

## Comments on COSO Monitoring Drafts

---

### Overall concerns

- Control Activities are ignored, and often identified as Monitoring.
- Risk responses, as management functions, are often called Control Activities.
- Many examples of risks are ineffective or missing controls, or impacts.
- COSO ERM is ignored
- All of internal control is looked at as about mitigating risks, rather than Risk Assessment being only one part.
- Existing management controls, like ISO, etc. are ignored.

### Exec Summary

Page 1 – It seems odd there is no mention of the COSO ERM document. The same is true for the other monitoring documents. Is ERM now an orphan?

Page 3 – This document refers to the three Internal Control Objectives (of which ICFR is one). Other COSO documents, including COSO IC, referred to those as business objectives. Is there a difference – I think so, and it should be addressed if a change from the original COSO framework is intended.

## Comments on COSO Monitoring Drafts

---

Page 5, #17 – This board-level role really should be linked to or called governance, to match the typical usage of the term governance.

### Guidance Volume

Page 3 – The footnote 6 states “The activity of correcting deficiencies may also be classified in the risk assessment or control activities component.” However in COSO IC and ERM, both responses to risks and correcting deficiencies are Management Activities, not internal controls. I believe this document continually confuses management functions or activities with internal controls, whereas earlier COSO documents were clear on the distinction.

Page 5 – This further confuses business objectives, such as profit making and strategy, from internal control objectives as referred to in these documents. It does this by referring to: “each internal control objective” and then the footnote brings in COSO’s Enterprise Risk Management — Integrated Framework, 2004, which includes strategy as an additional objective. The monitoring concepts discussed in this document can be applied equally to monitoring of “internal control over strategy”.

Page 6 – Item 17 says “This process view of the COSO Framework also shows that internal controls are developed (1) in response to one or more identified risks that affect the achievement of organizational objectives...” In prior COSO documents, responses to risks are management functions not internal controls. Does this monitoring document intend to change the original COSO framework in that manner?

Page 6 – Item 4 states: “Designing and implementing responses to the risks (e.g., internal control). ... 18. Many organizations design and implement monitoring procedures in conjunction with step #4 above.”

In COSO, this is the definition of a Control Activity, not a Monitoring function. This monitoring document continually confuses Control Activities with Monitoring – I think because it does not consider risk responses to be a management function, as did the original COSO framework.

Page 7 – under Item 2 it states “Are prioritized based on the importance of the control to achievement of the objective (i.e., the risk associated with the control’s failure), and …” This use of the term “risk” is confusing, and would be better referred to as “potential impact”. Uses continually are confused by the term “risk” so this document should clarify, rather than confuse, that issue.

Page 8 – in Item 3 “Facilitate prompt corrective actions where necessary” per the original COSO framework, these corrective actions are part of the management process, not part of internal control. It is not used incorrectly here, but this is a chance to further clarify the distinction.

Page 10 – at the top in referring to the board, other organizational initiatives, such as TQM, Six Sigma, ISO should be mentioned somewhere in the document, and this would be one place to do it. Continually ignoring the existence of those other methods of achieving objectives is damaging to the acceptance of COSO frameworks in businesses.

Pages 14-15 – The items these pages call monitoring are Control Activities in the COSO framework.

Page 16 – This Applying the Concepts example give good examples of Control Activities, not Monitoring.

## Comments on COSO Monitoring Drafts

---

Page 20 – Absolutely disagree with “Regardless, the assessment considers the importance of the risk *without* considering the expected effectiveness of internal control.” This Inherent Risk Analysis, ignoring the real world control already in place, is the single biggest driver of No Value Added work in the SOX/ICFR process. It makes the Risk Assessment process a theoretical exercise, rather than anything valid to the business. Big mistake.

Page 22 – Both these examples in 55 and 56 are Control Activities, not Monitoring. Not clearly distinguishing these two separate components of control makes this a very confusing document, when compared to the COSO definitions of prior years.

Page 25 – Same comment as above, and risk responses are management functions, not internal controls.

Page 29 – Item 67, these KRI’s and KPI’s are not monitoring, they are Information and Communication, in the COSO framework.

Page 30 -32 – Much of this information is already in internal auditing and external auditing standards, but you’ve chosen to use different words to describe the concepts. It will be confusing rather than useful.

Page 47 – this use of Risk significance and likelihood attempts to measure the impact of existing control deficiencies. That is a different use of the word Risk as a forward-looking concept in the Risk Assessment component. This will be very confusing. A better concept to use here would be Maturity Models related to internal controls.

Page 53 – Item 120 states “The ultimate goal of monitoring is met when organizations use the most efficient means possible to gather and evaluate appropriately persuasive information about the effectiveness

of the internal control system in addressing meaningful risks to organizational objectives.”

NO - risks are only one aspect of internal control. All the COSO components, including RA, relate to achieving objectives. A failure or weakness in control component, such as CE, does impact RA, but it has an impact on all objectives, not just one. So, a weak CE is a "risk" to all objectives, not just one.

Glossary-1 – In Board Monitoring, I wish you’d bring in the word governance here.

Glossary-2 – In Control Objective, this is a much different definition than is used for the COSO Internal Control Objectives (O, F, C). You should recognize the differences between entity and activity level controls, as used in the COSO framework.

Glossary-5 – Objective or objectivity. You also need to define the terms Internal Control Objective, and Business Objective here.

Glossary – also need to define the term “Risk”

### Volume III Application Techniques

Page 31 – This is an unwise example, as it confuses the term risk, with impact. “ 9. Overall, management recognizes that effective store inventory management is crucial to the organization’s operations and financial reporting objectives. As a case in point, we will follow one of those risk factors, “Inaccurate/improperly adjusted store inventory balances” (risk factor 2.b. below), through the monitoring process.” Just because someone does it this way does not mean it is a clear application of the COSO concepts. It is not.

## Comments on COSO Monitoring Drafts

---

Page 32 Item 11 – These are all “impacts of not achieving the objective” not risks. The example departs from the original COSO framework in its use of the term risk.

Page 33 Items 12-14 – these are all risk responses, which are management functions, not monitoring. This also ignores the existence of the Control Activities component of control.

Page 35 Item 16 – This sounds like a different meaning of the term Key Control from that in the draft COSO Monitoring documents.

Page 44 Item 29 states “The key for each organization is to implement internal control, including monitoring, that adequately manages or mitigates meaningful risks to organizational objectives in a cost-effective manner.” Internal controls are more than just mitigating risks – that is just the Risk Assessment and Control Activities components. The whole of Internal Control is about achieving objectives, and risks are just part of that.

Page 49 Item 16 – These are not “risks” they are just objectives with “not” in them. All these are ineffective controls. This is a very poor example, and not consistent with prior COSO IC document. The whole example is about failure of controls, not risks to achieving business objectives.

Page 50, Item 18 – I wish this would relate to a component of COSO, not just “controls” without any source.

Page 65 – all these items identified as Monitoring procedures are Control Activities in the COSO framework.