Implementing COBIT based Process Assessment Model for Evaluating IT Controls

By János Ivanyos, Memolux Ltd. (H)

Introduction

New generations 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 is 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 catalysts 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, audit committees, the internal and external auditors and even for the supervisory bodies to assess the effectiveness of enterprise risk management and internal controls over IT processes.

This paper provides a summary to the principles of the proposed Process Assessment Model for evaluating IT Controls based on COBIT 4.1 in accordance with the requirements of ISO/IEC 15504-2. However the same approach is applicable for setting up Process Assessment Model for Internal Financial Controls, as the control processes defined by the COSO 2006 Guidance are also conformant with the ISO/IEC 15504-2 requirements.

COBIT 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, directly derived from COBIT 4.1, has been used as the basis for the proposed IT Control Process Assessment Model. This COBIT based Process Reference Model associated with the process attributes defined in ISO/IEC 15504-2, provides a common basis for performing assessments of IT control process capability and reporting of results by using a common rating scale.

As Figure 1 presents, 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.
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) A process shall be described in terms of its Purpose and Outcomes.

  b) In any description the set of process outcomes shall be necessary and sufficient to achieve the purpose of the process.

  c) Process descriptions shall be such that no aspects of the measurement framework … beyond level 1 are contained or implied.

The COBIT 4.1 definition of control processes is in compliance with the PRM requirements of the ISO/IEC 15504-2 as shown in Figure 2:
The proposed Process Reference Model includes processes, which are grouped in four process categories, identical to the control domains as defined in the COBIT framework:

- **Plan and Organise (PO)** - Provides direction to solution delivery (AI) and service delivery (DS)
- **Acquire and Implement (AI)** - Provides the solutions and passes them to be turned into services
- **Deliver and Support (DS)** - Receives the solutions and makes them usable for end users
- **Monitor and Evaluate (ME)** - Monitors all processes to ensure that the direction provided is followed

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

The 34 IT control processes derived from COBIT 4.1 that are included in the process dimension of the proposed IT Control Process Assessment Model, are listed below:
Assessing IT Control Systems

Plan and Organize (PO)

PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organisation and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

Acquire and Implement (AI)

AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

Deliver and Support (DS)

DS1 Define and Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations

Monitor and Evaluate (MO)

ME1 Monitor and Evaluate IT Performance
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Compliance with External Requirements
ME4 Provide IT Governance

For the process dimension of the proposed IT Control Process Assessment Model, all the 34 IT control processes referred by COBIT 4.1, are included. 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 as presented in Figure 3:

![Process Attributes by capability levels](image)

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.

![Four point ordinal scale for evaluating the achievement of process attribute](image)

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 1 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.

The 0-2 capability level attributes are focusing on the instance view of the process (even if it operates
at entity level) while from level 3 the attributes are focusing on the corporate entity aspects. This
observation helps us to understand how the COBIT performance measurement concept fits to this
assessment model. Goals and metrics are defined in COBIT at three levels:

- **IT goals and metrics** that define what the business expects from IT and how to measure it
- **Process goals and metrics** that define what the IT process must deliver to support IT’s
  objectives and how to measure it
- **Activity goals and metrics** that establish what needs to happen inside the process to achieve
  the required performance and how to measure it

Figure 6 shows how COBIT links different level goals and metrics to support entity (or operational unit)
level business goals, as outcome measures become performance drivers of upper level goals:
Applying Enterprise Risk Management concept on IT Controls

In COSO Enterprise Risk Management (ERM) terminology, the 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 (measured via ratings of the process attributes), which the sponsor judges to be adequate to the organization’s business risk appetite and tolerance.

**Objectives Setting**

Entity or operational unit level objectives with their acceptable variations should be defined by using adequate metrics (indicators). Normally this is not difficult as business objectives of any organization or operational processes represent - easily quantifiable - value creation or protection.

However the quantification of risk appetite (crucial for risk management) is not evidential. The importance of the problem is derived from that risk appetite is the base for ranking risks during risk

---

Figure 6: Example of linking different levels of goals and metrics in COBIT
assessment for supporting the decision on selecting of the potential risk responses. If there are no objectively applicable indicators of risk appetite for neither entity nor operational levels, then the next steps of risk management will be processed based on incidental, subjective decisions.

Enterprise Risk Management (like in the case of COSO ERM model) sets objective categories. The strategic, operations, reporting (reliability) and compliance objectives should be investigated through the achievement of business goals concerning either the organization (in ERM), or the operational units and processes (in case of integrated control systems, like COBIT or COSO). Though different (performance, IT or financial, compliance, etc.) audit types can be defined based on the objective categories, it is evident that these categories can exist only in interconnection. Next Figure presents how the interconnection of these objective categories can be explained by ISO/IEC 15504 capability levels using the “outcome measures - performance drivers” relations from COBIT performance measurement concept.

Figure 7: Measurement of COSO objectives by ISO/IEC 15504 capability levels

One potential approach is that these objective categories are building on each other. Achievement of compliance objectives at operational (business) process level ensures that business activities are performed according to the prescribed or selected requirements of IT (or other internal) controls by achieving the IT process goals through the activity goals. Objectives of reliable operation – by achieving goals of reliable IT operation - presume the fulfillment of the compliance requirements, so the entity’s risk appetite related to the operational (business) processes can be defined by using of the indicators of the compliance requirements based on COBIT process definition.

The objectives of the effective and efficient operations related to operational units (achieving business goals) presume the fulfillment of reliable IT operation and compliance requirements. At this level, the entity’s risk appetite can be prescribed by using the indicators of reliable IT operation and compliance (to COBIT process) requirements.
Regarding the whole organization, the strategic objectives - broken down into defined business goals at operational unit levels – presume the fulfilment of effective and efficient operations, reliability and compliance requirements. For the whole organization, the entity’s risk appetite can be described by using the indicators of the prescribed effectiveness, reliability and compliance (to COBIT process) requirements for operational units, processes and business activities.

Notice the consequence of adapting risk management on IT (or other internal) control system of the organization concerning the organization-level risk tolerance (acceptable level of variation around entity’s control objectives) and risk appetite: The risk appetite for organizational risk strategy can be described by using the indicators of the overall IT (or other internal) control system requirements. So the consistent enterprise risk management presumes that the operation of IT (or other internal) control system of the organization is measurable by adequate indicators. These indicators play roles in setting objectives regarding IT (or other internal) control systems, as they are applicable for describing risk tolerances at defined levels. The indicators used for setting risk tolerance of lower level objective categories can be applied to define risk appetite of the next objective category level.

COBIT performance measurement also refers to the above approach as the outcome measure represents a performance indicator driving the higher-level business, IT function or IT process goal as shown on Figure 6.

In case of enterprise operation at less risk-awareness level, the strategic and business objectives are linked directly to business activities. In this case, there is no objectives (requirements) setting for the IT or other internal control system, so not only the consequent adaptation of control and risk management frameworks become unrealistic, but the withdrawal of using objectively applicable risk appetite of the organization causes incidental and subjective decisions in ranking of risks related to business activities.

Applying the COBIT performance measurement concept to the ERM objective categories helps us to understand how the capability dimension of the ISO/IEC 15504 measurement framework is adaptable. The capability dimension provides guidance to set target capability profiles by the assessment sponsor, and gives effective tool to the management to identify, understand and manage control risk areas. Figure 8 identifies the applicability of the capability levels for the assessment of the COBIT-based IT control systems:

![ISO/IEC 15504 capability levels for assessing COBIT-based IT control systems](image-url)
COBIT provides metrics only up to the IT goals. While they are also performance indicators for the business goals for IT, COBIT does not provide business goal outcome measures. That is one cause why applying the ISO/IEC 15504 capability dimension expands over the usability of COBIT maturity concept.

In COBIT, a generic definition is provided for the COBIT maturity scale rated from non-existent (0) to optimised (5), but interpreted for the nature of COBIT’s IT control processes, so a specific model is provided from the generic scale for each of the 34 processes. As shown in Figure 5, the achievement of the process attributes of ISO/IEC 15504 capability levels are measured by generic indicators from level 2, and those are independent from the nature of the assessed process. By this way the control processes from different domains specified by more than one Process Reference Models can be integrated into one Process Assessment Model. For example IT controls and financial controls can be evaluated together based on the same measurement framework of ISO/IEC 15504.

Figure 9 presents the general concept of how the ISO/15504 capability measurement is applicable for assessing internal control systems implementing the most accepted control frameworks such as COBIT and COSO. The presented 3 dimensions are those derived from the COSO enterprise risk management and internal control models:

- Management supervision and control of business processes and activities
- Governance processes supporting the design and operation of internal control system
- Objective categories measuring achievement of entity-level and operational goals

![Figure 9: Assessing COSO and COBIT based internal control systems](image-url)
Achieving “Compliance” Objective at Performed Process (Level 1)

The process dimension of the IT control assessment model adopts the process definitions of COBIT 4.1. The achievement of the process performance attributes represents that the management has good understanding of the basics of the IT control requirements and the business activities are managed by keeping in mind the IT control framework in an ad hoc base. There are evidences of achieving IT control process purpose, however not in a managed way.

The level 1 assessment results are mainly usable in further process improvement context.

Achieving Compliance objectives of all (relevant) IT control processes from the COBIT 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 compliance of IT activities cannot utilize these results. For example: a chain of control/audit procedures cannot reuse the level 1 assessment results at different management levels, like in the case of complex organizational or operational structures.

Achieving “Reliable IT Operation” Objective at Managed Process (Level 2)

This level represents that the Performed control process (already achieving compliance to COBIT objectives at level 1) is implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained. This level means that the achievement of the relevant goals of reliable IT operation is evidenced in a traceable way (evidences are sufficient and suitable for external bodies).

Besides level 1 achievement, the IT control process is managed and fulfils the reliable IT operation objective. At level 2 assessment the IT related business activities shall be investigated, whether the performance and work product management indicators related to the IT control processes are assessable and how they are evidenced.

At this level, the business activities are not only supported by comprehensive entity-level controls (as already resulted by level 1 achievements of the full set of IT control processes). Moreover, the performance and work products of the IT control processes are appropriately managed even at process levels; 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 IT related business activities.

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

Achieving “Effective and Efficient Operation” Objective at Established Process (Level 3)

At this level the Managed process (already achieving compliance and reliable IT operation objectives at level 2) is implemented by using a defined process capable of achieving its process outcomes and the relevant business goals.

Besides level 1 and 2 achievements, the IT control process is built into the operational processes regulated by entity level policies and procedures, and fulfils the objective of “Effective and Efficient Operation”. At level 3 assessment the IT related business activities should be investigated together with the entity level policies and procedures, whether the process definition and deployment indicators related to the business (operational) processes are assessable and evidenced.

The IT enabled 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 context to the
process dimension, level 3 type assessment of the full set of IT control processes has only limited additional value in comparison to level 2 achievements. As presented later, adding key controls to the process dimension represents specific implementation scope of the policies and procedures.

Setting different target levels for a subset of the processes from the COBIT 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 provides more reasonable assurance regarding the achievement of compliance (to COBIT process requirements) and reliable IT operation objectives. For example level 3 Monitor and Evaluate (MO) processes enhancing internal audit functions have real additional value for any type of organizations targeting lower capability levels for other IT control processes.

Level 3 achievements have some significant consequences. Firstly, 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 IT or other 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 IT 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 influences the minimum scope and coverage of level 3 standardization. In context of ERM, 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 either selected control processes from the basic set of the Process Reference Model or a subset of the relevant business processes operating at entity or even activity levels, with which the process dimension of the assessment model is necessarily extended.

As pointed out earlier, the ISO/IEC 15504 capability level 3 considerations go beyond the boundaries of COBIT’s performance and maturity measurements.

Achieving “Strategic” Objective at Predictable Process (Level 4)

At this level the Established process (already achieving compliance; reliability; 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 IT 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 are 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 IT control process and/or the related business processes, where control outcomes are built in, comprise key control.

“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 control objectives linked directly or indirectly to specific business objectives, the management will be able to adequately react to external and internal events representing inherent risks to IT related operation.

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 indicates that exceptions are handled within the accepted deviation (risk tolerance) at the settled risk levels (risk appetite) of the desired business objective. Financial impact shall be reasonably estimated and the resolution to the control exception shall be identified, scheduled and followed.

Evaluating IT 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 IT controls, necessary to define the coverage of the substantive examinations of the economy, efficiency and/or effectiveness of the organizations, 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).

Analysing Control Process related Risk based on Gap Assessment

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

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.

The process attribute gap 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 \textit{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 \textit{probability} of problem arising from the identified gap and the potential \textit{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 major gap at lower capability levels:

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicated by capability level where gap occurs</td>
<td>Indicated by extent of capability level gap</td>
</tr>
<tr>
<td>Slight</td>
<td>Significant</td>
</tr>
<tr>
<td>5 – Optimizing</td>
<td>Low Risk</td>
</tr>
<tr>
<td>4 - Predictable</td>
<td>Low Risk</td>
</tr>
<tr>
<td>3 - Established</td>
<td>Low Risk</td>
</tr>
<tr>
<td>2 - Managed</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>1 - Performed</td>
<td>Medium Risk</td>
</tr>
</tbody>
</table>

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.

COBIT maturity model also allows benchmarking and gap assessment on control deficiencies. However the specific nature of maturity levels of each IT control processes doesn’t allow risk ranking of control deficiencies based on a generic model as of ISO/IEC 15504.

\textbf{Purposes of ISO/IEC 15504 conformant Process Assessment}

The proposed Process Assessment Model is directed at assessment sponsors (executive managers) and competent assessors (IT auditors) who wish to select and implement a model, and associated documented process method, for assessment for either \textit{capability determination} (assurance engagements in audit literature) or \textit{process improvement} (consulting 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.
**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 term of “particular specified requirement” originally meant the supplier selection criteria. However, the ISO/IEC 15504 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.

**Reasons for IT Control Process Improvement**

As presented in the previous part, IT or other 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 IT control processes is theoretically explainable if the inherent risk of the IT activities and the related business processes is measured at very low level or the inherent risk is acceptable to fulfill regulatory compliance requirements. Otherwise level 2 capability target is the adequate requirement to assess control procedures against reliability objectives.

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

**Conclusion on effectiveness of IT controls**

ISO/IEC 15504 conformant process assessment includes not only traditional testing of IT controls, such as walkthroughs confirming adequacy of documentation and design, examination of related documents confirming consistent performance, etc., but it results in inputs for effectiveness considerations. The Process Assessment Profiles are used for making opinion about the effectiveness of control design, namely in what extent the design of controls meets the organizational risk appetite represented by the target control process capability profiles. Additionally the ISO/IEC 15504-4 based Control Risk Assessment provides practical tool for judgement about the effectiveness of control operation, whether the assessed process capability profiles of the IT controls constitute reasonable assurance concerning achievement of related business objectives, such as the low control process related risk levels represent remote likelihood that material weaknesses will not be prevented or detected on a timely basis.

This paper is based on the concept having been implemented for a COSO-based Process Assessment Model of evaluating Internal Financial Controls in accordance with the requirements of ISO/IEC 15504. The principles were presented for the ISO/IEC 15504 community (at SPICE DAYS and EuroSPI conferences) and for the internal audit related professionals (IIA conferences and workshops) in 2007 and 2008. Training materials and online course materials were developed by the financial support of the European Commission, and successful trial courses and exams of the “Certified European Financial Control Assessor” training programme were held in Ireland, Spain, Austria, Hungary and Romania.
References


- Internal Control — Integrated Framework (1992)

ISO/IEC 15504-2:2003/Cor 1:2004


Author’s biographies

János Ivanyos is one of the founders of Memolux Ltd., a Hungarian 70 people in staff accounting and IT service company established in 1989. As managing director he is responsible for Information Technology and Payroll Outsourcing services.

He is the leader of the IT and Quality Assessment section of the Hungarian Institute of Internal Auditors. He is an associate professor at the Budapest Business School and also a lecturer at the Corvinus University, teaching ISO/IEC 15504 based assessment of internal control and enterprise risk management systems. He is leading the “European Internal Financial Control Assessor” job-role committee of the European Certification and Qualification Association. He is a founding member and leader of the Governance Working Group of INTACS, an independent non-profit association aiming to foster the education and experience exchange of ISO/IEC 15504 (SPICE) assessors on a worldwide basis.

He was graduated as an economist at the Karl Marx University of Economics, Budapest in 1984. He has about 25 years experience in IT, and he has successfully managed many technically complex, international (Europe-wide) research and training projects since 1995. He is the author of several papers and proceedings of international conferences about process improvement (EuroSPI, SPICE DAYS) and internal auditing (IIA). The following key articles were published by Wiley:
