



5 April 2012

Our ref: ICAEW Rep 49/12

David Landsittel  
Chairman  
Committee of Sponsoring Organisations of the Treadway Commission

By e-mail

Dear Sir

**COSO framework exposure draft – Internal Control – Integrated Framework**

ICAEW is pleased to respond to your request for comments on the *Internal Control – Integrated Framework* exposure draft issued in December 2011.

Please contact me should you wish to discuss any of the points raised in the attached response.

Yours faithfully

Jonathan Hunt ACA  
Head, Technical Projects

**T** +44 (0) 7920 8755

**E** [jonathan.hunt@icaew.com](mailto:jonathan.hunt@icaew.com)



## ICAEW REPRESENTATION

### COSO – INTERNAL CONTROL – INTEGRATED FRAMEWORK

Memorandum of comment submitted in April 2012 by ICAEW, in response to COSO's exposure draft document on *Internal Control – Integrated Framework* published in December 2011

Contents	Paragraph
Introduction	1
Who we are	2
Introductory comments	5
Developments in the last twenty years	9
Missing elements	12
Fraud, IT and wider reporting	17
Checklist approach and the level of detail and documentation	21
Links to other COSO frameworks	25
Governance of COSO and due process	26

## INTRODUCTION

1. ICAEW welcomes the opportunity to comment on the exposure draft document *Internal control – Integrated Framework* published in December 2011 by The Committee of Sponsoring Organisations of the Treadway Commission (COSO) a copy of which was available from this link <http://www.ic.coso.org>

## WHO WE ARE

2. ICAEW is a world-leading professional accountancy body. We operate under a Royal Charter which obliges us to work in the public interest. ICAEW's regulation of its members, in particular its responsibilities in respect of statutory auditors, is overseen by the UK Financial Reporting Council. We provide leadership and practical support to over 138,000 member chartered accountants in more than 160 countries, working with governments, regulators and industry in order to ensure that the highest standards are maintained.
3. ICAEW members operate across a wide range of areas in business, practice and the public sector. They provide financial expertise and guidance based on the highest professional, technical and ethical standards. They are trained to provide clarity and apply rigour, and so help create long-term sustainable economic value.
4. This response reflects consultation with members of the ICAEW's Internal Audit Committee, which includes Heads of Internal Audit of FTSE 100 companies and academics, and some other interested parties.

## SECTION 1: INTRODUCTORY COMMENTS

5. We welcome the opportunity to comment on COSO's proposed Internal Control – Integrated Framework published in December 2011.
6. We have chosen not to answer the nineteen specific questions but to provide you with comments on a number of matters. We hope that, when evaluating all the responses, COSO is careful to balance the simple numerical, multiple-choice approach used in thirteen of the questions with the more qualitative, substantive analysis from respondents.
7. We believe that governance, risk and control are interlinked. Internal control is part of risk management which is part of the much wider topic of corporate governance. Hence risk and control is but one of many parts of the UK Corporate Governance Code which itself is supported by guidance to directors. In the case of internal control, this supporting guidance is often referred to as the Turnbull guidance.
8. It is from this integrated approach that we comment on COSO's proposed Internal Control – Integrated Framework document (the ICIF document).

## SECTION 2: MAJOR POINTS

### 2.1 Developments in the last twenty years

9. In the twenty years since the COSO Internal Control framework was first issued, boards and their management teams in the corporate and other sectors have become much more aware of the wide range and complexity of risks. Over that period, risk management has also become better established, including inter-alia the development of an international standard, ISO 31000.

10. Following the financial crisis, shareholders and other stakeholders have become more interested in information about risks and how they are controlled. Inadequate risk management is often quoted as a contributory factor to the financial crisis.
11. We are therefore disappointed that the proposed revisions to the ICIF document do not appear to reflect major developments in business risk and control over the last twenty years. The revised document can give an impression of the need to be seen to be doing something whilst not making changes that reflect the more significant, recent developments.

## 2.2 Missing elements

12. While there are three pages of names at the beginning of the short Executive Summary document, we find no mention of the words strategy, behaviour or culture which today are recognised as being a key part of helping to manage and control the risks of an organisation. For example, regular assessments of the culture of an organisation are an essential part of the governance, risk and control process. The assessments' results feed into the judgement process when assessing the application of principles.
13. Internal control is also relevant in the development of an organisation's strategy as well as to its implementation. Although COSO's less-used Enterprise Risk Management (ERM) document published in 2004 includes strategy as one of the four objectives, we were surprised that strategy is not included in a far more prominent way in the updated ICIF document. We believe that this will be a very noticeable omission and thus a significant weakness in the 168 page ICIF document.
14. We suggest that other omissions from the COSO cube include:
  - as a component: objective setting. We note that this is already included the ERM framework; and
  - as an objective: the safeguarding of assets. Although reference to this is included in the ICIF document, it is not included as a separate objective; yet it is so included in the IIA standards.
15. In addition, we suggest that the ICIF document overly focusses on the negative aspects of risk and control, with little mention of the upside of risk taking, value generation.
16. These omissions, and its length, may result in key stakeholder groups such as boards and senior management perceiving the ICIF document to be less relevant than it might otherwise be. The result might be that boards and senior management will have difficulty directly engaging with it and will then delegate it to others.

## 2.3 Fraud, IT and wider reporting

17. In many countries, a formal impact assessment of proposed changes to regulation is considered important. Albeit the COSO document is not formally regulation, its use is widespread and it is referenced in US regulation, particularly around the Sarbanes-Oxley Act. This impacts the status of the document and thus the due process required. We assume that, as part of its processes, the COSO board will address the issue of an impact assessment in respect of the proposed changes to the 1992 document with particular reference of how it will impact costs and benefits related to Section 404 reporting by companies and also by external auditors.

- 18.** The COSO board should be wary of the cost/benefit consequences of the ICIF document (and the as yet unseen evaluation tools document) that will impact companies, particularly smaller companies. We assume that COSO will want to avoid companies incurring unnecessary additional costs that exceed any related benefits, as well as minimising any additional administrative burdens and documentation requirements, in both the ICIF and evaluation tools documents. COSO should be wary of ‘make work’ exercises.
- 19.** In particular, we highlight the:
- substantially widened scope what was the financial reporting objective. This is now ‘reporting’ and covers internal and external, financial and non-financial reporting objectives;
  - proposed inclusion of fraud risk and technology controls as separate principles;
  - potential for substantially increased documentation and audit and assurance work related to the 17 principles and 81 attributes especially in context of achieving the proposed ‘effectiveness’ requirements.
- 20.** We suggest that assessing fraud risk (Principle 8) and ‘selects and develops general control over technology’ (Principle 11) are both important element of their respective generic principles ‘identifies and analyses risk’ (Principle 7) and ‘selects and develops control activities’ (Principle 10). Whilst fraud risk and IT controls are often referred to in external audit standards and also in literature from the audit firms, we are not convinced they should be accorded separate principle status. Having the wrong strategy or business model is probably a risk of greater magnitude than fraud risk, yet these matters do not have a separate principle.

#### **2.4 Checklist approach and the level of detail and documentation**

- 21.** The Executive Summary document comments that the list of principles is not a binary checklist but should be approached with judgement. We also note that the document states that, when assessing whether or not a system of internal control is effective, a determination is to be made as to what extent the principles and, in turn, the corresponding attributes associated with each component are present and functioning.
- 22.** We are concerned that when confronted with 98 topics (17 principles and their 81 attributes) in practice it is human nature for management and auditors to adopt more of a checklist-approach, particularly when faced with the proposed requirements for the assessment of effectiveness. This would indeed be an unfortunate consequence.
- 23.** We suggest that consideration might be given to including only the 17 principles in the ICIF document with the 81 attributes confined to a subsidiary, illustrative-only guidance document that has no binding authority. This would require assessors to think carefully and then make their considered, professional judgements against the principles alone.
- 24.** The ICIF document continues to give the impression of being developed so that it is capable of being externally audited. Unlike the Canadian CoCo framework, COSO appears to omit the softer and more subjective aspects related to risk and control, such as culture and people issues that are fundamental to good risk management and internal control but which are less easily externally audited.

#### **2.5 Links to other COSO frameworks**

- 25.** As noted in our introductory remarks, we believe that internal control, risk management and corporate governance are interlinked. COSO currently publishes a number of separate, somewhat lengthy and overlapping frameworks (internal control, internal control for smaller companies, Enterprise Risk Management etc.). Clarification is needed of how each framework interlinks with the others. A consolidation of frameworks into a more integrated approach could also be considered.

## 2.6 Governance of COSO and due process

26. ICAEW is a member body of FEE, the European Federation of Accountants. We support FEE's comments on the governance of COSO provided in the appendix to their comment letter to COSO dated 13 March 2012.
27. We hope that COSO will give full and careful consideration to all comments received on this and related matters from all respondents.
28. We assume COSO will provide substantive feedback on this, and all other significant issues raised by respondents, as part of the overall, due process for the ICIF document.

E [jonathan.hunt@icaew.com](mailto:jonathan.hunt@icaew.com)

Copyright © ICAEW 2012  
All rights reserved.

This document may be reproduced without specific permission, in whole or part, free of charge and in any format or medium, subject to the conditions that:

- it is appropriately attributed, replicated accurately and is not used in a misleading context;
- the source of the extract or document is acknowledged and the title and ICAEW reference number are quoted.

Where third-party copyright material has been identified application for permission must be made to the copyright holder.

[icaew.com](http://icaew.com)