Respondent: ALGA Professional Issues Committee

COBIT 5: The Framework and Process Reference Guide Exposure Drafts Questionnaire

Part 1. COBIT 5: The Framework

1. How would you **rate COBIT 5**: The Framework guidance in **supporting enterprises in establishing effective governance and management of enterprise IT**, from both a content and presentation perspective?

	Excellent	Good	Fair	Poor	Not Applicable
Content		**X**			
Presentation		**X**			

1a. Please explain your ratings, particularly if you selected only fair or poor.

These comments are from the Association of Local Government Auditors. Our review reflects a public sector auditors' perspective and represents about 400 audit organizations, totaling approximately 1,800 members.

COBIT 5 provides a comprehensive Framework, and we appreciate the effort to merge all authoritative guidance into one document. There are some key areas that have been added or modified that will be of value not only to all IT professionals but also to IT auditors and auditors in general.

We identified some key concerns, however, that could affect the usefulness of the Framework. These concerns address both the content and the presentation.

- While the Framework states that it is to be used by all – including nonprofits and the public sector -- once that statement is made the remainder of the framework seems to focus on the private sector. While many of the concepts are applicable to both, there are important differences that should be considered. (e.g., the concept of confidentiality of data and privacy is quite different, governance can differ significantly, the legislative and legal ramifications can also differ among other differences.)
- It is not clear if all audiences can be addressed by this document. There may be too much detail and technical information for executive and non technical readers. It may even be difficult to navigate by technical users. In addition, it is unclear at what level in the organization the framework should be applied.
- COBIT 5 focuses on Objectives, Risks and Value, and it does not give equal weight to controls. Controls are mentioned in the body of the Framework but need to be given more emphasis. This is a framework for IT, and if you do not control and monitor remediation, you cannot effectively govern or manage. When that occurs, you do not add value or achieve objectives.
- COBIT 5 does not appear to consider other IT guidance used by auditors of IT. Some best practice IT auditing guidance includes the IIA's *Global Technology Audit Guides* (GTAG) series and the General Accountability Office's *Federal Information Systems Control Manual (FISCAM).*

- While the Framework recognizes that change must be considered in applying its principles and guidance, emphasis should be made on the perpetual nature of change and the need to constantly refer to the framework. It is not a "snapshot application," but an on ongoing process.
- The language in the Framework is at times very conceptual (maybe even academic). We would suggest a clearer, practical presentation that IT, managers and other stakeholders can intuitively understand. While there are others, the text in the Information Model in Appendix H is an example.
- While mentioned in the body of the Framework (e.g. Capability and Process Models) we believe more emphasis should be given to performance measures/ measurability. We believe that the Framework should highlight the need for objectives to be identified at a level where they are measurable so that they can be effectively managed and governed. "Performance measurement" is only mentioned on p.63, Appendix G, in relation to ITGI (vs. in COBIT 4.1 it is emphasized up front on p.6, 14, and on p.18 in relation to the Maturity Model. "Metrics" is first cited in COBIT 5 on p.27, Goals Cascade example 4, and p.31 in the Generic Enabler Model, Goals and Metrics. The concept is obviously considered and addressed, but it needs more emphasis early-on.

2. COBIT 5: The Framework is built around **five principles** which are introduced in section 1 and further explained in detail in sections 3 through 6.

To what extent would you agree/disagree with the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The principles adequately describe the new vision on governance and management of enterprise IT.		X				
The principles and the new vision are clear to me.		X				
I think this new vision is an important improvement in COBIT 5.			X			

2a. Please explain your answers, particularly if disagreeing.

The "vision" is not actually explained, unless by this you mean the combination of the principles and the framework. In addition, the principals are not totally clear in this section, though it was mentioned that they would be discussed later on. We suggest minor edits in figure 1 to link the elements in Figure 1 and the subsequent Figures 2-6, to help clarify the principles; [e.g., Also suggest making Figure 1 a bit larger and including a little discussion of these interconnecting principles.]

The framework discusses applicability to all entities, units, assets, etc., but ISACA should consider building in discussion that only organizations that have policy-setting authority can implement the framework. For example, a unit may exist in a department in which the department sets the department-wide policy, or a department in an enterprise in which the corporate level sets the enterprise-wide policy.

In terms of improvement from COBIT 4.1, we see a lot of improvements but we also see that some areas were better addressed in COBIT 4.1
- Upon a quick re-review of COBIT 4.1 Executive Summary Figures only, a lot of good material that is presented clearly there is lost or buried in COBIT 5. For example, COBIT 4.1 Executive Summary Figure 1 had clear info on Dashboard/Scorecard and Benchmarking; Figure 2 clearly presented Strategic Alignment and Performance Measurement; Figure 3 had a good presentation of COBIT content from the perspective of Governance (Executives and

Boards) and Management; and Figure 4 had a clear overview of the Interrelationships of COBIT components. This clarity, and some important principles such as strategic alignment or dashboards, seems to be lost in the COBIT 5 Executive Summary.

- Looking further at the COBIT 4.1 Framework (focusing on the Figures, not text), it, too, had a lot of valuable information that was clearly presented and easily digestible. COBIT 4's Figures 5, 6, 8 (as an organizing principle), 10-14 (Maturity Model), 23, and other material, were very clear and useful. Perhaps COBIT 5 has gone beyond the desired critical mass of complexity and is actually less easy to understand and use than COBIT 4.1. (It is possible that this is a familiarity issue, but it seems more to be a clarity and usability issue with regard to key important principles.)
- Also, from our auditing perspective (representing local government auditing), COBIT 4 showed more clearly the role of audit (COBIT 4 Figure 4), whereas the role of audit in COBIT 5, and the audit function's use of COBIT, is almost non-existent.
- Another thing that was much more clearly addressed in COBIT 4.1 was the concept of Control Objectives. In COBIT 5, this term does not appear until p.46. Control Objectives are what the CO in COBIT is all about and we believe they should be given more prominence.

3. COBIT 5: The Framework, section 2 explains the **drivers and business benefits** brought by COBIT 5. To what extent do you agree/disagree with the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The stated benefits are a definite improvement brought by COBIT 5.		X				
The stated benefits are well described (no unfounded benefits or missing benefits).			X			
This section will assist in having COBIT 5 accepted and adopted by enterprises.			X			

3a. Please add any additional comments here.
We thought this section appropriately stressed how IT is a key function and should be integrated with the business. We would suggest, however, using the section to more clearly describe real-world business or organization benefits from having a sound IT approach to governance and management, instead of using this section to discuss why a new framework was needed, which is what it appears to do. In our opinion, a slight shift in languaging would make the model itself seem more valuable to users versus sounding as if the main point is promoting the value of COBIT 5.0 rather than the COBIT 4.1 model.

4. Having read COBIT 5: The Framework, section 4 on **business focus and stakeholder needs**, to what extent do you agree/disagree with the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
This section clearly demonstrates how real world stakeholder issues can be addressed using COBIT 5.		X				
This section will be very helpful for me to address stakeholder issues by translating them into enterprise IT-related goals and enabler goals.		X				
The more detailed content in appendices B, C and D was easy to find.		X				

4a. Please explain why you agreed or disagreed.

This section clearly maps the enterprise goals to the IT-related goals, and the section provides an appropriate disclaimer that these are meant to be used as guidelines that can be customized. The materials also provide a good description of the roles of internal and external stakeholders.

The Stakeholder needs outlined in Figure 10 (p.22) are a good set of questions. The value of the framework, however, will be in the answers. These appear to be partly addressed in the cascading goals, p.23, but still to-be-seen is if or how the questions are clearly answered. (This may be in the Process Reference Guide.)

5. COBIT 5: The Framework, section 5 deals with **enablers**. Appendix I H (this was a typo; there is no appendix I) contains more detailed descriptions of the different enabler categories. How much do you agree/disagree that:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The enabler concept provides a solid basis for governance and management.		X				
The generic enabler model is clear to me.			X			
I can see practical benefit in using the enabler models.		X				
I found the more detailed descriptions in appendix I to be useful		X				
The addition of examples throughout the text in appendix I helped me in understanding the enabler models.		X				

5a. Please explain your answers, particularly if you disagreed.

We appreciate the section adequately stressing the importance of the tone at the top for the organization.

The enablers section is not easy to digest as presented. The Information discussion is not clear and overly conceptual. For example, the concept of "Economical" is not well explained. The whole section on Information Economic Goals is confusing. We are not sure of the value the discussion brings to the Framework and struggled with the relevance of the information. Some simple concepts and key points to make clear are:
  • Economy (least cost)
  • Efficiency (through-put, or time and cost of producing), and
  • Effectiveness (suitability for use intended).
  • Integrity (actions are consistent with the principle being address and has nothing to do as to whether it is correct or free of error.)

Also, other quality attributes of information from COBIT 4.1 (p.61-62) are valuable and enduring (no need to evolve) and are more clear and simple to understand and apply. (i.e., Effectiveness, Efficiency, Integrity, Reliability, Availability, Confidentiality, and Compliance.)

The drafters should consider coming back to look at definitions presented and work on them in relation to a time-tested, enduring, authoritative source such as *Data Quality for the Information Age* by Redman (1996).

The framework refers to "Good Practices," but the more accepted and widely-used term is "Best Practices."

We suggest that ISACA create a better layout and flow for Appendix H. It would help to give the reader more direction and structure on how to use it.

6. COBIT 5: The Framework, section 6 elaborates on the **difference between governance and management.** To what extent do you agree/disagree with the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The difference between both makes sense.		**X**				
The difference between both is clearly explained.)			**x**			
Making the distinction is an important benefit of COBIT 5.		**X**				
The new COBIT 5 Process Reference Model (p.35) is a good demonstration of the relationship between governance and management processes.		**X**				

6a. Please explain why you agreed or disagreed.

The terminology of Committed vs. Involved (p.14) does not seem to make sense in describing Governance versus Management. We suggest omitting that language, and staying with more straight-forward language that clearly distinguishes between the two, such as Governance involves steering and Management involves implementing.

- The discussion of Governance and Management in Section 1 (sub-section 5) needs to be given more prominence by moving that sub-section forward (to make it sub-section 1).
- Almost every figure that has Governance in its title (many of them) has content that is relevant to both Governance and Management. We suggest modifying the figures to reflect this by changing the titles to Governance and Management wherever appropriate.
- Figure 36 in Appendix H is the most useful.
- We suggest combining and consolidating the info that is in p. 13-14, 33-34, and 67-69 (Appendix H) to make it more concise and usable without requiring looking all over the place.
- We suggest (since in our response we represent the auditing perspective), that the writers better clarify how audit and assurance fit into governance and /or management. Currently audit is only discussed as stakeholders with needs or as part of pain points. Audit is actually a part of governance, and can be used as part of management (It is considered a level 4 control per one variation of the COSO model.)

Many Governance and Management activities are listed. We appreciate that monitoring is included as a responsibility of both, since that is often an area overlooked.

7. COBIT 5: The Framework, section 7 includes an overview of implementation guidance. Knowing that the "COBIT 5: Implementation Guide" will be issued together with COBIT 5: The Framework, how much do you agree/disagree with the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
This section is useful.		**X**				
This section is clearly written.			**X**			

7a. Please explain why you agreed or disagreed.

This section would be helpful for an enterprise to use as a guide for implementing the framework. If the framework itself were clearer, however, it would be even more useful.

The correlation between the Seven Phases of the Implementation Lifecycle (Figure 22) and the explanations are not always easily followed.

We have minor suggestions for the terminology on p.40 – avoid use of potentially inflammatory words, like "ignorance". Consider using something like "lack of awareness" and instead of (in the Life Cycle Approach, item 1) "one-off," use "one-time" which is more understandable.

8. COBIT 5: The Framework, section 8 explains the change from the COBIT 4 Capability Maturity Model (CMM) to a process capability assessment approach based on the ISO/IEC 15504 standard. To what extent would you agree/disagree with the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The differences between both models are clearly explained.		**X**				
This section will allow me to consider the need for a proper migration toward the new approach, based on appropriate guidance from ISACA.			**x**			
This section adequately introduces the new ISACA approach and its benefits.			**x**			

8a. Please explain why you agreed or disagreed.

The COBIT 5 model was introduced, but that introduction was light and needed more detail about the new framework.

We like the Process Capability Model and all the templates, but we have some concerns. In summary, the added concept of "achieving the process objective" is valuable, but there seem to be some conflicts in the definitions and suggested ways of rating the levels. In addition, some of the concepts (attributes) may be too nebulous or complex to be usable in a practical way, unless clear examples are provided. More detail:
- The consideration of whether process objectives are being achieved seems of value and perhaps the clearest benefit or improvement of COBIT 5. This is defined as Level 1, Performed, whereas it seems that it would be difficult for a process to consistently achieve (or largely or fully achieve) its objectives without being at least Managed, Established, and

Predictable, if not Optimized. So the concept of "achieving the process objective" seems valuable to clarify, but there seems to be a disconnect in how it is defined in the Levels.

- There is also lost benefit of the 3 lower levels in COBIT 4.1 of Non-existent, Ad-Hoc, and Repeatable being combined into just one level (Incomplete) in COBIT 5. It does not appear that the extra rigor of achieving the COBIT 5's Level 1 is worth the trade-off of no longer knowing the "worst-established" processes that may be at the lowest level of the COBIT 4.
- The differences between the six COBIT 4.1 Maturity Model Levels and the six COBIT 5 ISO/IEC 15504-based Capability Levels (Figure 25, p.48) may not clearly add enough value to be worth adopting, unless an organization is already following ISE/IEC 15504 standards, such that no conversion is needed.
- Without an example rating scale, it seems difficult to conceptualize how a standard rating scale would be developed that would consider both the Level 1 ratings (p.49 bottom) of Not achieved, Partially achieved, Largely Achieved, and Fully Achieved, and the other 2-5 of Managed, Established, Predictable, and Optimised.
- Finally, although we can see some value in considering (Figure 26, p.48) the Process Capability Attributes of COBIT 5 (Process, Performance, Performance Mgt., Work Product Mgt., Deployment, Definition, Controlled, Measured, Optimisation, Innovation, and Performance), these concepts may be nebulous, and the Process Capability Attributes of COBIT 4 may be more straight-forward to apply (Awareness and Communication; Policies, Processes and Procedures; Tools and Automation; Skills and Expertise; Responsibility and Accountability; Goals and Metrics).

9. Having read the complete COBIT 5: The Framework publication, how would you rate the following:

	Excellent	Good	Fair	Poor	Not Applicable
Structure of the document		X			
Readability of the document			X		
Clarity of the document			x		
Document is fit for purpose		X			

9a. Please explain your ratings, particularly if you selected only fair or poor.

Although the structure is systematic, the document was difficult to navigate and not easily understood at times. We believe this is due not only to the amount of redundancy, but also due to confusing terminology. It is possible that many potential readers will not spend the time needed to fully grasp the concepts in the framework. This may be true especially of executive-level readers whose time is limited.

We suggest the redundancy and repetition be removed.   We also suggest that ISACA move the 4 pages of acknowledgements to the end. In addition, we recommend adding a well-written, concise acknowledgement statement to all the contributors on the inside cover. This could be under the section labeled ISACA, making reference to the detailed acknowledgements of specific contributors at the end, and then start with the Table of Contents on p.2.

10. Please submit any additional comments on the COBIT 5: The Framework here.

In general, the COBIT 5 framework is easier to read and understand than previous versions. The layout also makes it easier to follow. The framework appropriately highlights and focuses on the importance of integrating IT with business. There are a few areas of improvement noted:
- Better descriptions and explanations of the figures
- Better section headers to guide the reader on where they are
- Minor edit on page 21 ("A set of sources" instead of "A set if sources"); also noted various other minor edits throughout
- Page 26 says "Overall, COBIT 5 defines 18 IT-related goals, listed in **figure 13.**" However through the documents (Framework and Process Reference Guide) 17 IT-related goals are listed.

11. Barrier: Of the following, which do you believe will pose the greatest barrier to effective governance of your enterprise's IT in the coming year?

Choose **one** of the following answers

The enterprise uses too many frameworks.	
There is no clear stakeholder value.	
Business users are not involved.	
The enterprise's culture/structure is not conducive to effective governance.	**X**

.

12. Driver: Which one of the following is the most significant driver for the governance of your enterprise's IT?

Choose **one** of the following answers

Avoid negative incidents.	
Manage costs and resources.	**X**
Increase agility to support future business changes and deliver benefits.	
Achieve better balance between innovation and risk avoidance.	
Comply with industry and/or governmental regulations.	

Part 2. COBIT 5: Process Reference Guide

1. Having read COBIT 5: Process Reference Guide, section 2 on the goals cascade, how much do you agree/disagree that the goals cascade:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
Is useful to translate stakeholder needs into attainable goals		**X**				
Is clear and well described		**X**				
Provides sufficient information to allow using it in practice		**X**				
Contains mappings that make sense and are useful		**X**				

1a: Please make any additional comments here.

None.

2. COBIT 5: Process Reference Guide, section 3, describes the COBIT 5 process model and section 4 of the process reference model. How much do you agree/disagree that:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The process model and its components are clear to me.		**X**				
The process model is complete and contains all required components.			**X**			
The process reference model (figure 9) is clear to me.		**X**				
The process reference model (figure 9 is complete).			**X**			

 2a: Please make any additional comments here.

It is unclear how the "Evaluate" piece for governance fits into the Governance and Management process reference model (Figure 9).

3: COBIT 5: Process Reference Guide, section 5 includes the detailed process information. How much do you agree/disagree that:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
The layout and accessibility of information is good.	**X**					
The information provided is at the right level of detail to benefit my organization.	**X**					
All process related information I need is included.			**X**			

3a. Please make any additional comments here.

It is difficult to know if all related information is included without actively using the reference guide. The Process Reference Guide appears to include a good amount of information that an enterprise could use as guidance for incorporating the COBIT 5 framework processes. The Process Reference Guide ties together the framework by linking the process to IT-related goals that it supports.