 recommended that US companies should report publicly on the effectiveness of internal control. Concern by directors and others about this recommendation led to COSO reconvening and inviting Coopers & Lybrand's New York office to research the meaning of internal control, how its effectiveness could be assessed and how it could be reported upon, resulting in COSO's 1992 *Internal Control – Integrated Framework* publications.

By chance rather than by initial intent, COSO therefore became a standing committee. Significantly COSO published their *Enterprise Risk Management – Integrated Framework* in 2004, to which we also refer later in this Note.

Importance of COSO for accountants and auditors

Three of the five COSO bodies are professional accounting bodies. *Internal Control – Integrated Framework* is widely used for Sarbanes-Oxley s404 purposes, which involves in-house accountants and external auditors of US quoted companies. So it could be construed as appropriate for accounting bodies to respond to COSO's December 2011 consultation on revising, for the first time, *Internal Control – Integrated Framework*. The other two COSO bodies are the association of US accounting academicians (American Accounting Association) and The Institute of Internal Auditors. Over the years the latter has been the principal driving force behind COSO.

The SEC rule on CEOs and CFOs assessing and certifying to the effectiveness of internal control over financial reporting, *per* s404 of Sarbanes-Oxley (2002), requires that they use a recognised internal control framework. The SEC stipulate the criteria which would determine whether a framework were acceptable to use for this purpose, and they identify three frameworks as being acceptable – COSO, CoCo (Canada) and Turnbull. Most use COSO (1992) since SOX is a US reporting requirement.

Interface with COSO's 2004 Enterprise Risk Management Framework

A key paragraph in the COSO 2004 *Enterprise Risk Management – Integrated Framework* reads:

'Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in *Internal Control – Integrated Framework*. Because that framework is the basis for existing rules, regulations and laws, that document remains in place as the definition of and framework for internal control. While only portions of the text of *Internal Control – Integrated Framework* are reproduced in this framework, the entirety of that framework is incorporated by reference into this one.'

Clearly it would be acceptable for COSO's *Enterprise Risk Management – Integrated Framework* to be used for SOX s404 purposes, but most use just the *Internal Control – Integrated Framework*. Indeed, a failing is that s404 compliance and attestation work too often focuses almost exclusively on 'control activities' and insufficiently on COSO's other four components of internal control – see below.

Internal control as a large part of risk management

In the above quotation COSO disposed of the view that 'risk management' is part of 'internal control' – a view that had been encouraged by 'risk assessment' being one of the five essential components of internal control in COSO's internal control framework (see 'Rubik cubes' below). Rather, internal control is seen as being a large part of risk management which in turn is an important part of an entity's internal governance processes, as illustrated in this diagram:

Figure 1 The relationship between governance processes, risk management and internal control



We do not yet have a COSO framework on internal governance processes. If one were to be developed it would likely require inputs from other bodies in addition to COSO.

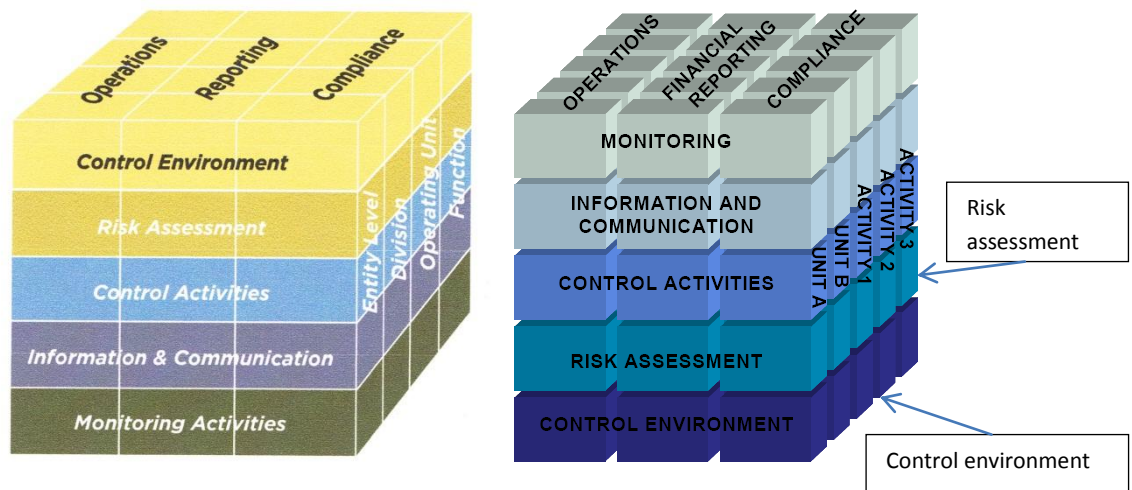
Common ground between 1992 and 2012

The definition and five components of internal control remain unchanged in this 2011 Exposure Draft, as does the famous 'Rubik cube' except for two incidental changes to the cube which don't alter its meaning but which are not without significance.

The first welcome change is that much more informative labels are used on the right face of the cube, though they still leave something to be desired as 'processes' is absent. The COSO internal control framework is appropriate for assessing the effectiveness of business processes, and so 'processes' should be there.

The second change is that the vertical ordering of the five essential components of internal control on the front face has been reversed (see below). This loses the opportunity to indicate visually that the 'control environment' (tone at the top, policies relating to control, etc) is the foundation upon which the other essential components of internal control are built, although it brings the representation in line with COSO's 2004 ERM framework 'Rubik cube'.

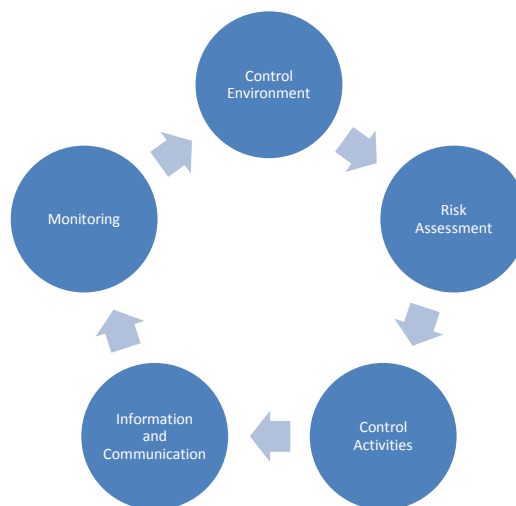
Figure 2 Proposed 2012 internal control 'Rubik cube' (left), and 1992 cube (right)



Relationship between COSO's five internal control components

COSO stresses inadequately the logical relationship between the five COSO internal control components. A diagram (and discussion thereon) such as this one (below) would be useful as it would emphasise the process character of internal control which is nevertheless present in COSO's internal control definition.

Figure 3 The process relationship of COSO's five internal control components



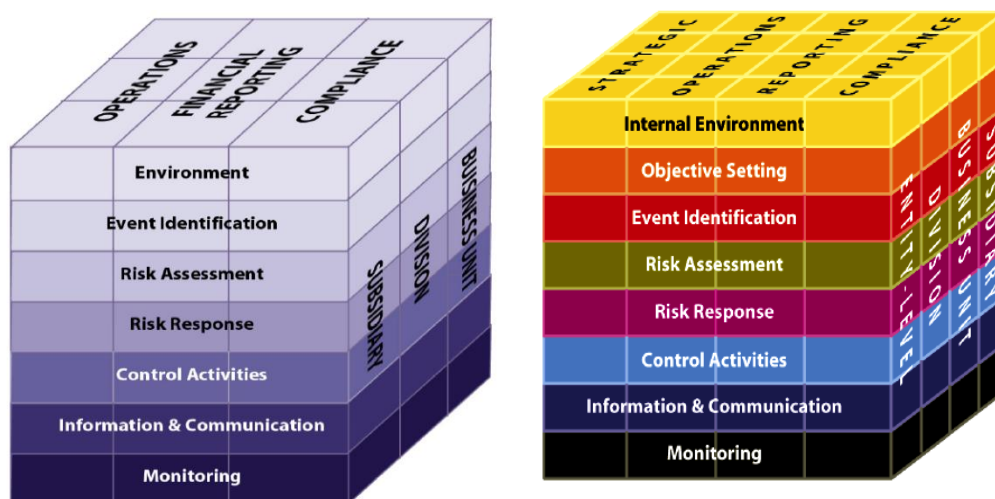
Internal control 'principles' and 'attributes'

COSO's internal control exposure draft now, for the first time, codifies the internal control concepts introduced in the 1992 *Framework* into principles' and 'attributes'. Although these are not explored in this Note, it is likely that this is the main change which should be the focus of responses to the consultation draft, due by 31st March 2012.

Making the internal control concept more robust

In the earlier quotation from COSO's 2004 *Enterprise Risk management – Integrated Framework*, COSO expressed the view that their ERM framework is 'a more robust conceptualisation' than their 1992 internal control framework. In what way(s) is it more robust and to what extent does this indicate a flaw in the internal control framework which is continuing into the proposed new internal control framework? In this context, it may be helpful to explore how the ERM framework evolved during its development. In 2001 COSO commissioned PwC's New York office to work on developing the ERM framework. An unpublished 2002 pre-exposure draft depicted the ERM 'Rubik cube' as shown below (left), which was to be revised also as shown below (right):

Figure 4 Abandoned 2002 ERM 'Rubik cube' (left) and final 2004 'Rubik cube' (right)



I remember responding to the pre-exposure draft (above left) by pointing out that risk management is important at the strategy formulation stage as some strategies are too risky to be adopted. I drew attention to GEC/Marconi as an example. I believe PwC and COSO welcomed this comment as it allowed their 2004 ERM framework to become significantly differentiated from their 1992 internal control framework. It allowed for 'strategic' to be added as a fourth objective of ERM, and this in turn suggested 'Objective setting' to be added as an essential component of ERM. 'Objective setting' on the front face of the 'Rubik cube' is the counterpart of 'strategic' on the top face. All the other components are the same in both frameworks. (The internal control framework's 'risk assessment' is split into three elements in the ERM framework ('event identification', 'risk assessment' and 'risk response' – all of which were subsumed within the single 'risk assessment' in the 1992 internal control framework. Because this was an ERM framework it was considered appropriate to give separate emphasis to each of these three elements of risk assessment.)

Rather than using the label 'control environment' the oxymoron 'internal environment' is used, presumably because this is an ERM rather than an internal control framework. The result however is that the ERM framework views the *entire* management process, including 'objective setting' through the lens of risk management.

The key issue here is that the 1992 internal control framework and its 2012 proposed revision exclude 'strategic' and 'objective setting'. So, to use COSO's wording, it remains a less 'robust conceptualisation and tool for management'. Internal control should not apply only when strategy has been adopted when it should be designed to provide reasonable assurance that strategic objectives will be achieved. Prior to strategy adoption, there should be effective internal control over strategy formulation. Some strategic options may be too risky because effective internal control over the implementation of those strategies may not be possible.

It is also conceptually unsound to exclude 'objective setting' as an essential component of internal control. This is so because to achieve high level objectives it is necessary to establish lower level objectives, and to achieve those lower level objectives calls for even lower level objectives to be set – and so on. The internal control lens which views the management process should, as with ERM, have a field of view which is wide enough to embrace *all* of the management process, including objective setting.

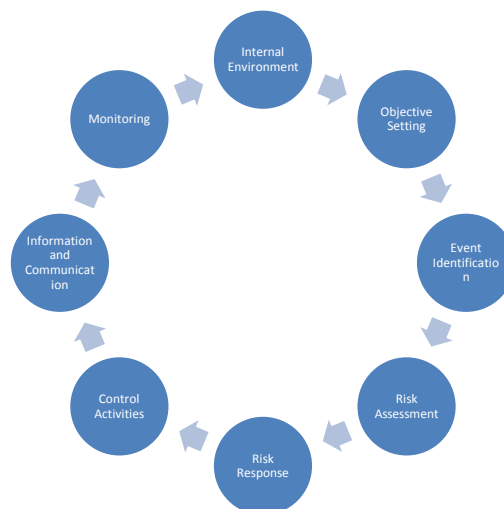
This would bring ERM and internal control into closer alignment, as they should be. Neither would this be surprising. COSO defines ERM in a way closely similar to internal control:

'Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives'

Relationship between COSO's eight enterprise risk management components

COSO's ERM Framework also had no diagram such as we suggest here:

Figure 5 The process relationship of COSO's eight ERM components



COSO's definition of internal control

Beyond that, COSO proposes to define internal control in an unchanged way:

'Internal control is broadly defined as a process, effected by the entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.'

COSO's 2011 exposure draft to some extent rectifies a 1992 perceived failure to give sufficient stress to the 'safeguarding of assets' as an objective of internal control. In 1992 this led some parties, including the US General Accounting Office, to delay their adoption of the 1992 framework until COSO had issued an *Addendum* in 1994 explaining that COSO had intended that 'safeguarding of assets' was subsumed within the objective of internal control which reads, within the definition of internal control, as the 'effectiveness and efficiency of operations'. Now COSO specifically states that operations objectives ...

'pertain to effectiveness and efficiency of the entity's operations, including operations and financial performance goals *and safeguarding assets against loss*' [italics added].

However, COSO's definition of internal control, continuing as it does unchanged, still does not refer to 'safeguarding of assets' as one of the objectives of internal control. Contrast this with the *Standards* of The Institute of Internal Auditors which, at Std. 2130.A1 itemises *four* objectives of internal control, *viz.*:

'The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.'

(The IIA Standards also give these as the objectives of risk management, at Std. A2120.A1.)

It is surprising to have this misalignment between COSO and The IIA in view of the very active involvement of The IIA in COSO's affairs and the previous concern of public sector audit and accounting bodies about insufficient stress on 'safeguarding of assets'.

Note that while COSO's definition of enterprise risk management does not itemise the objectives of ERM, it is clear that COSO's ERM Framework is aligned to their internal control framework with respect to the objectives of both.

Unlike The IIA, COSO is also deficient in omitting to state within the definition of internal control that compliance controls also have the objective of providing reasonable assurance of compliance with policies, procedures and contracts – not just laws and regulations.

Postscript

The draft *Framework* volume, at 154pps, is about the same length as the 1992 *Framework* volume. It is not clear whether COSO plans to produce an *Evaluation Tools* volume which, in 1992, was 203 pps. Similarly, COSO's 2004 ERM *Framework* volume was partnered by a 105 pps *Application Techniques* volume. There is considerable scope to improve on the 1992 *Evaluation Tools* volume.

37 PwC contributors are credited for this consultation draft compared to 5 PwC people for the final 1992 publication.

Nine recommendations to COSO

(Refer to above notes)

1. 'Processes' should be added to the right face of the 'Rubik' cube, as the COSO internal control framework is also appropriate for designing and assessing effective internal control over business processes, in addition to what is already referred to on the right face of the 'Rubik cube'.
2. Consideration be given by COSO to restoring the 1992 vertical ordering of the five components on the front face of the 'Rubik cube'. Although this would be inconsistent with COSO ERM (2004) it would restore the visualisation that the 'control environment' is the foundation upon which effective control is built and upon which the other essential components of internal control depend.
3. Consideration be given by COSO to including a diagram similar to Figure 3 to emphasise the process relationship between COSO's five internal control components.
4. To make the internal control concept more robust, along the lines of 2004 COSO ERM, add 'strategic' as an objective of internal control, since strategy needs to be developed in a well-controlled way.
5. To make the internal control concept more robust, along the lines of 2004 COSO ERM, add 'objective setting' as an essential component of internal control, since although internal control is designed to give reasonable assurance of the achievement of objectives, achieving those objectives will entail setting lesser objectives, and achieving those lesser objectives will mean that still lesser objectives must be set, and so on. So there cannot be effective internal control without the setting of objectives.
6. Add 'safeguarding of assets against unauthorised use or disposition' as a separate, fourth objective of internal control within the definition of internal control and elsewhere in the framework.
7. Add (to the definition of internal control as well as elsewhere) that compliance control is designed to give reasonable assurance of compliance with policies, procedures and contracts – in addition to compliance with laws and regulations.
8. As in 1992 COSO should develop an 'Evaluation Tools' volume or similar. It would be all the better for being put out to at least a limited exposure before being finalised.
9. To complete the trilogy, COSO consider developing a framework on internal governance processes, with inputs from other bodies additional to COSO.

Andrew Chambers
Professor of Corporate Governance

