

5 November 2008

Scott L. Mitchell  
Chairman and CEO  
OCEG  
6245 N. 24<sup>th</sup> Parkway, Suite 212  
Phoenix, AZ 85016

***RE: GRC Capability Model, Red Book Version 2 Exposure Draft***

Dear Mr. Mitchell:

Congratulations on the issuance of the discussion document Red Book Version 2. We very much appreciate the opportunity to provide comments on it. These comments are offered on behalf of ISACA and the IT Governance Institute (ITGI) in my capacity as chair of the Professional Issues Working Group and former international president of both organizations.

ISACA is an independent, non-profit, international professional, technical and educational organization dedicated to being a recognized global leader in IT governance, security, control and assurance. With more than 86,000 constituent individuals in more than 160 countries, ISACA is uniquely positioned to fulfill the role of a central global, harmonizing source of knowledge, guidance and practice standards in these areas. Its strategic alliances with other organizations in the financial, accounting, auditing and IT professions create an unparalleled level of integration and commitment ensuring value and practical applicability of our products and services to our constituents and the global business community.

ITGI strives to assist enterprise leaders in their responsibility to make IT successful in supporting their enterprise's mission and goals. Its goals are to raise awareness and understanding of IT-related governance, risk management and control issues among boards of directors, executive management and chief information officers (CIOs) and to provide them with practical guidance and tools. Our ultimate goal is to help ensure that enterprise's use of IT exceeds expectations, delivers business value and mitigates risks.

ISACA is a membership association and research institute that is focused on **information and related technology** (IT) governance, risk management and compliance issues. Thus, our comments are restricted to those areas of the Red Book that we believe are most relevant to our focus. These are:

- Technology Components, the groupings and the way they support the GRC and publication objectives in subsequent detailed entries—page 23, lines 18-39
- P8, Preventive Technology Controls—page 70
- D3.4, Design & Implement Detective Technology Controls—page 90
- I3, Technology & Infrastructure—pages 133-134

**General comment**

Overall, the OCEG Red Book 2 Framework (“the framework”) provides a comprehensive framework to support enterprises looking to ensure they have addressed all of their GRC needs appropriately. The provision of this broad framework should enable enterprises to develop a coordinated approach to GRC across their business, in pursuit of “principled performance.” We fully support this goal. The framework is presented at a level that requires further detailed support and guidance on more specific areas, including IT, which is addressed through the authority documents concept. ISACA and ITGI look forward to using our knowledge and intellectual property to help OCEG and the Red Book framework effectively identify and reference IT-related authority documents.

**Primary observation**

The Red Books draft presents a holistic business framework view that stresses the need for GRC activities to be integrated within the overall business activities.

Overall, our understanding of the framework content is that inconsistency exists in the scope of IT and IT controls applicability within it as follows:

- Preventive controls at P8 appear to deal with all types of risks to enterprise objectives.
- Detective controls at D3.4 may be perceived to deal only with risks to GRC objectives.
- Technology & Infrastructure content at I3 is clearly limited in scope to the “GRC system.”

These inconsistencies leave the overall message somewhat confusing. Specific examples of these confusing messages related to the framework’s IT content can be found in attachment B.

**Recommendation:** OCEG should determine the intended scope of the IT-related content in the framework (i.e., narrowly focused on GRC activities or broadly focused on enterprise goals and objectives), assess the implications for the framework users and adjust the content appropriately to consistently address the intended scope. Our preference would be for a more broadly focused scope. Consistent treatment of such a scope will help ensure that the technology-related framework components support the full enterprise needs including GRC activities and other broader enterprise goals and objectives outside of the “GRC system.”

Our secondary and more detailed comments are included in attachment A.

Again, we appreciate the opportunity to comment on the draft. Thank you for considering our views. We would be happy to discuss them with you in further detail.

Respectfully submitted,



Everett C. Johnson, CPA  
Chair, Professional Issues Working Group  
Past International President, 2005-2007  
ISACA ([www.isaca.org](http://www.isaca.org))  
IT Governance Institute ([www.itgi.org](http://www.itgi.org))

**Attachment A: Secondary Comments in Page Order**

Reference	Comments
<p><b>Lines 19-39, Technology Components, page 23</b></p>	<p><i>Observation:</i> This section opens with the statement that “Technology Components describe infrastructure, applications and information services ...” It then further describes that the “GRC Capability Model, Technology Components” are categorized as “Business Applications, GRC Core Applications or Infrastructure.” The term “information services” is omitted from the second list and two types of applications are introduced.</p> <p><i>Issue:</i> This is confusing to the framework user.</p> <p><i>Recommendation(s):</i> We recommend that the components referred to in the section are made consistent, possibly by adding “information services” to the second list.</p> <p>Further, the Red Book concept of Technology Components should be strengthened by adding two resource elements into “information services” and how they are presented and referenced in the Red Book framework. These two resource elements are “Information” and “People.” This would be consistent with the Control Objectives for Information and related Technology (COBIT) framework, which is based on four information and related technology resources—Applications and Infrastructure (already addressed in Red Book 2.0), and also Information and People (not addressed in Red Book 2.0).</p>
<p><b>P8, page 70 (and D3.4, page 90)</b></p>	<p><i>Observation:</i> P8, Preventive Technology Controls, is presented at a higher level within the framework. D3.4, Design &amp; Implement Detective Technology Controls, appears to be presented at a lower level of the framework. This inconsistency in approach is part of a broader inconsistency between the P and D components of the framework.</p> <p><i>Issue:</i> This inconsistency in the levels at which technology (and other) controls are dealt with in the framework may confuse framework users.</p> <p><i>Recommendation(s):</i> We recommend that OCEG reassesses the reason for, and implications of, the inconsistent treatment of preventive and detective controls within the framework and either make them consistent or explain the rationale for the inconsistency to users.</p>
<p><b>P8, Principle 01, page 70</b></p>	<p><i>Observation:</i> This principle refers to “common points of failure in controls” and “technology control <i>{that}</i> can be applied to address multiple controls.”</p> <p><i>Issue:</i> The phrasing of this principle is somewhat confusing; particularly in the way the term control is used.</p> <p><i>Recommendation(s):</i> We recommend the following wording: “The organization should identify common points of failure in processes, controls, or other enterprise objectives and determine what preventive technology controls can be applied to address these risks.”</p>

Reference	Comments
<p><b>P8, Common SOF 02, page 70</b></p>	<p><i>Observation:</i> This “Common Source of Failure” refers to “Not fully evaluating role based access needs.”</p> <p><i>Issue:</i> It is not made clear why the failure to effectively implement this specific control technique is referenced here. Failure of any and all control options could be listed here.</p> <p><i>Recommendation(s):</i> We recommend that this entry be deleted, since it appears to be a specific instance of SOF 04 in the same list: “Not identifying ways that a process can be violated, circumvented or manipulated.”</p>
<p><b>P8, Practices P8.1, page 70</b></p>	<p><i>Observation:</i> The practice in full states “Define Technology Controls.”</p> <p><i>Issue:</i> This statement is too brief to be established effectively (although we note that the sub-practices on page 71 do help clarify the intent of the practice.</p> <p><i>Recommendation(s):</i> We recommend the following wording “Define adequate and appropriate preventive technology controls to provide reasonable assurance of the achievement of process, technology and enterprise objectives.”</p> <p>We further recommend that this is a specific area of the framework where reference should be made to COBIT (specifically the control objectives within COBIT 4.1 and the related COBIT Control Practices) and other relevant ITGI authority documents. We believe such references would be of value to your audience in this area of the framework.</p>
<p><b>D3.4, Sub-practice 01, page 90</b></p>	<p><i>Observation:</i> The practices listed are generally most effective when implemented as preventive rather than detective technology controls. We could not identify a rationale for the selection of these few specific technology controls.</p> <p><i>Issue:</i> If the framework presents these controls only in a detective manner, key technology control objectives will be missed and exposure to unnecessary risk could occur.</p> <p><i>Recommendation(s):</i> We recommend that this section be revised to read something similar to: “Monitor detective technology control indicators (e.g., audit trail and transaction log analysis results, initiative progress, status and risk reporting) to identify actual or potential misconduct.”</p>
<p><b>I11.1 Sub-practice 03, page 128</b></p>	<p><i>Observation:</i> The practices listed here are a list of specific, detailed information characteristics.</p> <p><i>Issue:</i> This level of detail has not been identified in any of the other areas reviewed (with the exception of D3.4, sub-practice 01, page 90, which was referenced previously). It does not appear appropriate to deliver this level of detail in this high level GRC framework. We believe that the key deliverable material supporting this entry should adequately address the more specific needs of this sub-practice.</p> <p><i>Recommendation(s):</i> Reword this entry as follows: “Define and maintain a process for classifying and inventorying data/information.”</p>

<b>Reference</b>	<b>Comments</b>
<b>I3, Principle 03, page 133</b>	<p><i>Observation:</i> The principle does not address the need to ensure that the GRC solution benefits planned for are actually delivered.</p> <p><i>Issue:</i> The aspect of benefit delivery is often overlooked by enterprise management.</p> <p><i>Recommendation(s):</i> Extend the principle with the following wording “...<i>designing approaches, strategies and controls</i> and ensure that the planned benefits are delivered once these are implemented.”</p>

## Attachment B: Detailed Support for Primary Comment

The framework content related to IT and the treatment applied appears to be inconsistent with the integrated approach by which the framework is introduced. This leaves the overall message somewhat confusing.

We were not clear whether the intent was to include:

- Only those IT controls, technology and infrastructure aspects of enterprises that relate to GRC activities, or
- Those IT controls, technology and infrastructure aspects of enterprises that support a broad range of enterprise goals and objectives (including GRC).

As presented on page 8 of the draft, information technology is stated to be typically “A GRC activity.” By taking this narrow position, important technology detective control and infrastructure aspects of enterprise IT, in support of broader enterprise goals and objectives, may be missed by users of the framework. We recommend the broader approach.

Examples of the confusing messages related to IT can be found with the framework components P/P8, D/D3/D3.4 and I/I3/I3.1/I3.2, as follows:

1. P8 addresses the need of an enterprise to “Implement technologies to reduce the likelihood and impact of undesirable events and activities” (page 70) as part of the framework, to “Promote and motivate desirable conduct, and prevent undesirable events and activities, using a mix of controls and incentives” (page 44), which is the definition of the P component of the framework that deals with “Prevent & Promote” activities. We detected no actual or implied limitation to a “GRC system” in reviewing the P8 content and would therefore conclude the scope of P8 was intended to support a broad range of enterprise goals and activities.
2. D3.4, however, relates to the “Design and Implement [*ation of*] Detective Technology Controls” that are focused on “Implement and monitor automated detective technology controls to promptly identify actual or potential misconduct” (page 90). This component is within D3 that addresses the “Design and establish [*ment of*] controls to detect actual or potential adverse events and weaknesses in the GRC system” (page 87). It is unclear whether the adverse events referred to here relate to the whole enterprise or just to the GRC system, which should be clarified. The overall D component deals with the need to “Detect actual and potential undesirable conduct, events, GRC system weaknesses, and stakeholder concerns using a broad network of information gathering and analysis techniques” (page 77), which ordinarily would be an enterprise objective.

As a result, the detective technology controls referenced in D3.4 may be read as having a “GRC system” scope limitation, since the apparent limitation of D3 scope to the “GRC system” could misdirect the framework user to ignore detective controls, including technology controls, that would mitigate against undesirable events or activities and thereby compromise achievement of enterprise goals and objectives not directly related to GRC.

3. The I3 framework component deals with “Technology & Infrastructure” (page 133). Specifically it addresses the “Enable [*ment of*] the GRC system with a technology architecture that integrates with and, where appropriate, uses existing investments in technology” (page 133). This component is within the I framework component (Inform and Integrate) that specifically deals with the need to “Capture, document and manage GRC information so that it efficiently and accurately flows up, down and across the extended

enterprise, and to external stakeholders” (page 125). I3.1 appears to address the total enterprise “existing technology environment” but that I3.2 focuses on “technology to enable GRC processes and information flows” (page 134).

As a result, I3 (Technology & Infrastructure) is clearly limited in scope to the “GRC system.” This scope limitation does not support the framework user in considering the “Technology & Infrastructure” aspects related to achievement of enterprise business goals and objectives. *[Also, I3.1 appears to have a wider focus than the GRC system scope set at the higher component levels of I and I3.]*