

July 11, 2008

Dear Mr. Rittenberg,

Please find attached the detailed feedback on the COSO's exposure draft, Guidance on Monitoring Internal Control Systems, what I promised in my previous letter. These critical comments are not intended to put aside the results of the huge and fruitful work performed by the Monitoring Team, however they aim to (maybe a bit over)emphasize the needs of further considering and utilizing the other views (dimensions) of the COSO framework than unit/activity levels. In order to support better understanding of these comments, I also attach a revised working paper of using ISO/IEC 15504 international standard for assessing internal financial controls. (A former version was sent by commenting the 2007 Draft.)

If the proposed approach were considered as being out of the scope of the current Monitoring Guidance, then I would suggest to let the proposed idea open for further discussions and development by involving any possible interested parties including COSO and ISO/IEC 15504 professionals.

The ISO/IEC 15504 (SPICE) communities are interested in sharing and extending their knowledge and experiences into new areas such as internal financial controls. During the recent SPICEDAYS 2008 Conference in Prague, which was the latest event of the most potent world-wide SPICE community (e.g. including German Automotive Industry), some participants - after discussion of the COSO models' applicability - proposed to set up a new working group within iNTACS. iNTACS (www.intacs.info) is an independent non-profit association aiming to foster the education and experience exchange of ISO/IEC 15504 (SPICE) assessors on a world-wide basis.

The proposers of the Working Group on Governance Models aim to put the COSO and SPICE models together in order to commonly utilize both professional communities' methodology developments and best practices. Corporate governance experts can exploit the applicability of the ISO/IEC 15504 assessment model, while SPICE assessors and trainers can develop their skills toward new application domains. The new SPICE models, such as the proposed COSO based Assessment Model will contribute to the achievement of iNTACS' general objectives:

- Support and Development of ISO/IEC 15504 compliant methods (SPICE)
- Support of certification of ISO/IEC 15504 Assessors
- Accreditation of Certification Bodies
- Development and Maintenance of Syllabus for Assessor Trainings compliant to the needs of specific domains

The proposed activities of the Working Group include:

- Making working relationship and agreement with the global and national institutes holding property rights
- Developing and maintaining new reference models - such as the COSO based reference model - for ISO/IEC 15504 validation
- Developing and maintaining assessment models and guidance based on the validated reference models
- Supporting the development of training materials and assessment tools ensuring property rights
- Supporting translations into different languages
- Performing trial assessments
- Disseminating results

When the working group is setting up I will contact you for discussing necessary arrangements (e.g. copyright issues). Meanwhile I would like to ask the Monitoring Team to consider whether the proposed ISO/IEC 15504 assessment approach is applicable for the current scope of the Monitoring Guidance. In case of positive feedback the proposers of the iNTACS working group are ready to cooperate.

I am looking forward to receiving feedback from the Monitoring Team.

Best regards,

Janos Ivanyos
Memolux Ltd
IIA Hungary - IT section
iNTACS founding member

COSO Guidance on Monitoring Internal Control Systems
Public Comment Form – Spring 2008

Thank you in advance for providing feedback on COSO's exposure draft, *Guidance on Monitoring Internal Control Systems*. Your candid responses will allow us to gauge its effectiveness and improve the final document, benefiting organizations of all sizes and their stakeholders.

This comment form follows the order of the Guidance. You may also complete it online (which is our preferred method of collecting feedback) through a link posted at <http://www.coso.org/guidance.htm>. Each section contains brief questions regarding the Guidance and also offers respondents an opportunity to provide general feedback unrelated to the questions. If you prefer, you may provide feedback without answering the questions. The demographic information requested in the last section will help us group and analyze the responses.

You may submit this form or other written feedback via email to COSOMonitoring@gt.com or fax it to COSO Monitoring at 704.337.2979.

We would like to receive all comments by August 15, 2008. Note that they will be posted to the COSO Web site as submitted, with no redaction of identifying information.

If you have any questions about accessing or responding to the discussion document, please contact Jay Brietz at 704.632.6916.

We know your time is valuable, and we thank you again for your thoughtful completion of this comment form. Your feedback is integral to the success of the final document.

Larry E. Rittenberg, PhD, CPA, CIA
Chairman, COSO

Questions/Commentary

Volume II – The Guidance

Chapter I. Monitoring as a Component of Internal Control Systems

1. Does the Guidance adequately describe the role of internal control monitoring (paragraphs 6–10)?

Somewhat

Comments:

Paragraph 10 emphasizes the differences between control processes and control activities: "Throughout this guidance, the terms "internal controls" and "controls" are used to refer to the control processes and elements put in place to achieve the objective of any of the five COSO Framework components. The term "control activities" refers specifically to internal controls that achieve the objective of the COSO Framework's control activities component." However the above term of "control activities" doesn't allow to distinguish between monitoring and control activities. The 2007 version of the Monitoring guidance referred to "root-cause analysis" as a distinguishing feature of monitoring from control activities. This approach seems to be under considered in the new version.

2. Additional comments regarding Chapter I.

Comments:

The reference to the COSO ERM model is still very limited, which will certainly cause misunderstanding within the target audience. Figure 2 is modified a bit from the original one (of the 2006 Guidance), however just changing the "financial reporting objectives" into "organizational objectives" does not mean clear message about how the supplementary components (Objective Setting, Event Identification, Risk Response) of the ERM model should be applied.

Paragraph 17 refers somehow to the ERM principles, however this presentation is not followed consequently in the later parts. If the "root-cause analysis" concept had been followed, then the prioritising would have also focused on control risk areas, not just on the importance of control activities.

It is not clear how the risks of control failures should be prioritised for designing and executing monitoring procedures. What are the organizational objectives regarding effectiveness and efficiency of the internal control system, how much risk the management and the board are willing to accept, and how can these targets be measured (in the form of "risk tolerance" and "risk appetite")? Answering these questions is a precondition for risk-based evaluation of effectiveness and efficiency of internal control system.

The "root-cause analysis" concept should have been also followed in the later parts of the document. More (at least balanced) focus should have been done on monitoring the COSO components through the achievement of the COSO objectives than mainly dealing with the lower level objectives of the underlying control activities. This unbalanced view of monitoring causes that the document seems to be more an implementation guidance of key controls

rather than a monitoring guidance of the entire internal control system.

Chapter II. Establishing a Foundation for Monitoring

3. Is the model for monitoring presented in paragraph 19 a complete and accurate outline of the monitoring process?

Somewhat

Comments:

The current Model for Monitoring is based more adequately on the risk management concept than in the first draft. However there are some unclear and unnecessary overlaps with the other components of the COSO model.

As commented before, the "root-cause analysis" concept is missing. Prioritising based on importance of controls should be (also) performed by applying ERM principles (Objective Setting, Event Identification, Risk Response) on the internal control system. The structure presented in Figure 3 seems to be more adequate to an implementation guideline of control activities.

On page 8, the "Assessing and reporting" phase of the Monitoring Model refers to providing support for conclusions regarding the effectiveness of internal control. This important objective is not really supported by the later parts neither in the Guidance (Volume II) nor in the Application Techniques (Volume III). There is no guidance how the persuasive information should be processed in order to objectively support effectiveness conclusions.

4. Do you agree with the description of the roles of management and the board with respect to monitoring (see paragraphs 23–24)?

Somewhat

Comments:

Explanation and example of Paragraph 23 refer basically to monitoring of control activities by the senior management, while Paragraph 24 refers to monitoring of the internal controls (as a system). This could falsely indicate that the senior management should only monitor the control activities, while the board's responsibility is limited to monitor the implementation of the internal controls by the senior management. Principle 2 (Board of Directors) of the COSO 2006 Guidance refers correctly to the role of the board.

The presented way of describing the roles of management and board also leads to a redundancy with the above mentioned COSO Principle, furthermore it doesn't emphasize sufficiently the role of management regarding to monitoring of the other components within the internal control system.

5. Do you agree with the description of the characteristics of evaluators (see paragraphs 25-33)?

Somewhat

Comments:

Paragraphs 25-33 refer to the characteristics related to the operational view (as Figure 4 shows). All of the presented competence and objectivity considerations are valid and very important, however they are extensively related to the control activities. Competence and objectivity considerations should also include the other two dimensions of the COSO cube (control components and objectives).

6. Is the discussion about establishing a baseline understanding of internal control effectiveness clear, correct, complete, and useful (see paragraphs 34–36)?

Somewhat

Comments:

Paragraphs 34-36 are presenting more an implementation concept of control activities rather than of monitoring internal control system. That is why there are redundancies with the COSO Risk Assessment component.

However the four components of the "Baseline Understanding of Internal Control Effectiveness" concept would be applicable to support conclusions regarding the effectiveness of internal control system instead of the monitoring program (as stated in Paragraph 36). If these components were implementing ERM principles on the entire internal control system (by performing control risk assessment) instead of focusing just on the control activities (as presented), then the results of the control risk assessment (as a periodic separate evaluation) would be used to support effectiveness conclusions regarding the internal control system. This is a missing element of the "Assessing and reporting" phase of the proposed Monitoring Model. (See comment on Question 3).

7. Additional comments regarding Chapter II.

Comments:

Figure 4 represents well the above-mentioned conceptual problems. While the COSO 2006 Guidance focused on the Component dimension of the COSO cube, this Monitoring Guidance provides a view of the internal control system from the business operations (units/activities) dimension. Paragraph 10 clearly states, that monitoring should consider "how the entire internal control system manages the risks", however the presented foundation for monitoring concept is focusing much more on implementing control activities (which is otherwise very useful!) than assessing the effectiveness and efficiency of the entire internal control system.

Chapter III. Designing and Executing Monitoring Procedures

8. Figure 7 on page 18 and paragraphs 42–49 are designed to provide an overview of the core of monitoring — designing and executing monitoring procedures. Do the graphic and related summary paragraphs properly summarize the process of monitoring?

No

Comments:

This part is again focusing on a subset of the control activities. As the "implementation" approach bowled out the "root-cause analysis" concept of monitoring it is understandable why this part is about how to implement key controls. However objectives of Principles 19-20 of the COSO 2006 Guidance are not about implementing key controls.

Key controls are means to ensure that organization achieves its business objectives. Ongoing and/or separate evaluations should enable management to determine whether the other components of internal controls continue to function over time. Which are the key controls ensuring that internal controls continue to function over time? How they are derived from business objectives? Without applying COSO ERM concept we can not easily answer these questions.

At first the management and the board should set objectives regarding how the internal control components should function. Then the possible events effecting these objectives should be identified. By performing the relevant risk assessment, the potential risk responses should be identified and ranked based on cost/benefit analysis.

Unfortunately this part of the proposed Monitoring Guidance doesn't apply appropriately the risk management concept on the internal control system, as its scope is limited to the operational view of control activities. Risk prioritisation as presented in Paragraph 44 means only reuse of the results of the Risk Assessment component without adding the risks of control system failures to the scope.

9. The Guidance indicates that effective and efficient monitoring evaluates controls that address "meaningful risks" to an organization's objectives. Paragraphs 50–54 provide guidance regarding assessing risks and how prioritizing risk influences monitoring. The intent is to provide guidance (1) without being prescriptive as to how risk assessment should be done, and (2) without delving so deeply into the risk assessment component that the focus of the Guidance shifts away from monitoring. Do you believe the Guidance properly addresses the role of risk assessment in the context of internal control monitoring?

No

Comments:

This part of the Guidance is just an overview of how the risk assessment should be applied in general. It contains very limited additionality in context of monitoring internal controls. Risks regarding failure of internal controls are not presented here.

Paragraph 52 states that "the assessment considers the importance of the risk without considering the expected effectiveness of internal control." This statement is not applicable to those key controls which are designed to prevent other control failures or to detect such

failures before they have an opportunity to become material to the organization's objectives. A well-established (measurable) risk appetite should be set by considering effectiveness expectations based on cost/benefit analysis.

10. The Guidance defines the term “key controls” (see paragraphs 46–47 and 55–57). The project team chose to define the term because (1) it is widely used in practice, but is not consistently defined; and (2) the Guidance proposes that, in order to conclude that the internal control system effectively addresses a given risk, organizations may not need to evaluate every control that addresses that risk — thus, the term distinguishes between controls that will be subjected to monitoring procedures and those that will not. Do you believe the concept of “key controls” is properly addressed in the Guidance?

Somewhat

Comments:

The concept of distinguishing key controls from other control activities is applicable for monitoring. However the new version of the Guidance has lost the “root-cause analysis” concept, which would otherwise help to define the necessary targets of monitoring. There is no guidance on how the key control concept is applicable regarding the objectives and components of internal controls.

11. Information that is evaluated to assess controls effectiveness provides varying levels of support. The Guidance defines “persuasive information” as that which is capable of providing adequate support for a conclusion about the effectiveness of internal control. Persuasive information is further defined as that which is “suitable and sufficient in the circumstances” (see paragraphs 59–60). Do you agree with the general premise of persuasive information as outlined in the Guidance?

Somewhat

Comments:

"Persuasiveness" of information regarding the effectiveness of the internal control system should indicate in what extent the information supports the conclusion on effectiveness. In this context the suitability can be different when the same information is used for monitoring a group of control activities or the entire internal control system. Therefore identifying persuasive information should start with setting attributes measuring effectiveness of internal controls at the appropriate levels. It would be practical if these attributes had similar meanings for different processes at those levels where the conclusion on effectiveness of the entire system is necessary. For example attributes of effectiveness regarding fulfillment of specific compliance objectives can differ by operating business processes, however attributes of achieving reliable reporting objective should be generic.

12. The Guidance discusses the difference between direct and indirect information as being one of the primary factors influencing the persuasiveness of information. Feedback from the September public discussion document indicated broad support for this aspect of the Guidance, but also indicated a need to refine and clarify the material. Is the current discussion of direct and indirect information (in paragraphs 64–72 and in the Applying the Concepts section beginning on page 34) clear, correct, complete, and useful?

Somewhat

Comments:

Useful implementation practices to the 15th and 16th Principles of the COSO 2006 Guidance.

13. The Guidance states that reliable information is accurate, verifiable, and from an objective source (paragraphs 73–75). Is the concept of reliability, as described in the document, clear, correct, complete, and useful?

Somewhat

Comments:

Useful implementation practices to the 15th and 16th Principles of the COSO 2006 Guidance.

14. Is the concept of timeliness of information (paragraphs 76–77), as described in this document, clear, correct, complete, and useful?

Somewhat

Comments:

Useful implementation practices to the 15th and 16th Principles of the COSO 2006 Guidance.

15. The “Sufficient Information” section (paragraphs 78–79) has been expanded based on feedback from the September public discussion document. Is this expanded material clear, correct, complete, and useful?

Somewhat

Comments:

Useful implementation practices to the 15th and 16th Principles of the COSO 2006 Guidance.

16. Based on feedback from the September discussion document, the section regarding “Ongoing Monitoring and Separate Evaluations” has been simplified. It now more clearly articulates that the primary difference between the two is not how they are performed, but how often and by whom. The Guidance then addresses the factors an organization might consider in deciding between the two processes. Do you believe this section is clear, correct, complete, and useful?

Somewhat

Comments:

There is no guidance how the persuasive information should be processed in order to objectively support effectiveness conclusions.

17. A paragraph has been added to the document to address the monitoring of controls outsourced to others (paragraph 90). Is this paragraph clear, correct, complete, and useful?

Yes

Comments:

18. The “Using Technology for Monitoring” section has been simplified from the September 2007 draft, and a discussion regarding “continuous controls monitoring” has been added (see paragraphs 91–94). Is this section clear, correct, complete, and useful? (Note: Some commenters to the September 2007 discussion document indicated a desire for direction in applying the monitoring guidance to controls over information technology (IT). A comprehensive discussion regarding monitoring IT controls has been included in Volume III.)

Yes

Comments:

19. Additional comments regarding Chapter III.

Comments:

This part is focusing on a subset of the control activities (key controls). As the "implementation" approach bowled out the "root-cause analysis" concept of monitoring it is understandable why this part is about how to implement key controls. However control risk assessment should have been also applied.

It might seem to be too academic pushing in front the risk management regarding how effectively the COSO components support the achievement of COSO objective categories, however this concept comes directly from the COSO definitions. The fact, that it is much easier to define a set of more or less isolated objectives, events and risk responses regarding well established operational activities, doesn't mean that management and auditors can miss to perform risk management practices regarding the entire internal control system.

For example: without setting measurable "risk appetite" as an objective regarding the operation of the internal control system, the risk assessment on an individual business process can't be performed consistently, otherwise the risk ranking (or prioritisation) would be done occasionally.

An other issue of the presented prioritisation concept is that those controls which are designed to prevent other control failures or to detect such failures before they have an opportunity to become material to the organization's objectives, are not always identified as key controls as they have loose or just indirect connection to business objectives. Without adequately implementing control risk assessment, these controls (which are also referred as key controls by Paragraph 46) can be hardly identified.

Chapter IV. Assessing and Reporting Results

20. Is the section “Prioritizing and Communicating Results” clear, correct, complete, and useful?

Somewhat

Comments:

The concept is clear, however there is no guidance how the likelihood that the deficiency will result in an error can be objectively measured.

21. Is the section “Reporting Internally” clear, correct, complete, and useful?

Somewhat

Comments:

The assurance and consulting engagements of the evaluators (auditors) could have been mentioned here.

22. Is the section “Reporting Externally” clear, correct, complete, and useful?

Yes

Comments:

23. Additional comments regarding Chapter IV.

Comments:

Comment on Question 3 already refers to the fact that the objective of providing support for conclusions regarding the effectiveness of internal control is not really assisted by the Guidance and Application Techniques.

Paragraph 95 says: "This final stage enables the results of monitoring to either confirm previously established expectations about the effectiveness of internal control or highlight identified deficiencies for possible corrective action." Comparing the target and assessed attributes regarding effectiveness of internal control would be a potential tool for measuring likelihood and significance of control failure risks.

Target attributes of internal control effectiveness are representing measurable risk appetite of the entity. Conclusion regarding the effectiveness of internal control would be well supported by the gap assessment on targets (expectations) and monitoring results. It is evident, that setting lower level targets of effectiveness (by approval of more risks due to higher cost of controls) has effect on conclusion. The same gap (monitoring result) will cause different conclusions based on how the risk appetites are set by different entities or entity levels.

Chapter V. Scalability of Monitoring

24. Chapter V, “Scalability of Monitoring,” is designed to show how monitoring might differ between organizations based on their size and complexity. It is designed to complement and summarize other references to size and complexity that are spread throughout the document. Is this chapter clear, correct, complete, and useful?

Yes

Comments:

Section VI. Assessing the Effectiveness and Efficiency of Monitoring

25. Is Chapter VI, “Assessing the Effectiveness and Efficiency of Monitoring,” clear, correct, complete, and useful?

Somewhat

Comments:

Just as in the case of other COSO components, monitoring effectiveness and efficiency conclusions should be supported by the gap analysis of the target and assessed attributes. See comment on Question 23.

Other General Areas/Topics

26. Does the Executive Summary (Volume I) effectively summarize the guidance contained in Volume II?

Yes

Comments:

27. Apart from your comments above, should anything be added or changed to improve the Guidance, making it more practical to implement? If so, please summarize your recommended additions or changes below.

Yes

Comments:

Using ISO/IEC 15504 process assessment principles and techniques contributes to the development of innovative approaches in monitoring the effectiveness of internal control in the following aspects:

- Providing Assessment Model for all internal control components and principles by using the COSO based Process Reference Model.
- Offering tools for internal control risk assessment supporting the communication of internal control weaknesses and the considerations of necessary corrective actions.
- Focusing on specific and generic assessment indicators applicable for compliance, reliable reporting, operational effectiveness and strategic objectives.
- Applying assessment indicators for collecting evidences from business activities and entity/corporate levels, as well.
- Differentiating “internal controls” as a system from the underlying “control activities” as the object of monitoring.
- Linking operational effectiveness considerations of business processes to the achievement of internal control objectives.

Related working paper can be downloaded from:

http://hun.ia-manager.org/file.php/1/Summary_of_IFCA_Principles_V6.pdf

28. Overall, do you believe the document advances the understanding of what effective monitoring should look like in any given organization?

Somewhat

Comments:

A more balanced view of all the three dimensions of the COSO framework should have been considered in monitoring. Applying COSO ERM principles directly on the internal control system (by performing control risk assessment) would have provided more tools of supporting conclusions regarding the effectiveness of the entire internal control system. There is no guidance how the persuasive information should be processed in order to objectively support effectiveness conclusions.

Volume III – Application Techniques

Chapters II–IV. Brief Examples Linked to Volume II Chapters

29. Chapters II–IV of Volume III contain brief examples of how various organizations currently monitor internal control in ways that are consistent with the concepts embodied in Volume II — the Guidance and are organized to correspond with the Guidance. As the introduction to Volume III indicates, the examples are not intended to mandate how monitoring should be performed, but to articulate how the Guidance might be applied. Do the examples achieve that objective? (Note: Please elaborate if you believe certain of the examples should be edited or deleted or if you recommend inclusion of other examples.)

Yes

Comments:

Guidance Summaries together with the Examples are very well developed, and often more informative in supporting better understanding than the original text of the Guidance.

30. The appendices to Volume III relate to the examples discussed in question #29 and show some of the tools the various organizations use for monitoring. Are the appendices helpful without appearing to be prescriptive?

Yes

Comments:



Chapter V. Comprehensive Examples

31. Chapter V of Volume III contains comprehensive examples of how two organizations monitor internal control over a given risk area. These examples attempt to demonstrate application of the monitoring process from start to finish, as outlined in the Guidance. Like the earlier examples, those in Chapter V are intended to be descriptive rather than prescriptive. Do these two examples help demonstrate application of the Guidance?

Yes

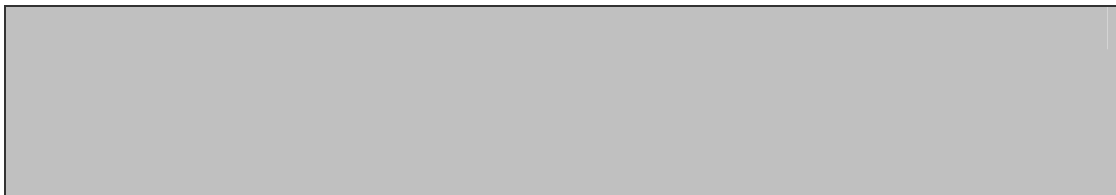
Comments:

The very good comprehensive examples demonstrate the strengths and also limitations of the Guidance.

32. Chapter V of Volume III also contains a discussion of monitoring information technology (IT) controls that address financial reporting-related risks. This discussion was included because (1) many people have requested specific guidance regarding monitoring IT controls related to financial reporting, (2) IT-related risks are pervasive across most organizations, and (3) the ways in which those risks are controlled are fairly consistent across organizations, making the discussion applicable in a broad sense. Without being prescriptive, does the discussion about monitoring IT controls articulate how such monitoring might be performed?

Yes

Comments:



33. Additional comments regarding Volume III.

Comments:

Volume III is much more informative than Volume II, as it doesn't contain unnecessary theoretical paraphrases and it is supported by well selected examples. However practical examples of control risk assessment supporting conclusions on effectiveness are missing.

Demographic Information

34. Your name

János Ivanyos

35. Your email address

ivanyos@memolux.hu, janos.ivanyos@iia.hu

36. Your position (select the position from which you answered the questions above)

Consultant

IT section leader of IIA Hungary, iNTACS member working on Governance Models

37. Country

Hungary

38. Name of organization (should correspond to position selected in Question 36 above)

Memolux Ltd., member of IIA Hungary, founding member of iNTACS

39. Classification of the above-named organization (select one)

Professional association

Communities of Internal Auditing and ISO/IEC 15504 Process Assessment

40. Annual revenues of the above-named organization

N/A

41. Public float (market cap) of the above-named organization, if a public company

N/A

Implementing COSO based Process Assessment Model for Evaluating Internal Financial Controls

By János Ivanyos, Memolux Ltd. (H)

Introduction

New generation of governance models referring to either IT or Internal Control – like COBIT [1] and COSO [2] - are extended with business perspective willing to gain top management's ear. But the practice shows, this opening solely does not enough to reach a breakthrough, because models became more complicated than it could be applied without some difficulties. Very frequently exposed that the best catalyst of improvement programs are the more and more mandatory rules coming into force. Sarbanes-Oxley Act for US SEC registrants and their affiliates (all over the world), the Basel II framework and the proposed modification of the Company Law in the EU require not only the implementation of risk management and internal control systems, but the periodic disclosure of effectiveness conclusions performed by the executive management.

Compliance and capability issues have come into the view of the management as the huge cost of compliance readiness activities calls the attention of the sustainability and the added business value of such efforts. This challenge has been answered by utilizing the ISO/IEC 15504 process assessment standard [3], and its evaluation model concept applicable for the executive managers, boards of directors, the internal and external auditors and even for the supervisory bodies to assess and disclosure the internal control effectiveness of enterprise risk management and financial reporting processes.

This paper provides a summary to the principles of the proposed Process Assessment Model for evaluating Internal Financial Controls in accordance with the requirements of ISO/IEC 15504-2. However the same approach is applicable for setting up Process Assessment Model for IT Governance, as the COBIT 4.1 descriptions of control processes are also conformant with the ISO/IEC 15504-2 requirements.

COSO based Process Assessment Model

An integral part of conducting an assessment is to use a Process Assessment Model (PAM) constructed for that purpose, related to a Process Reference Model (PRM) and conformant with the requirements defined in ISO/IEC 15504-2. ISO/IEC 15504-2 provides a framework for process assessment and sets out the minimum requirements for performing an assessment in order to ensure consistency and repeatability (objectivity) of the ratings.

The Process Reference Model, derived from the COSO 2006 Guidance (Internal Control over Financial Reporting — Guidance for Smaller Public Companies), has been used as the basis for the proposed Internal Financial Control Process Assessment Model. This COSO based Process Reference Model associated with the process attributes defined in ISO/IEC 15504-2, provides a common basis for performing assessments of internal financial control process capability and reporting of results by using a common rating scale.

The Process Assessment Model defines a two-dimensional model of process capability. In one dimension, the process dimension, the processes are defined and classified into process categories. In the other dimension, the capability dimension, a set of process attributes grouped into capability levels is defined. The process attributes provide the measurable characteristics of process capability.

Figure 1 shows the relationship between the general structure of the ISO/IEC 15504-2 conformant Process Assessment Model and the COSO control processes (grouped into the 5 components).

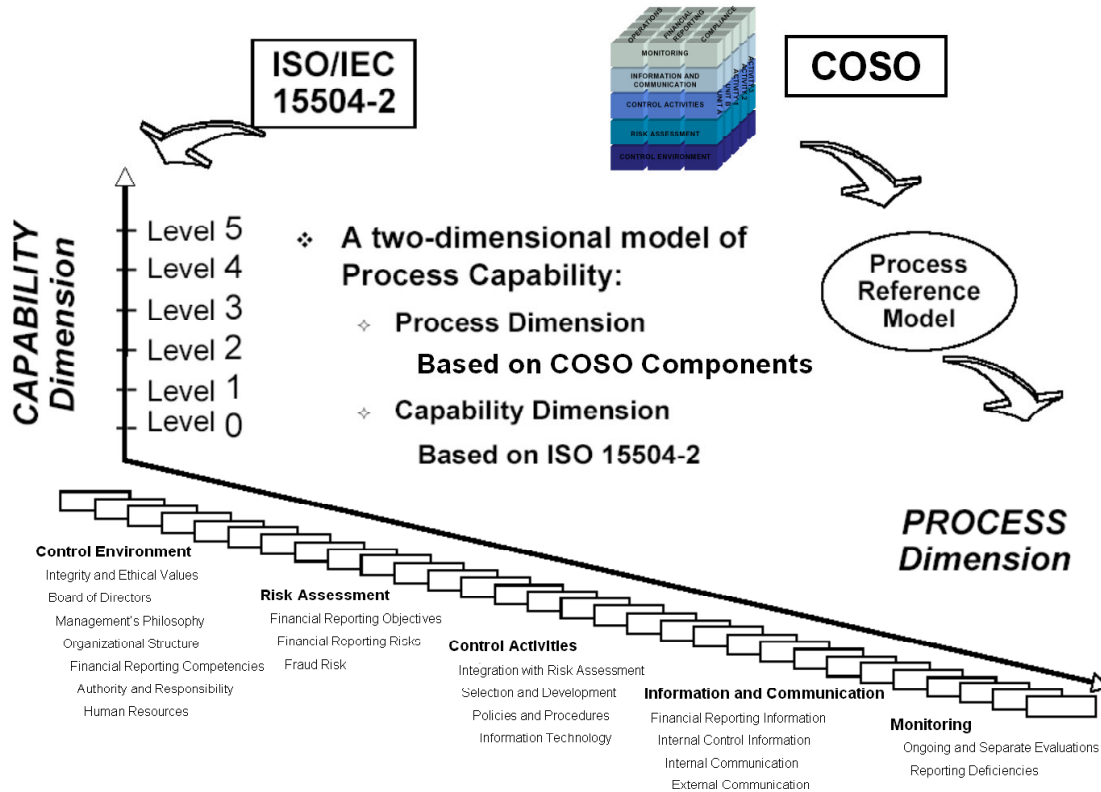


Figure 1: COSO components as Process Dimension of the Process Assessment Model

The Process Assessment Model expands upon the Process Reference Model by adding the definition and use of assessment indicators. Assessment indicators comprise indicators of process performance and process capability and are defined to support an assessor's judgment of the performance and capability of an implemented process.

ISO/IEC 15504-2 requires that processes included in a Process Reference Model satisfy the following:

"The fundamental elements of a Process Reference Model are the set of descriptions of the processes within the scope of the model. These process descriptions shall meet the following requirements:

- A process shall be described in terms of its Purpose and Outcomes.*
- In any description the set of process outcomes shall be necessary and sufficient to achieve the purpose of the process.*
- Process descriptions shall be such that no aspects of the measurement framework ... beyond level 1 are contained or implied."*

The proposed Process Assessment Model includes processes, which are grouped in five process categories, identical to the control components defined in COSO models, which are:

- Control Environment;
- Risk Assessment;
- Control Activities;
- Information and Communication;
- Monitoring.

The processes included in the same category contribute to a complementary area. This categorization can also help assessors in defining the assessment scope in term of process selection.

The COSO 2006 Guidance called “Internal Control over Financial Reporting — Guidance for Smaller Public Companies” is in compliance with the PRM requirements of the ISO/IEC 15504-2. Volume II of the Guidance has a structure of Principles and Attributes, which is equivalent with the process identification via Purpose and Outcomes.

The COSO guidance provides a set of twenty basic Principles representing the fundamental conceptual processes associated with and drawn directly from the five components of the internal control *Framework*. Supporting each Principle are Attributes, representing characteristics associated with the Principle.

The guidance says “although each attribute generally is expected to be present within a company, it may be possible to apply a principle without every listed attribute being present”. However, from common internal control assessment perspective we handle the Attributes “as *process outcomes ... necessary and sufficient to achieve the purpose of the process*” which described by the relevant Principle. During an assessment the assessor can judge whether a specific Attribute handled as necessary and sufficient process outcome in the PRM, is practically assessable within the context of the specific assessment scope (characterized by organization type, size, complexity, etc.)

Figure 2 presents how the content of the COSO 2006 Guidance can be used for mapping with PRM:



Figure 2: COSO Guidance as Process Reference Model

The processes from COSO 2006 Guidance that are included in the process dimension of the proposed Internal Financial Control Process Assessment Model, are listed below:

Control Environment (CE)

1. **Integrity and Ethical Values (IEV).** Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
2. **Oversight Board (OB).** The board of directors and/or audit committee understands and exercises oversight responsibility related to financial reporting and related internal control.
3. **Management's Philosophy and Operating Style (MPO).** Management's philosophy and operating style support achieving effective internal control over financial reporting.
4. **Organizational Structure (OS).** The company's organizational structure supports effective internal control over financial reporting.
5. **Financial Reporting Competencies (FRC).** The company retains individuals competent in financial reporting and related oversight roles.
6. **Authority and Responsibility (AR).** Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.
7. **Human Resources (HR).** Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

Risk Assessment (RA)

1. **Financial Reporting Objectives (FRO).** Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.
2. **Financial Reporting Risks (FRR).** The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.
3. **Fraud Risk (FR).** The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Control Activities (CA)

1. **Integration with Risk Assessment (IRA).** Actions are taken to address risks to the achievement of financial reporting objectives.
2. **Selection and Development of Control Activities (SD).** Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives.
3. **Policies and Procedures (PD).** Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.
4. **Information Technology (IT).** Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Information And Communication (IC)

1. **Financial Reporting Information (FRI).** Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.
2. **Internal Control Information (ICI).** Information used to execute other control components is identified, captured, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.
3. **Internal Communication (IC).** Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.
4. **External Communication (EC).** Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Monitoring (MO)

1. **Ongoing and Separate Evaluations (OSE).** Ongoing and/or separate evaluations enable management to determine whether internal control over financial reporting is present and functioning.
2. **Reporting Deficiencies (RD).** Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

For the *process dimension*, all the 20 internal control processes referred as Principles in the COSO guidance, are included within the process dimension of the proposed Internal Financial Control Process Assessment Model. Each process in the Process Assessment Model is described in terms of a purpose statement. These statements contain the unique functional objectives of the process when performed in a particular environment. A list of specific outcomes is associated with each of the process purpose statements, as a list of expected positive results of the process performance.

Satisfying the purpose statements of a process represents the first step in building a level 1 process capability where the expected outcomes are observable.

A capability level is a set of process attribute(s) that work together to provide a major enhancement in the capability to perform a process. Each level provides a major enhancement of capability in the performance of a process. The levels constitute a rational way of progressing through improvement of the capability of any process and are defined in ISO/IEC 15504-2.

Within a Process Assessment Model, the measure of capability is based upon the nine process attributes (PA) defined in ISO/IEC 15504-2. Process attributes are used to determine whether a process has reached a given capability. Each attribute measures a particular aspect of the process capability. At each level there is no ordering between the process attributes; each attribute addresses a specific aspect of the capability level.

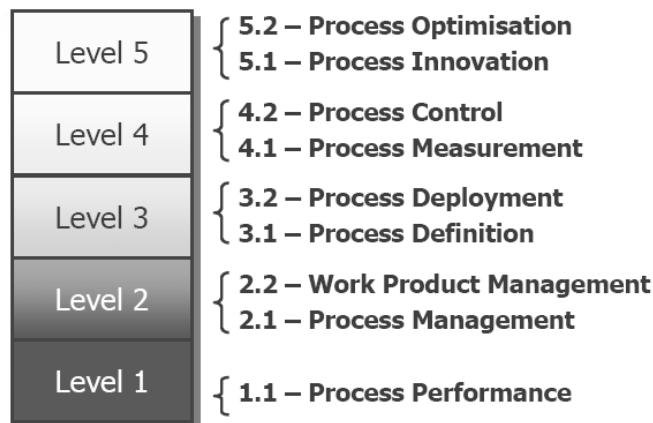


Figure 3: Process Attributes by Capability Levels

The process attributes are evaluated on a four point ordinal scale of achievement, as defined in ISO/IEC 15504-2. They provide insight into the specific aspects of process capability required to support process improvement and capability determination.

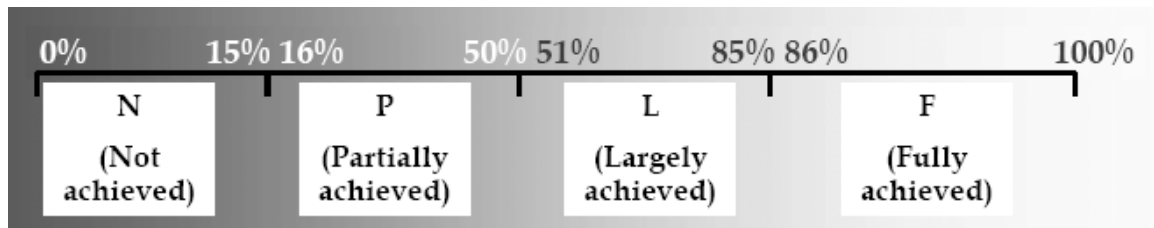


Figure 4: Four point ordinal scale for evaluating the achievement of process attribute

The Process Assessment Model is based on the principle that the capability of a process can be assessed by demonstrating the achievement of process attributes on the basis of evidences related to *assessment indicators*. There are two types of assessment indicators: process capability (generic) indicators, which apply to capability levels 2 to 5 and process performance (specific) indicators, which apply exclusively to capability level 1. The process attributes in the capability dimension have a set of process capability indicators that provide an indication of the extent of achievement of the attribute in the instantiated process. These indicators concern significant activities, resources or results associated with the achievement of the attribute purpose by a process.

Assessment indicators are used to confirm that certain practices were performed, as shown by observable evidence collected during an assessment. All such evidences come either from the examination of work products of the processes assessed, or from statements made by the performers and managers of the processes.

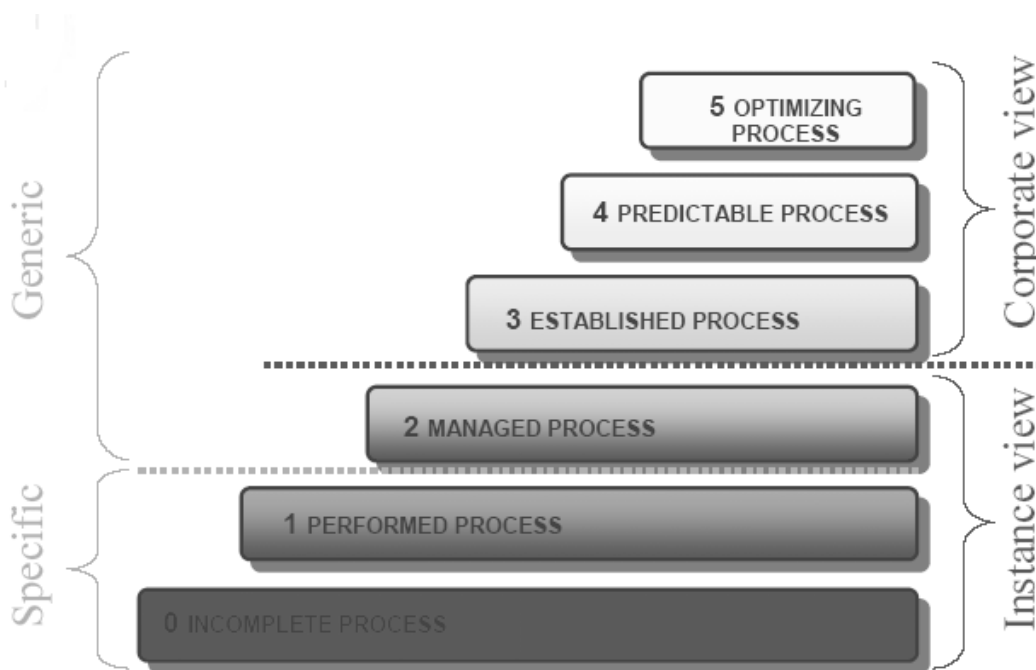
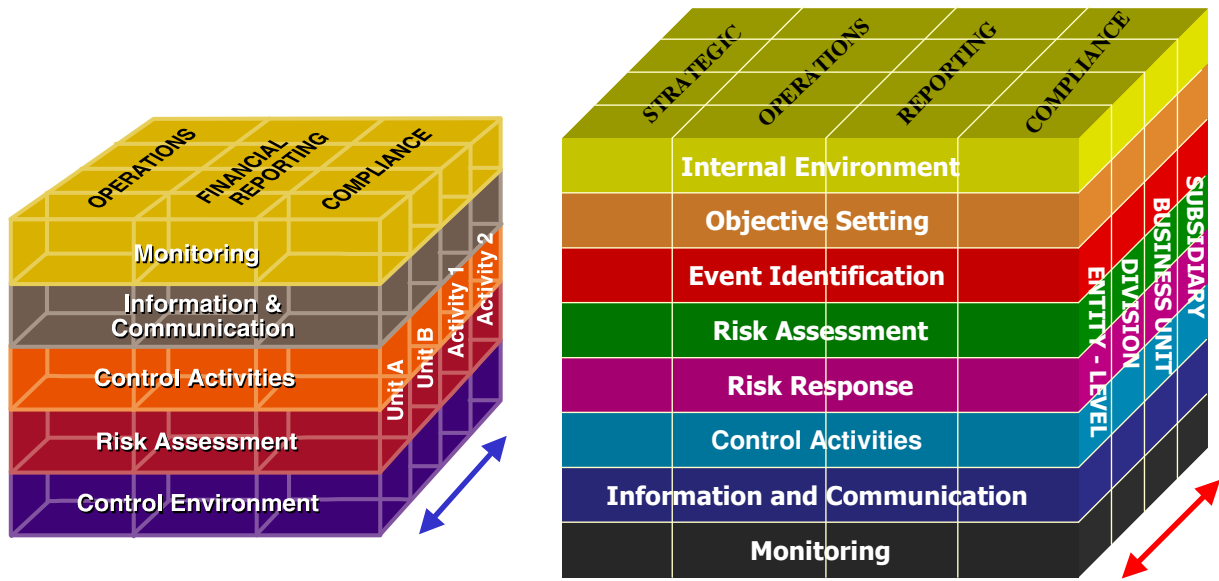


Figure 5: Assessment indicators per capability levels

The first three capability levels are focusing on the instance or activity view of the processes, while from level 3 the attributes are focusing on the corporate entity view. This observation helps us to understand how the COSO Internal Control and ERM frameworks fit into this assessment model. As shown in Figure 6 the third dimension of the Internal Control framework is the Unit/Activity, while in ERM the third dimension is the corporate structure.



Source: www.coso.org

Figure 6: Activity (Instance) and Entity (Corporate) views within the dimensions of the COSO models

Capability Levels and their business context

In COSO ERM terminology management considers risks strategy in the setting of objectives, such as:

- *Risk Appetite* of the entity - a high-level view of how much risk the management and the board are willing to accept.
- *Risk Tolerance* - the acceptable level of variation around objectives - is aligned with risk appetite.

In ISO/IEC 15504 terminology the set of target process profiles expresses the target capability, which the sponsor judges to be adequate to the organization's business risk appetite and tolerance.

Figure 7 shows that while the COSO Internal Control components are used for setting up the process dimension of the ISO/IEC 15504 conformant Process Reference Model, the ERM principles contribute to the set-up and usage of the assessment indicators measuring the achievement of the COSO objective categories through the ISO/IEC 15504 capability levels.

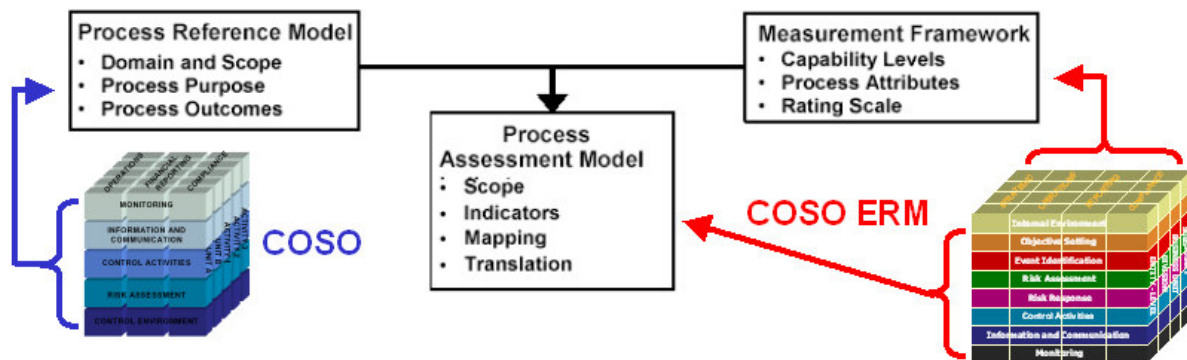


Figure 7: ISO/IEC 15504 capability levels and COSO objective categories

Mapping and applying the main objective categories of the COSO Internal Control and ERM models into the capability dimension of the ISO/IEC 15504 measurement framework provide guidance to set target capability profiles by the assessment sponsor, give effective tool to the management to identify, understand and manage control risk areas.

Figure 8 identifies the applicability of the capability levels to the COSO main objective categories:

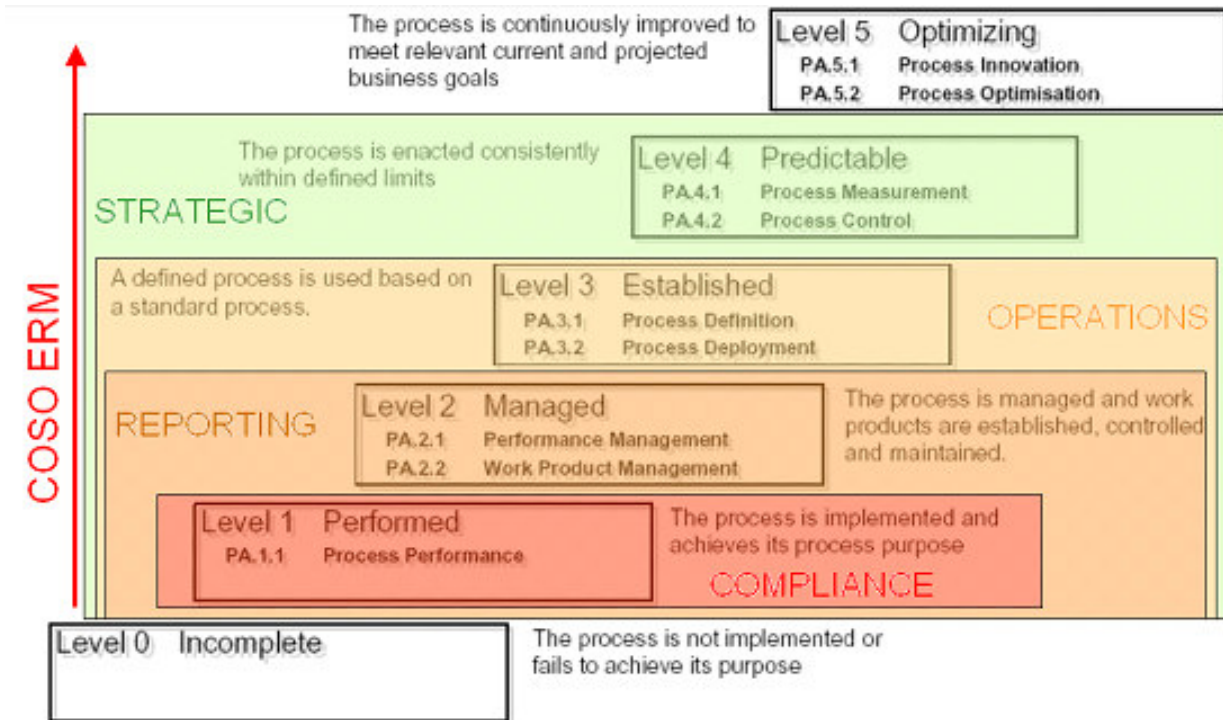


Figure 8: ISO/IEC 15504 capability levels and COSO objective categories

Achieving Compliance Objectives at Performed Process Level (1)

The process dimension of the assessment model adopts the same process definitions (Principles) as the COSO 2006 Guidance. The achievement of the process performance attribute represents that the management has good understanding of the basics of the internal control requirements and the financial reporting activities are managed by keeping in mind the components of internal control framework in an ad hoc base. There are evidences of achieving control process purpose, however not in a systematic way.

As mainly focusing on fulfilment of the sectoral and accounting regulatory requirements in financial reporting related business activities, the Level 1 assessment results are mainly usable in further process improvement context.

Achieving Compliance objectives in all (relevant) internal financial control processes from the COSO based Process Reference Model provides good image and reputation of the management in both internal and external environments. However external bodies having wider scope than just verifying periodic financial statements cannot utilize these results. For example: a chain of control/audit structures cannot reuse the Level 1 assessment results at different management levels, like in the case of complex European funding structures or banking supervisory functions.

In private sector, even in the case of strict regulatory requirements like SOX, Level 1 assessment results on the full set of internal financial control processes can be sufficiently utilized by the stakeholders. As these processes are building up a comprehensive framework, the complementarities

of the outcomes and purposes of these processes can provide reasonable assurance even for reliability of financial reporting, as the COSO 2006 Guidance aims it. However, the complexity of business activities and corporate structures, the applicability of risk management principles makes management and shareholders considering advantages of lower control risk levels.

Achieving Reliable Reporting Objectives at Managed Process Level (2)

This level represents that the Performed control process (already achieving compliance objectives at Level 1) is implemented in a *managed* fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

Besides Level 1 achievements, the internal control process is managed and fulfils the reliable reporting objectives. At Level 2 assessment the financial reporting activities shall be investigated, whether the performance and work product management *indicators related to the internal control processes* are assessable and how they are evidenced.

At this level, the financial reporting (related) activities are not only controlled in a systematic way (as already resulted by Level 1 achievements of the full set of internal control processes). Moreover, the performance and work products of the internal control processes are appropriately managed; also providing reusable evidences for wider scoped external or supervisory investigations. The lower control risk level resulted by Level 2 achievements provides higher credibility of the results of all financial reporting related activities.

Complex institutional structures and business or programme/project activities in all sectors require Managed process capability level, which in case of internal financial controls contribute to reliability of reporting processes in such circumstances.

Achieving Effective and Efficient Operation Objectives at Established Process Level (3)

At this level the Managed process (already achieving compliance and reliable reporting objectives at Level 2) is implemented by using a defined process capable of achieving its process outcomes.

Besides Level 1 and 2 achievements, the internal control process is built into the operational processes and fulfils the objective of “Effectiveness and efficiency of operations”. At Level 3 assessment the financial reporting related activities should be investigated together with the organizational/entity level policies and procedures, whether the process definition and deployment *indicators related to the business processes* relevant for financial reporting are assessable and evidenced.

The “Related Business Activities” (work product) resulted by the “Financial Reporting Objectives” control process shall define these relevant business processes. Either the scope of the “Policies and Procedures” control process can cover wider integration with other business processes, or the related business activities can be grouped into an optional process category to be assessed against the attributes of the Managed process level in advance. Without adding specific business processes to the process dimension, Level 3 type assessment of the full set of internal control processes has only limited additional value in comparison to Level 2 achievements.

Achieving Level 2 capability profile for the entire set of processes from the COSO based Process Reference Model already represents Level 3 achievement for those control processes which are not embedded into other business activities due to business area, type, size, etc. This is typical case for smaller companies, where for example the Control Environment processes performed by top management are closely or directly influence employees’ actions. Vice versa: a major capability Level 3 (process deployment attribute) gap at a control process - which outcome is embedded into a relevant business process - causes significant gap at a lower capability level of “Policies and Procedures” control process.

However, setting different target levels for a subset of the processes from the COSO based Process Reference Model can be also reasonable. Fulfilling Level 3 process attribute targets at those processes which are not (necessarily) embedded into other business activities, together with Level 2 results at some other control processes can also provide more reasonable assurance regarding the achievement of compliance and reliable reporting. For example Level 3 Monitoring processes enhancing internal audit functions can have real additional value for any type of organizations targeting lower capability levels for other control processes.

The cornerstone of applying practices for Level 3 process attributes is how the scope of the internal financial control system is defined. If the scope is narrowed just to financial reporting activities, then a full set of processes from the COSO based Process Reference Model fulfilling Level 2 capability profiles can provide reasonable assurance to achieve compliance and reporting objectives. If the scope is widely open to other business activities identified among the “Related Business Activities” defined by the “Financial Reporting Objectives” control process, the “Policies and Procedures” control process can be supported and implemented by advanced business-driven management approach aiming higher capability profile.

Very often the controls embedded into business processes are referred as control activities. Level 3 considerations also help us to understand the differences between the internal controls as a system and the control activities as parts of the related business activities. When the process dimension is extended with the relevant business processes, then the Level 3 type of assessment will evidence how the internal control system supports the implementation of the “Policies and Procedures” by developing and monitoring of the control activities embedded into the business processes.

Level 3 achievements have some significant consequences. Once, this is the level where the process capability determination aspects of the ISO/IEC 15504 conformant assessment can be widely utilised by external parties for assurance purposes. Normally the “Standard Policies and Procedures” at entity level are not divided or separated into different application areas; so different assurance activities (e.g. internal control, quality management, information system management, etc.) can apply for the same set of standards within an organization.

Secondly, this is the level where entity/organization level performance of the “Related Business Activities” can be assessed. It is a very important issue to define adequately the scope and coverage of standard processes, and how they facilitate embedding the outcomes of internal control processes into operational processes. Too complex scope and excrement coverage can result too much cost of controls, high bureaucracy, inefficient usage of resources. If the scope and coverage is too narrow (e.g. limited to financial administration activities), the Level 3 advantages do not fully prevail.

Thirdly, Level 3 achievements represent the base for applying ERM principles. In this context, the range of the key control processes also influence the minimum scope and coverage of Level 3 standardization. If the internal financial control assessment has a limitation in scope to the material weaknesses in financial statements not be prevented or detected on a timely basis by internal controls, then the range of the key controls will be a subset of the financial control activities. In wider (ERM) context, the key controls are all those processes, which are necessary and sufficient for keeping business performance within a tolerable variance from business objectives. Key controls are selected control processes from the basic set of the Process Reference Model and/or a subset of the relevant business processes, with which the process dimension of the assessment model is necessarily extended.

Achieving Strategic Objectives at Predictable Process Level (4)

At this level the Established process (already achieving compliance; reliable reporting; and effective and efficient operation objectives at Level 3) operates within defined limits to achieve its process outcomes.

Besides Level 1, 2 and 3 achievements, the internal control process is incorporated into the enterprise risk management system and fulfils the Strategic objectives relating to high-level goals, aligned with and supporting the entity’s mission. At level 4 assessment the key controls shall be investigated, how

they are applied in strategy setting and across the enterprise together with the entity level risk management, whether the process measurement and process control *indicators related to the achievement of entity objectives* are assessable and evidenced.

Setting of Level 4 target capability presumes, that the concerning internal financial control process and the related business processes where control outcomes are built in comprise *key controls*.

“Key controls are those significant controls within our business processes, which if operating correctly will both ensure and give assurance that the organization is achieving its key business objectives” [4]

By customising the generic financial reporting objectives linked directly to specific business objectives the management will be able to adequately react to external and internal events representing inherent risks to financial reporting.

A key control exception can happen at any time (e.g. automated process is not working, inadequate segregation of duties is identified or loss contingency is realized, etc.). Achieving Level 4 process attributes means that exceptions are handled within the accepted deviation (risk tolerance) of the settled risk levels (risk appetite) to the desired business objective. Financial impact shall be reasonably estimated and the resolution to the control exception shall be identified, scheduled and followed.

Evaluating internal control process related risk

The Control Risk Assessment performed on ISO/IEC 15504 conformant process assessment results, provides feedback to the management whether the existing gaps between the target and assessed capability profiles represent acceptable control risk level for the sponsor (“the individual or entity, internal or external to the organizational unit being assessed, who requires the assessment to be performed, and provides financial or other resources to carry it out” - *ISO/IEC 15504-1, 3.13*).

This approach provides more flexible and customisable method to evaluate the system of internal (financial) controls, necessary to define the coverage of the substantive examinations of the economy, efficiency and/or effectiveness of the organisations, activities, programmes or functions concerned.

ISO/IEC 15504 standard provides guidance on how to utilise a conformant process assessment within a process improvement programme or for process capability determination.

Setting target capability

The sponsor should determine which processes from the selected Process Reference Model are (most) important for the pre-defined requirements (Process Capability Determination) or business goals (Process Improvement).

Also the sponsor should specify a target process profile, showing which process attributes are required for each selected process. Also the necessary rating for each process attribute should be given. Only ratings of “Fully achieved” or “Largely achieved” should be set. “Partially achieved” rating has no meaning to set, as this would indicate that the achievement would be unpredictable in some aspects. “Not required” should be noted for a process attribute taken to be unnecessary.

The set of target process profiles expresses the target capability, which the sponsor judges to be adequate (to the organization’s business risk appetite and tolerance). Figure 9 presents example target and assessed process profiles for 5 selected sample Internal Financial Control processes:

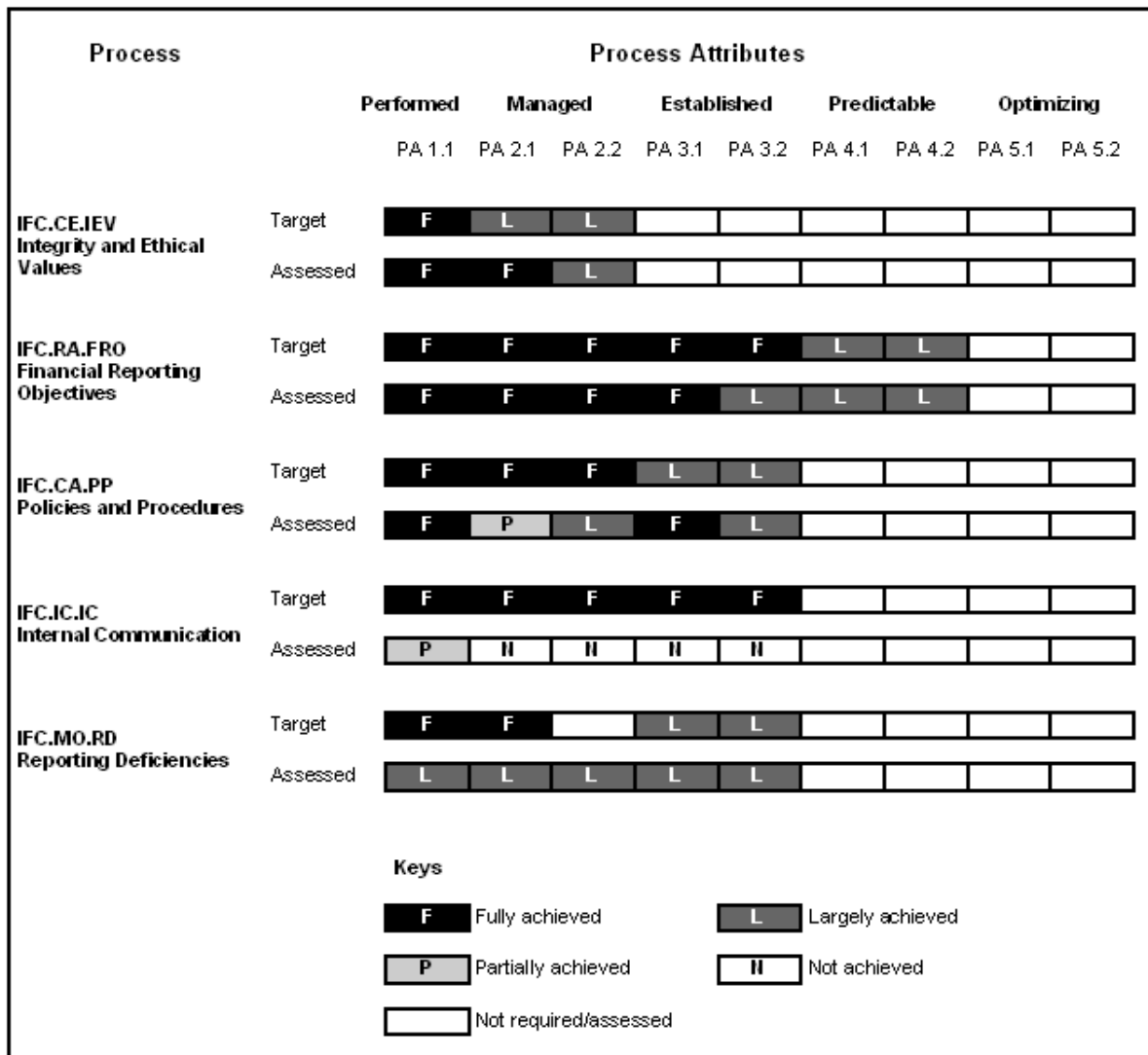


Figure 9: Example target and assessed process profiles

Gap assessment

Process-related risk can be inferred from the existence of gaps between the target and the assessed process profiles.

The potential consequence of a gap depends on the capability level and the process attributes where the gap identified. Some Internal Financial Control related considerations and examples (by using the above example process profiles) are presented as follows:

Typical consequence of the gap at Level 1 PA 1.1 Process performance attribute is that not all of the relevant process outcomes (Attributes of COSO Principles) are achievable, and no recoverable documentation exists to track the necessary control. E.g. Management communication to personnel in roles affecting financial reporting is not adequately documented, so updates on internal or external finance matters are not taken into consideration.

At Level 2 PA 2.1 Performance management gap, the typical consequences are the missing deadlines, lack or inefficient use of resources, unclear responsibilities, uncontrolled decisions, etc. E.g.

Management communication with oversight board or personnel is not planned or scheduled; the related management does not do deficiency disclosure in time; unauthorized decisions are done at period closing; policies and procedures are not under revision on a timely base.

At Level 2 PA 2.2. Work product management attribute, the gap can cause unpredictable quality of reports, parallel entries and inconsistent documentation, increased rework cost, consolidation problems. E.g. Old versions of policies and procedures are also in use; identified exceptions are not communicated; internal communication is not filed in a systematic way.

At Level 3 PA 3.1 Process definition gap, the consequences are that best practices and learnt lessons are not taken into account during revision of policies and procedures or the outcomes of the related control processes are not identical in the operational procedures. E.g. Missing or formal description of internal communication procedures withhold staff members to use alternative reporting lines informing oversight board about material weaknesses or improvement suggestions.

At Level 3, the PA 3.2 Process deployment gap can cause inconsistent applications of financial controls built into the operational procedures. Identified opportunities are lost due to inefficient deployment effort. E.g. The oversight board does not take the internal auditor's consultative role and efforts seriously; the financial statement assertions are not properly linked to the business processes during risk assessment; information technology controls do not reflect adequately to the complexity of the IT environment.

At Level 4 PA 4.1 Process measurement gap, the consequences are that the key controls are not properly identified, designed or operating in order to achieve process performance objectives and business goals or detect performance problems early. E.g. the resolution of key control exceptions is not covered in risk assessment.

At Level 4 PA 4.2 Process control gap, the consequences are that the quantitative performance objectives and the defined business goals do not meet. E.g. Short monthly/yearly closing deadline can cause unpredictable materiality of accruals, management estimates and reserves.

Analysing control process related risk

Annex A of ISO/IEC 15504-4 presents an example approach summarized below.

The process attribute gap - presented in the previous part - can be categorized into "None", "Minor" and "Major" categories based on the distance of target and assessed ratings. E.g. one-step gap is evaluated as minor, two or more steps distance deems major gap in case of "Fully achieved" attribute target. At "Largely achieved" target even the one step distance ("Partially achieved") means major gap.

The *probability* of problem occurrence is derived from the extent of process attribute gaps and from the capability level where they occur. Capability level gaps are categorized as follows:

None	- No major or minor gaps
Slight	- No gap at Level 1, and only minor gaps at higher levels
Significant	- A minor gap at Level 1, or a single major gap above
Substantial	- A major gap at Level 1, or more than one major gap above

The process related risk depends on both the *probability* of problem arising from the identified gap and the potential *consequence*. In general the consequences depend on the capability levels where the gaps occur.

As it is shown in Figure 10, the high risk arises from a substantial gap at a lower capability level.

Consequence Indicated by capability level where gap occurs	Probability Indicated by extent of capability level gap		
	Slight	Significant	Substantial
5 – Optimizing	Low Risk	Low Risk	Low Risk
4 - Predictable	Low Risk	Low Risk	Medium Risk
3 - Established	Low Risk	Medium Risk	Medium Risk
2 - Managed	Medium Risk	Medium Risk	High Risk
1 - Performed	Medium Risk	High Risk	High Risk

Figure 10: Risks associated with capability levels

If risks are identified at more capability levels, then the highest risk measure shall be considered as the process related risk.

Based on the presented approach risk analysis shall determine which process or processes represent the greatest degree of risk. Figure 11 presents examples of Internal Financial Control related risk assessment using example process profiles from Figure 9, where the process profiles showed gap at 3 internal financial control processes:

- IFC.RA.FRO - Financial Reporting Objectives;
- IFC.CA.PP - Policies and Procedures; and
- IFC.IC.IC - Internal Communication

IFC.RA.FRO - Financial Reporting Objectives

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	L	L
Assessed profile	F	F	F	F	L	L	L
Process attribute gap	-	-	-	-	minor	-	-
Capability level gap	-	-		slight		-	
Capability level risk	-	-		low		-	
Process related risk	low						

IFC.CA.PP - Policies and Procedures

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	L	L	-	-
Assessed profile	F	P	L	F	L	-	-
Process attribute gap	-	major	minor	-	-	-	-
Capability level gap	-	significant		-		-	
Capability level risk	-	medium		-		-	
Process related risk	medium						

IFC.IC.IC - Internal Communication

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	-	-
Assessed profile	P	N	N	N	N	-	-
Process attribute gap	major	major	major	major	major	-	-
Capability level gap	subst.	substantial		substantial		-	
Capability level risk	high	high		medium		-	
Process related risk	high						

Figure 11: Internal Financial Control related risk assessment examples

Reasons for internal financial control process improvement

As presented in the previous part, internal control process related risk evaluation is based on the gaps between the target and the assessed process attribute ratings. Setting lower target capability for internal financial control processes is theoretically explainable if the inherent risk of the financial reporting activities and the related business administration processes is measured at very low level or the inherent risk is acceptable to fulfil regulatory compliance requirements. Otherwise Level 2 capability target is the adequate minimum requirement to assess control procedures against reliability objectives of financial reporting.

In more complex environment (featured by business type, size, sectoral regulations, etc.) the continual improvement of business administration processes is desirable. Integration of financial controls with business operations is necessary, when not only the reliability, accuracy and availability of the financial information are critical, but the effectiveness of the related operational activities is also required. Assessing internal financial controls, together with the business processes where they are embedded, against up to Level 3 process attributes is reasonable for the big or multinational organizations, publicly listed companies under SOX regulation, financial institutes, and specific public service companies managing public funds.

Process Capability Determination

The purpose of process capability determination (PCD) is to identify the strengths, weaknesses and process related risks associated with selected processes with respect to a *particular specified requirement*.

The terminology of particular specified requirement originally meant supplier selection criteria, however the new standard approach is more generalized. The PCD assessment is somehow an extended compliance audit or review, where the specified compliance criteria are translated into target capability profiles of the selected processes. The difference from process improvement (PI) approach is that the PCD main goal is to identify the alterations and to determine the potential risks coming from alteration comparing to the pre-defined requirements.

Hereby some practical examples of different PCD sponsorship cases:

1. *Financial Statement Audit.* External financial auditor can use PCD results as sufficient competent evidential matter to design the nature and timing of the necessary substantive tests. Also the Audit Committee, which is responsible to engage and determine compensation of the external audit firm, can utilize PCD results to effectively negotiate the necessary audit effort and fee.
2. *Evaluation of Internal Control Systems By Bank Supervisory Authorities.* State Supervisory Authorities responsible for finance sector has to set up evaluation methods applicable for different types of banking organizations.

3. *Managing and monitoring EU Structural Funds*. Although the Structural Funds are part of the Community budget, the way in which they are spent is based on a system of shared responsibility between the European Commission and Member State governments. Verification of (operational and financial) control systems can be done by the Commission and/or by the State. PCD concept can be applicable for both.
4. *“Single audit model”*. The single audit approach is based on sharing results and prioritising cost-benefit principles in order to minimise the duplication of control work, and maximise the level of control, which can be achieved with a given level of resources. Sharing well-defined and documented control information can permit reliance on controls at each level in the chain. A formalised assessment of costs and benefits at each level will enable the demonstration that the controls in place have optimised the residual risk of error in the underlying transactions.

Impact on Internal Audit assignments

The IIA's definition of internal auditing refers to "...bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." This definition incorporates the broad advisory and assurance role that internal auditing can have regarding an organization's governance processes. Aspects of internal auditing's role in governance are addressed in performance standard 2130 of the International Standards for the Professional Practice of Internal Auditing [5]:

The common interpretation of ISO/IEC 15504 capability levels and COSO objectives showed in Figure 8 provides an innovative method for internal auditors to implement the 2130: Governance standard. The Process Capability Determination (PCD) and Process Improvement (PI) context of ISO/IEC 15504 provides the effective tool for internal auditing having the following significant responsibilities in corporate governance activities:

- Performing assessments to provide assurance that governance structures and processes are properly designed and operating effectively.
- Providing advice on potential improvements to governance structures and processes.

Figure 12 presents how the Process Improvement and Capability Determination approaches are applicable for the two types of Internal Audit Engagements:

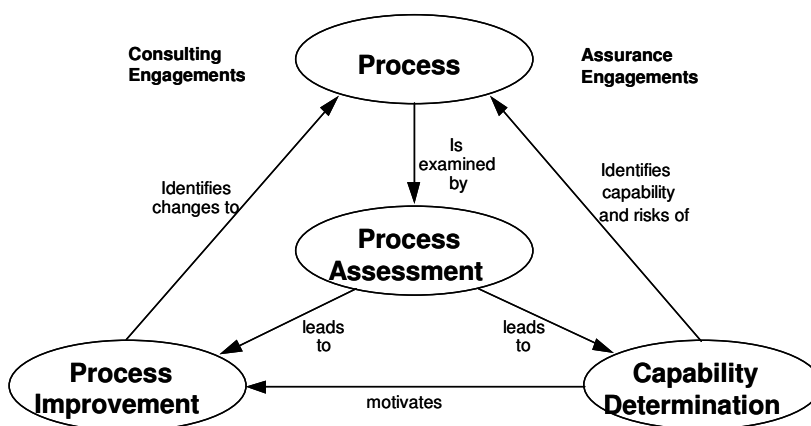


Figure 12: ISO/IEC 15504 and Internal Audit Engagements

Relevant guidance of internal audit engagements can be found in the The IIA's Professional Practices Framework and in the Practice Advisories [6].

Monitoring internal control systems

As the COSO materials refer to the fifth component: internal control systems are monitored to assess the quality of the system's performance over time. Monitoring is designed to ensure that internal control continues to operate effectively.

Using ISO/IEC 15504 process assessment principles and techniques contributes to the development of innovative approaches in monitoring the effectiveness of internal control in the following aspects:

- Providing Assessment Model for all internal control components and principles by using the COSO based Process Reference Model.
- Offering tools for internal control risk assessment supporting the communication of internal control weaknesses and the considerations of necessary corrective actions.
- Focusing on specific and generic assessment indicators applicable for compliance, reliable reporting, operational effectiveness and strategic objectives.
- Applying assessment indicators for collecting evidences from business activities and entity/corporate levels, as well.
- Differentiating "internal controls" as a system from the underlying "control activities" as the object of monitoring.
- Linking operational effectiveness considerations of business processes to the achievement of internal control objectives.

The outcomes (Attributes) of the "Financial Reporting Information" and "Internal Control Information" processes (Principles) of the Information and Communication component ensure that the suitable and sufficient information are available as persuasive evidences for concluding on effectiveness of internal controls.

Systems based audit approach and COSO based, ISO/IEC 15504 conformant process assessment

Traditional interpretation of systems based auditing is driven by the actual systems in place and controls are related to these. It assumes that the systems in place cover all risks and frequently relies on "internal control questionnaires", that is standard documents used every time an audit is carried out. Risk based auditing experts call the attention of the dangers of these questionnaires comparing them to risk based approach [7]:

- *The questionnaires can be incomplete. In particular, they might not check the management of all significant risks.*
- *Since many are not linked to risks, there is no indication as to the importance of the test and the consequence if the control tested is found to be ineffective.*
- *They can lead to a 'box ticking' exercise by staff anxious to hit the budgeted time, without gaining an understanding of what they are doing. In this way, major risks, which are not being managed properly, may be missed.*
- *They don't encourage management to identify and control their risks.*

Mapping and applying the COSO and COSO ERM main objective categories into the capability dimension of the measurement framework can avoid these potential drawbacks. Targeting capability profiles by the assessment sponsor gives effective tool to the management to identify, understand and manage control risk areas. By achieving level 4 attributes for selected control processes, management can implement risk management principles in a cost effective way.

The proposed assessment model, consisting both process and capability dimensions, enforces not only the simple usage of the "internal control questionnaires" and checklists, but also considering the relevant set of the assessment indicators. Keeping the standard requirements of the ISO/IEC 15504 conformant assessment process helps to implement this advanced measurement concept into the internal and external audit procedures standardized by different ways in different sectors. The control

risk assessment method derived from ISO/IEC 15504 provides an adequate tool for avoiding traditional drawbacks of systems based auditing.

The next figure illustrates how the risk and control tools presented by the COSO publications and the ISO/IEC 15504 conformant assessment concept can be applied together:

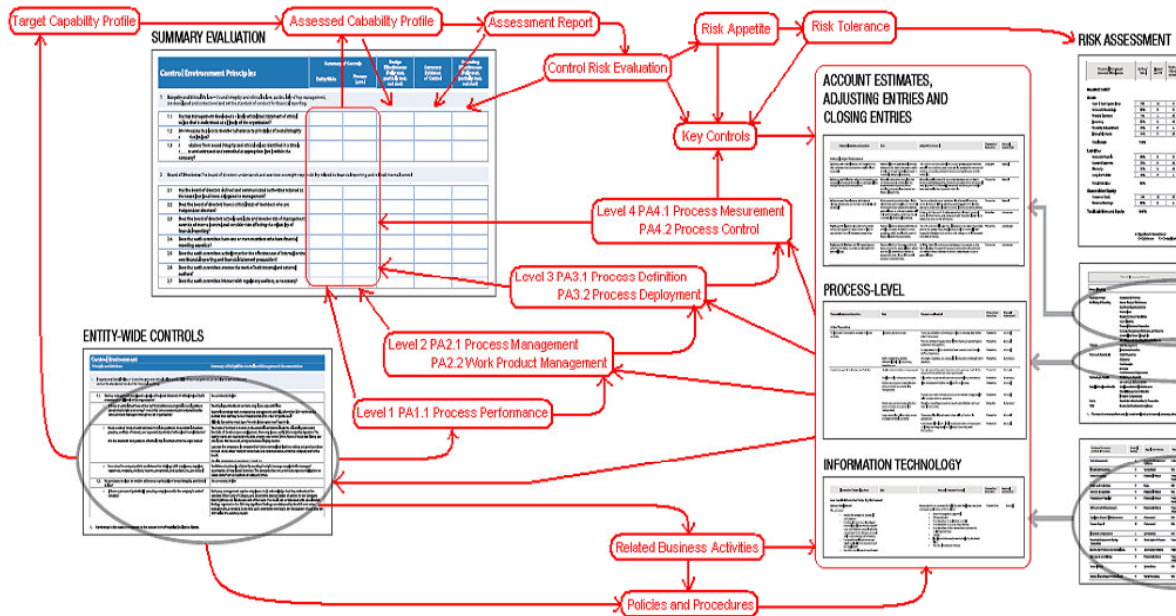


Figure 13: COSO Control Matrices and ISO/IEC 15504 Assessment

The proposed Process Assessment Model is directed at assessment sponsors (executive managers) and competent assessors (auditors) who wish to select and implement a model, and associated documented process method, for assessment for either *capability determination* (assurance audit engagements) or *process improvement* (consulting audit engagements). Additionally it may be of use to developers of assessment models in the construction of their own model, by providing examples of good control and management practices.

In this context the different terminologies used for *compliance* (or regulatory), *financial* and *performance* audits can be mapped to the capability dimension of this COSO based Process Assessment Model. In some regulatory circumstances compliance requirements measured at level 1 also enforce fulfilment of level 3 (operational) process attributes for a well-defined set of processes from control activities. The nature of similar overlaps in objectives of different audit types can be explained and supported by using ISO/IEC 15504 process assessment principles and techniques.

The COSO based process assessment principles presented in this paper were used for development of the Skill Card and the related training materials of the “Certified European Internal Financial Control Assessor” programme including adaptation of the Principles, Attributes and Approaches of the COSO 2006 Guidance as agreed with the COSO Board for Spanish, German, Romanian and Hungarian translations. This project (Project number: HU/B/05/B/F/PP-170013) was carried out with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme. By utilizing the final results of the pilot project, Europe-wide training providers offer the certification and training programme accredited by the European Certificates Association (<http://www.eu-certificates.org/>) from September 2007. Working groups of SAI, IIA, ISACA and ISO/IEC 15504 communities are invited for future cooperation. See more details at <http://www.training.ia-manager.org/> or contact to ivanyos@memolux.hu.

References

- [1] Information Systems Audit and Control Foundation, IT Governance Institute: COBIT - Control Objectives for Information and related Technology
- [2] The Committee of Sponsoring Organizations of the Treadway Commission (COSO):
 - Internal Control — Integrated Framework (1992)
 - Enterprise Risk Management – Integrated Framework (2004)
 - Internal Control over Financial Reporting — Guidance for Smaller Public Companies (2006)
- [3] ISO/IEC 15504-1:2004 Information technology -- Process assessment -- Part 1: Concepts and vocabulary
ISO/IEC 15504-2:2003 Information technology -- Process assessment -- Part 2: Performing an assessment
ISO/IEC 15504-2:2003/Cor 1:2004
ISO/IEC 15504-3:2004 Information technology -- Process assessment -- Part 3: Guidance on performing an assessment
ISO/IEC 15504-4:2004 Information technology -- Process assessment -- Part 4: Guidance on use for process improvement and process capability determination
ISO/IEC 15504-5:2006 Information technology -- Process Assessment -- Part 5: An exemplar Process Assessment Model
- [4] Key Controls: The Solution for Sarbanes-Oxley Internal Control Compliance, Vorhies,J.B, The IIA Research Foundation, 2004
- [5] The Institute of Internal Auditors (The IIA): The International Standards for the Professional Practice of Internal Auditing
- [6] Professional Practices Framework, The IIA Research Foundation, March 2004
- [7] Risk based internal auditing - an introduction, David M. Griffiths, 30 January 2006

Larry E. Rittenberg, PhD, CPA, CIA
Chairman,
The Committee of Sponsoring Organizations of the Treadway Commission

9 June 2008

Sent by email to lrittenberg@bus.wisc.edu

Dear Mr. Rittenberg,

Thank you for the opportunity to provide feedback on COSO's exposure draft, *Guidance on Monitoring Internal Control Systems*.

At first I would like to highlight our interest and position regarding COSO models and their supporting guidance documents:

My company Memolux Ltd. coordinated a pan-European training initiative called "*European Internal Financial Control Assessor*" co-financed by the European Commission during 2005-2007. The key objective of this training programme is setting up a modular structure of internal controls for financial reporting, which is commonly applicable in each sector under related specific regulatory directives. This modular structure is the base for applying standard assessment method for evaluating effectiveness and efficiency of internal control systems. The features – called Principles, Attributes and Approaches in the COSO 2006 Guidance - of internal financial control processes and the adaptation of the *ISO/IEC 15504 process assessment methodology* are presented at the training courses containing online and traditional learning elements.

The COSO internal control framework and the ISO/IEC 15504 process assessment methodology were used for the development of the skill card and the related training materials of the "*European Internal Financial Control Assessor*" programme including adaptation of the Principles, Attributes and Approaches of the COSO 2006 Guidance as agreed with the COSO Board for *Spanish, German, Romanian, and Hungarian translations* in the fall of 2006.

The success of the pilot trainings and the positive feedbacks from some national IIA chapters provided us opportunities for disseminating the applied methodology in the ECIIA 2007/2 Newsletter and at pan-European IIA events in Hungary, Croatia, Austria, Czech Republic, Slovakia, and during the IT Symposium of the 2007 IIA Global Conference in Amsterdam.

For developing and delivering professional trainings in multi-lingual environment for internal financial control assessors, we evidently focus both on the conceptual issues and the presentable practical examples. By these reasons our training partners from some European countries are also strongly interested in using the new *Guidance on Monitoring Internal Control Systems*.

We will send our detailed response by using the on-line form by 15 August 2008, but in this letter I would like to highlight some conceptual issues and a possible methodological approach in advance for further considerations. Some brief comments on the new version as follows:

- The current version is much more structured than the first one and together with the underlying examples it presents a huge knowledge library for evaluating internal controls. However the size and the content structure of the Guidance Volumes are applicable more for an overall COSO *implementation* guide than just for the monitoring guidance.
- The current Model for Monitoring is based more adequately on the risk management concept than in the first draft. However there are some unclear *overlaps with the other components* of the COSO model. Even the first draft referred “root-cause analysis” as a distinguishing feature of monitoring from control activities. This approach seems to be under considered in the new version.
- The reference to the *COSO ERM* model is still very limited, which will certainly cause misunderstanding within the target audience. Figure 1 of the Executive Summary is modified a bit from the original one (of the 2006 Guidance), however just changing the “financial reporting objectives” into “organizational objectives” does not mean clear message about how the supplementary components (Objective Setting, Event Identification, Risk Response) of the ERM model should be applied.
- It is not clear how the *risks of control failures* should be prioritised for designing and executing monitoring procedures. What are the organizational objectives regarding effectiveness and efficiency of the internal control system, how much risk the management and the board are willing to accept, and how can these targets be measured (in the form of “risk tolerance” and “risk appetite”)? Answering these questions is a precondition for risk-based evaluation of effectiveness and efficiency of internal control system.
- Figure 4 of Volume II also represents the above-mentioned conceptual problems. While the 2006 Guidance focused on the Component dimension of the COSO cube, this Guidance provides a view of the internal control system from the business operations (units/activities) dimension. Paragraph 10 of Volume II clearly states, that monitoring should consider “how the *entire* internal control system manages the risks”, however the presented monitoring model and application techniques are focusing much more on implementing *control activities* (which is otherwise very useful!) than assessing the effectiveness and efficiency of the entire internal control system.

For “balancing” the activity dimension of the proposed Monitoring model, we suggest to build up the third COSO dimension’s aspect as well. This would also represent a direct reference to the ERM model by providing means for the management and the board in defining risk appetite and organizational objectives with related tolerance regarding the entire internal control system. One potentially applicable “capability” (“maturity”) based approach is presented briefly below:

Applicability of the ISO/IEC 15504 capability levels to the COSO main objective categories

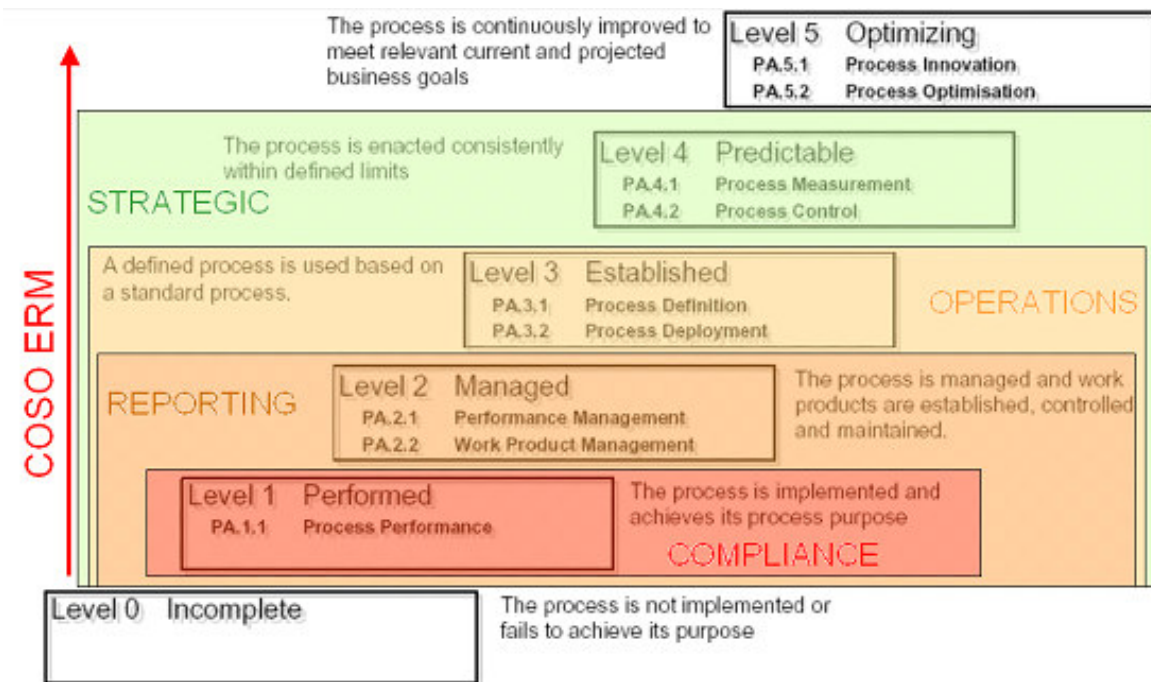


Figure 1: ISO 15504 capability levels and COSO objective categories

Mapping and applying the COSO and COSO ERM main objective categories into the capability dimension of the ISO 15504 measurement framework provide guidance to set target capability profiles by the assessment sponsor, give effective tool to the management to identify, understand and manage control risk areas.

Evaluating internal control process related risk

The Control Risk Assessment performed on ISO 15504 conformant process assessment results, provides feedback to the management whether the existing gaps between the target and assessed capability profiles represent acceptable control risk level for the sponsor.

This approach provides more flexible and customisable method to evaluate the system of internal (financial) controls, necessary to define the coverage of the substantive examinations of the economy, efficiency and/or effectiveness of the organisations, activities, programmes or functions concerned.

ISO/IEC 15504 standard provides guidance on how to utilise a conformant process assessment within a process improvement programme or for process capability determination.

Setting target capability

The sponsor should determine which processes (Principles) from the selected Process Reference Model (based on the COSO 2006 Guidance) are (most) important for the pre-defined requirements (Process Capability Determination) or business goals (Process Improvement).

Also the sponsor should specify a target process profile, showing which process attributes are required for each selected process. Also the necessary rating for each process attribute should be given. Only ratings of “Fully achieved” or “Largely achieved” should be set. “Partially achieved” rating has no meaning to set, as this would indicate that the achievement would be unpredictable in some aspects. “Not required” should be noted for a process attribute taken to be unnecessary.

The set of target process profiles expresses the target capability, which the sponsor judges to be adequate (to the organization’s business risk appetite and tolerance). Figure 2 presents example target and assessed process profiles for 5 selected sample Internal Financial Control processes:

Process		Process Attributes									
		Performed		Managed		Established		Predictable		Optimizing	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2	
IFC.CE.IEV Integrity and Ethical Values	Target	F	L	L							
	Assessed	F	F	L							
IFC.RA.FRO Financial Reporting Objectives	Target	F	F	F	F	F	L	L			
	Assessed	F	F	F	F	L	L	L			
IFC.CA.PP Policies and Procedures	Target	F	F	F	L	L					
	Assessed	F	P	L	F	L					
IFC.IC.IC Internal Communication	Target	F	F	F	F	F					
	Assessed	P	II	II	II	II					
IFC.MO.RD Reporting Deficiencies	Target	F	F		L	L					
	Assessed	L	L	L	L	L					
Keys											
		F	Fully achieved				L	Largely achieved			
		P	Partially achieved				II	Not achieved			
		Not required/assessed									

Figure 2: Example target and assessed process profiles

Gap assessment

Process-related risk can be inferred from the existence of gaps between the target and the assessed process profiles.

The potential consequence of a gap depends on the capability level and the process attributes where the gap identified. Some Internal Financial Control related considerations and examples (by using the above example process profiles) are presented as follows:

- Typical consequence of the gap at Level 1 PA 1.1 Process performance attribute is that not all of the relevant process outcomes (Attributes of COSO Principles) are achievable, and no recoverable documentation exists to track the necessary control. E.g. Management communication to personnel in roles affecting financial reporting is not adequately documented, so updates on internal or external finance matters are not taken into consideration.
- At Level 2 PA 2.1 Performance management gap, the typical consequences are the missing deadlines, lack or inefficient use of resources, unclear responsibilities, uncontrolled decisions, etc. E.g. Management communication with oversight board or personnel is not planned or scheduled; the related management does not do deficiency disclosure in time; unauthorized decisions are done at period closing; policies and procedures are not under revision on a timely base.
- At Level 2 PA 2.2. Work product management attribute, the gap can cause unpredictable quality of reports, parallel entries and inconsistent documentation, increased rework cost, consolidation problems. E.g. Old versions of policies and procedures are also in use; identified exceptions are not communicated; internal communication is not filed in a systematic way.
- At Level 3 PA 3.1 Process definition gap, the consequences are that best practices and learnt lessons are not taken into account during revision of policies and procedures or the outcomes of the related control processes are not identical in the operational procedures. E.g. Missing or formal description of internal communication procedures withhold staff members to use alternative reporting lines informing oversight board about material weaknesses or improvement suggestions.
- At Level 3, the PA 3.2 Process deployment gap can cause inconsistent applications of financial controls built into the operational procedures. Identified opportunities are lost due to inefficient deployment effort. E.g. The oversight board does not take the internal auditor's consultative role and efforts seriously; the financial statement assertions are not properly linked to the business processes during risk assessment; information technology controls do not reflect adequately to the complexity of the IT environment.
- At Level 4 PA 4.1 Process measurement gap, the consequences are that the key controls are not properly identified, designed or operating in order to achieve process performance objectives and business goals or detect performance problems early. E.g. the resolution of key control exceptions is not covered in risk assessment.

- At Level 4 PA 4.2 Process control gap, the consequences are that the quantitative performance objectives and the defined business goals do not meet. E.g. Short monthly/yearly closing deadline can cause unpredictable materiality of accruals, management estimates and reserves.

Analysing control process related risk

The process attribute gap - presented in the previous part - can be categorized into “None”, “Minor” and “Major” categories based on the distance of target and assessed ratings. E.g. one-step gap is evaluated as minor, two or more steps distance deems major gap in case of “Fully achieved” attribute target. At “Largely achieved” target even the one step distance (“Partially achieved”) means major gap.

The *probability* of problem occurrence is derived from the extent of process attribute gaps and from the capability level where they occur. Capability level gaps are categorized as follows:

- None - No major or minor gaps
- Slight - No gap at Level 1, and only minor gaps at higher levels
- Significant - A minor gap at Level 1, or a single major gap above
- Substantial - A major gap at Level 1, or more than one major gap above

The process related risk depends on both the *probability* of problem arising from the identified gap and the potential *consequence*. In general the consequences depend on the capability levels where the gaps occur.

As it is shown in Figure 3, the high risk arises from a substantial gap at a lower capability level.

Consequence Indicated by capability level where gap occurs	Probability Indicated by extent of capability level gap		
	Slight	Significant	Substantial
5 – Optimizing	Low Risk	Low Risk	Low Risk
4 - Predictable	Low Risk	Low Risk	Medium Risk
3 - Established	Low Risk	Medium Risk	Medium Risk
2 - Managed	Medium Risk	Medium Risk	High Risk
1 - Performed	Medium Risk	High Risk	High Risk

Figure 3: Risks associated with capability levels

If risks are identified at more capability levels, then the highest risk measure shall be considered as the process related risk.

Based on the presented approach risk analysis shall determine which process or processes represent the greatest degree of risk. Figure 4 presents examples of Internal Financial Control related risk assessment using example process profiles from Figure 2, where the process profiles showed gap at 3 internal financial control processes:

- IFC.RA.FRO - Financial Reporting Objectives;
- IFC.CA.PP - Policies and Procedures; and
- IFC.IC.IC - Internal Communication

IFC.RA.FRO - Financial Reporting Objectives

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	L	L
Assessed profile	F	F	F	F	L	L	L
Process attribute gap	-	-	-	-	minor	-	-
Capability level gap	-	-		slight		-	
Capability level risk	-	-		low		-	
Process related risk	low						

IFC.CA.PP - Policies and Procedures

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	L	L	-	-
Assessed profile	F	P	L	F	L	-	-
Process attribute gap	-	major	minor	-	-	-	-
Capability level gap	-	significant		-		-	
Capability level risk	-	medium		-		-	
Process related risk	medium						

IFC.IC.IC - Internal Communication

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	-	-
Assessed profile	P	N	N	N	N	-	-
Process attribute gap	major	major	major	major	major	-	-
Capability level gap	subst.	substantial		substantial		-	
Capability level risk	high	high		medium		-	
Process related risk	high						

Figure 4: Internal Financial Control related risk assessment examples

Reasons for internal financial control process improvement

As presented in the previous part, internal control process related risk evaluation is based on the gaps between the target and the assessed process attribute ratings. Setting lower target capability for internal financial control processes is theoretically explainable if the inherent risk of the financial reporting activities and the related business administration processes is measured at very low level or the inherent risk is acceptable to fulfil regulatory compliance requirements. Otherwise Level 2 capability target is the adequate minimum requirement to assess control procedures against reliability objectives of financial reporting.

In more complex environment (featured by business type, size, sectoral regulations, etc.) the continual improvement of business administration processes is desirable. Integration of financial controls with business operations is necessary, when not only the reliability, accuracy and availability of the financial information are critical, but the effectiveness of the related operational activities is also required. Assessing internal financial controls, together with the business processes where they are embedded, against up to Level 3 process attributes is reasonable for the big or multinational organizations, publicly listed companies under SOX regulation, financial institutes, and specific public service companies managing public funds.

Process Capability Determination

The purpose of process capability determination (PCD) is to identify the strengths, weaknesses and process related risks associated with selected processes with respect to *a particular specified requirement*.

The terminology of particular specified requirement originally meant supplier selection criteria, however the new standard approach is more generalized. The PCD assessment is somehow an extended compliance audit or review, where the specified compliance criteria are translated into target capability profiles of the selected processes. The difference from process improvement (PI) approach is that the PCD main goal is to identify the alterations and to determine the potential risks coming from alteration comparing to the pre-defined (e.g. external) requirements.

Monitoring internal control systems

As the COSO materials refer to the fifth component: internal control systems are monitored to assess the quality of the system's performance over time. Monitoring is designed to ensure that internal control continues to operate effectively.

Using ISO 15504 process assessment principles and techniques contributes to the development of innovative approaches in monitoring the effectiveness of internal control in the following aspects:

- Providing Assessment Model for all internal control components and principles by using the COSO 2006 Guidance (based Process Reference Model).
- Offering tools for internal control risk assessment supporting the communication of internal control weaknesses and the considerations of necessary corrective actions.
- Focusing on specific and generic assessment indicators applicable for compliance, reliable reporting, operational effectiveness and strategic objectives.
- Applying assessment indicators for collecting evidences from business activities and entity/corporate levels, as well.
- Differentiating “internal controls” as a system from the underlying “control activities” as the object of monitoring.
- Linking operational effectiveness considerations of business processes to the achievement of internal control objectives.

The outcomes (Attributes) of the “Financial Reporting Information” and “Internal Control Information” processes (Principles) of the Information and Communication component (from the COSO 2006 Guidance) ensure that the suitable and sufficient information are available as persuasive evidences for concluding on effectiveness of internal controls.

Systems based audit approach and COSO based, ISO 15504 conformant process assessment

Traditional interpretation of systems based auditing is driven by the actual systems in place and controls are related to these. It assumes that the systems in place cover all risks and frequently relies on “internal control questionnaires”, that is standard documents used every time an audit is carried out. Risk based auditing experts call the attention of the dangers of these questionnaires comparing them to risk based approach:

- *The questionnaires can be incomplete. In particular, they might not check the management of all significant risks.*
- *Since many are not linked to risks, there is no indication as to the importance of the test and the consequence if the control tested is found to be ineffective.*
- *They can lead to a ‘box ticking’ exercise by staff anxious to hit the budgeted time, without gaining an understanding of what they are doing. In this way, major risks, which are not being managed properly, may be missed.*
- *They don’t encourage management to identify and control their risks.*

(Risk based internal auditing - an introduction
David M. Griffiths, 2006)

Mapping and applying the COSO and COSO ERM main objective categories into the capability dimension of the measurement framework can avoid these potential drawbacks. Targeting capability profiles by the assessment sponsor gives effective tool to the management to identify, understand and manage control risk areas. By achieving level 4 attributes for selected control processes,

management can implement risk management principles in a cost effective way.

The proposed assessment model, consisting both process and capability dimensions, enforces not only the simple usage of the “internal control questionnaires” and checklists, but also considering the relevant set of the assessment indicators. Keeping the standard requirements of the ISO 15504 conformant assessment process helps to implement this advanced measurement concept into the internal and external audit procedures standardized by different ways in different sectors. The control risk assessment method derived from ISO 15504 provides an adequate tool for avoiding traditional drawbacks of systems based auditing.

In case of any interest of re-using or further developing the above presented assessment approach, please don't hesitate to contact me:

János Ivanyos
IIA Hungary – IT section

Address: 1024 Budapest
Keleti K. u. 46.
Hungary
Tel./Fax: +36 1 336 1505 / +36 1 336 1506
E-mail: janos.ivanyos@iaa.hu
ivanyos@memolux.hu

Yours sincerely,



János Ivanyos
managing director
Memolux Ltd.

Cc David A. Richards,
R. Trent Gazzaway