Governance SPICE

ISO/IEC 15504 for Internal Financial Controls and IT Management

By János Ivanyos, Memolux Ltd. (H)

1. Evaluating Internal Controls against Governance Frameworks

Corporate Governance is the totality of principles aligned with the shareholders' interests, which strive for transparency and a well-balanced ratio between leadership and control, whilst retaining decision-making ability and efficiency at the highest level of the company. Internal control system integrated with enterprise risk management includes the policies, procedures, practices and organisational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

Regulatory requirements like the Sarbanes-Oxley Act for US SEC registrants and their affiliates (all over the world), the Basel II framework, the Company Law in the EU, the European and national directives for governmental and public sector organizations, etc. require not just the implementation of risk management and internal control systems based on internationally recognized frameworks, but also the periodic disclosure of effectiveness conclusion performed by the executive management. However some of these regulations are still limited to financial reporting, the global crisis showed that wider focus of risk management and internal controls has real business value. In the past 5 years many-many thousands of such periodic assessments were performed worldwide in industry, financial and governmental sectors and the regulators are keen to further develop mandatory rules and guidelines increasing stakeholder's benefit from disclosures.

The global crisis also reminds that many former periodic assessments concluding positive opinion on effectiveness of internal controls were failed at those companies, where the insularly used economic models for risk assessment were not aligned with the time horizon of the strategic business objectives. Accountability of executive management and oversight boards should be established and supported by using integrated assessment models applicable for both operational and financial processes. Those assessment models which can cover the most activity areas relevant for strategic objectives have added value to line managers, executive management, internal and external auditors and oversight bodies, as they help to optimize monitoring efforts of different operations based on common measurement of achieving objectives.

Major governance scandals, independently from the recent global financial and economic crisis, call the attention that not only the basic business operations (production, sales, supply chain, etc.) need to be assessed, audited or certified to the conformance with specific standards, but all the governance related processes. The Satyam case shows that even those big IT companies, which are committed to quality and process improvement issues, can fail to avoid governance breakdowns such as fraudulent financial reporting.

Taking a more in depth look into the reasons as to why corporate governance has failed in recent years, it can be concluded that these are primarily due to shortcomings in risk management and internal control. Within the context of corporate governance, management therefore needs to concentrate above all on the optimisation of operational processes by improving monitoring and controls.

Risk management and control frameworks contribute to improve corporate governance by principles-based reference models, good practices and evaluation methods.

Process capability and organizational maturity issues have come into the view of the management as the huge cost of regulatory compliance activities request consideration of sustainability and added business value of such efforts. This challenge has been answered by utilizing the ISO/IEC 15504 process assessment standard (also called as SPICE) [1] and its evaluation model concept applicable for the executive managers, the boards of directors, the audit committees, the internal and external auditors and the supervisory bodies for assessing the effectiveness of internal controls even in different business units and activities, IT management and financial reporting processes.

The term of "Governance SPICE" refers to the assessment of Governance, Risk Management and Internal Control processes and is based on different concepts:

- Corporate Governance Principles (OECD)
- Recognized Control Frameworks (COSO & COBIT)
- Risk Tolerance and Risk Appetite (as of COSO ERM)
- Performance Measurement (as of COBIT)
- Process Capability Assessment (ISO/IEC 15504-2:2003)
- Evaluating Process-related Risk (ISO/IEC 15504-4:2004)
- Organizational Maturity (ISO/IEC TR 15504-7:2008)

Internal and external audit standards (like IIA and ISA) recommend system based evaluation of existing internal controls against internationally recognized control frameworks like COSO (Internal Control – Integrated Framework) [2] and COBIT (Control Objectives for Information and related Technology) [3]. The contents of these frameworks are applicable to set up Process Reference Models in compliance with ISO/IEC 15504-2 requirements.

The COSO and COBIT based Process Reference Models associated with the process attributes defined in ISO/IEC 15504-2 provide a common basis for performing assessments of process capability regarding internal controls and reporting of results by using a common rating scale. ISO/IEC 15504 offers not only transparent method for assessing performance of relevant internal control processes, but also tools for assessing control risk areas based on the gaps between target and assessed capability profiles.

Audit standards define assurance and consulting engagement types of audit work similarly to the process capability determination and process improvement contexts of ISO/IEC 15504 process assessment. Using COSO or COBIT descriptions for process dimension and ISO/IEC 15504 measurement framework for capability dimension provides common methodology for all parties responsible for implementing and monitoring internal controls even at different operational units of an organization. Mapping target capability profiles to business objectives also helps to put internal controls into the perspectives of Enterprise Risk Management (ERM).

Quality requirements of the international internal and external audit standards force to evaluate the assessment skills, procedures and practices of the auditors/audit departments in making opinion about the internal controls of the audited organization. The proposed training scheme of Governance SPICE also offers transparent ways to auditors/audit departments for acquiring relevant skills and knowledge.

2. ISO/IEC 15504 Process Assessment (SPICE)

2.1 Process Assessment Model

An integral part of conducting an assessment is to use a Process Assessment Model (PAM) constructed for that purpose, related to Process Reference Model(s) (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.

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 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 judgement of the performance and capability of an implemented process.

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.

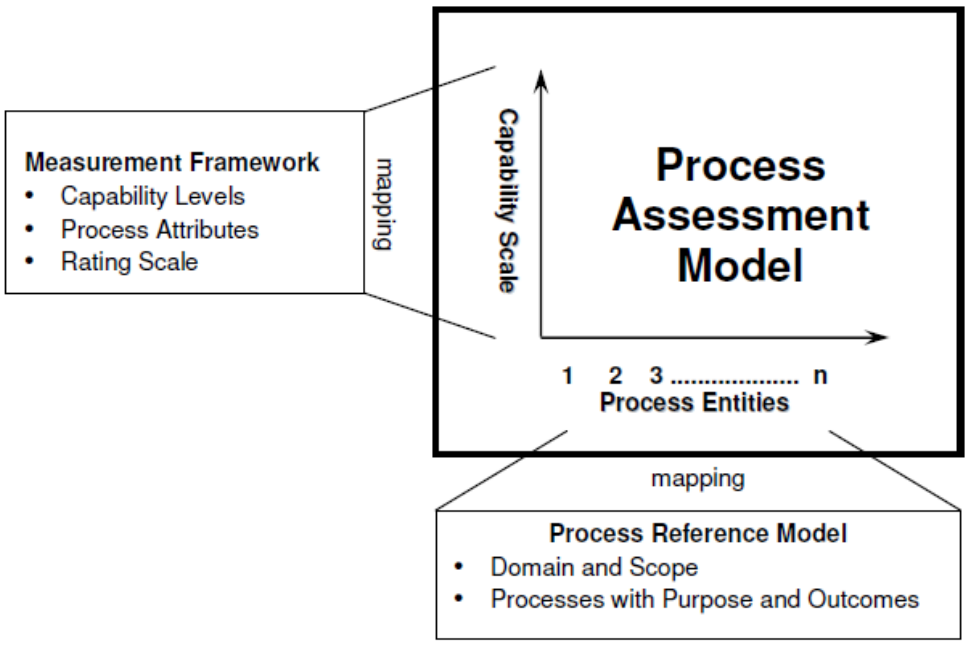


Figure 1: Components of ISO/IEC 15504 Process Assessment

2.2 COSO based Process Reference Model

The Process Reference Model, directly 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 (PRM) 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 COSO 2006 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 - Integrated 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 2006 Guidance as source for the Process Reference Model

The 20 internal financial control processes derived from the 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 understand and exercise 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 entity's organizational structure supports effective internal control over financial reporting.
5. Financial Reporting Competencies (FRC). The organization 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 organization 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 organization, 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 organization, 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* of the proposed Internal Financial Control Process Assessment Model, all the 20 internal control processes referred as Principles in the COSO 2006 Guidance, are included.

2.3 COBIT based Process Reference Model

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 3:

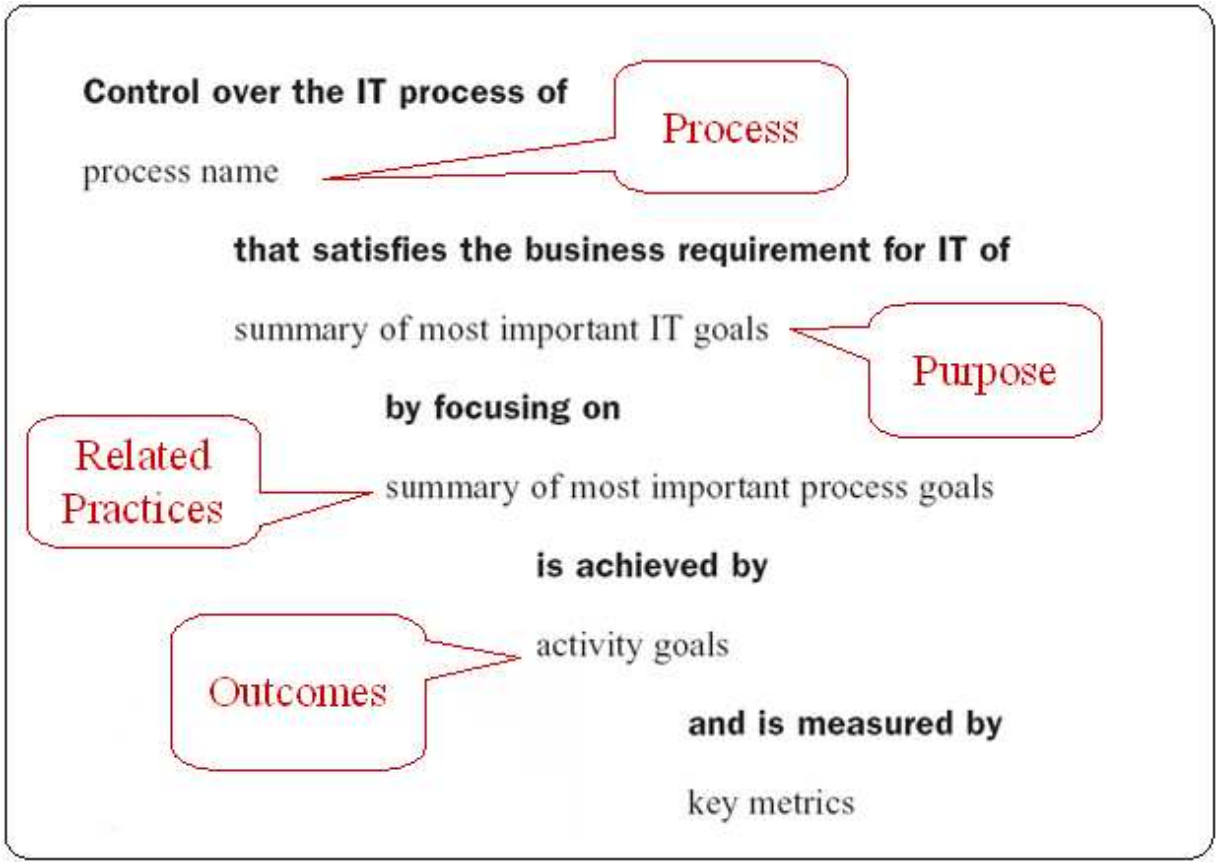


Figure 3: ISO/IEC 15504 conformant process description of COBIT 4.1

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. 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 34 IT control processes derived from COBIT 4.1 are listed below:

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.

2.4 Capability Dimension of the Process Assessment Model

Figure 4 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).

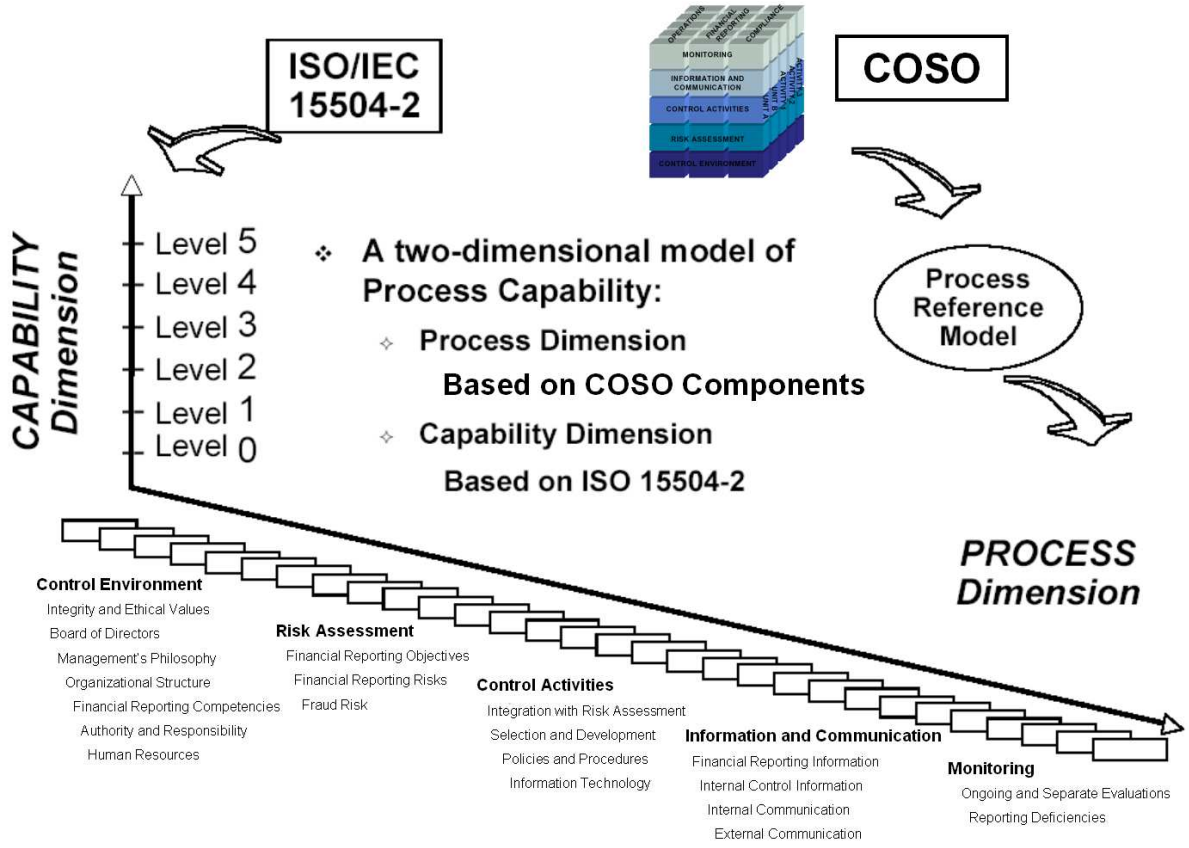


Figure 4: COSO components as process dimension of the Process Assessment Model

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.

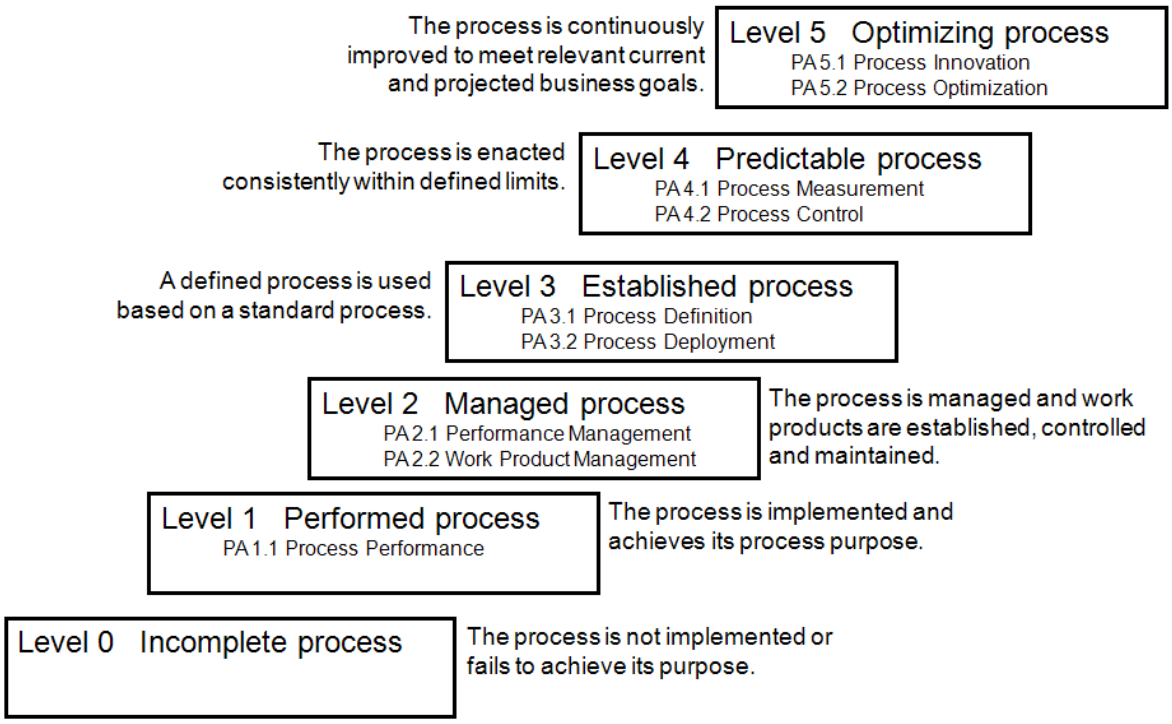


Figure 5: Process Attributes by capability levels

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.

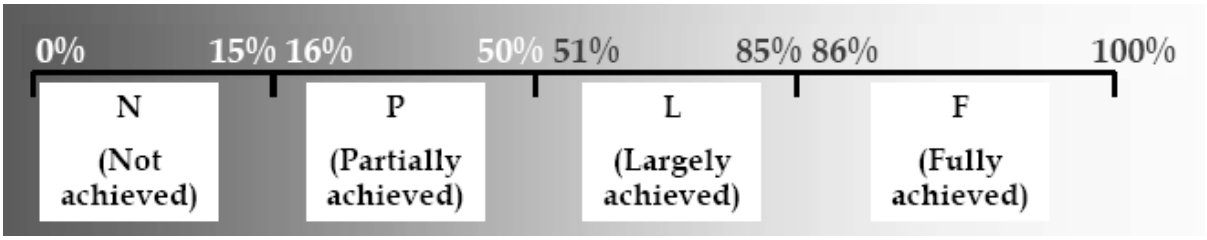


Figure 6: Four point ordinal scale for evaluating the achievement of process attribute

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 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.

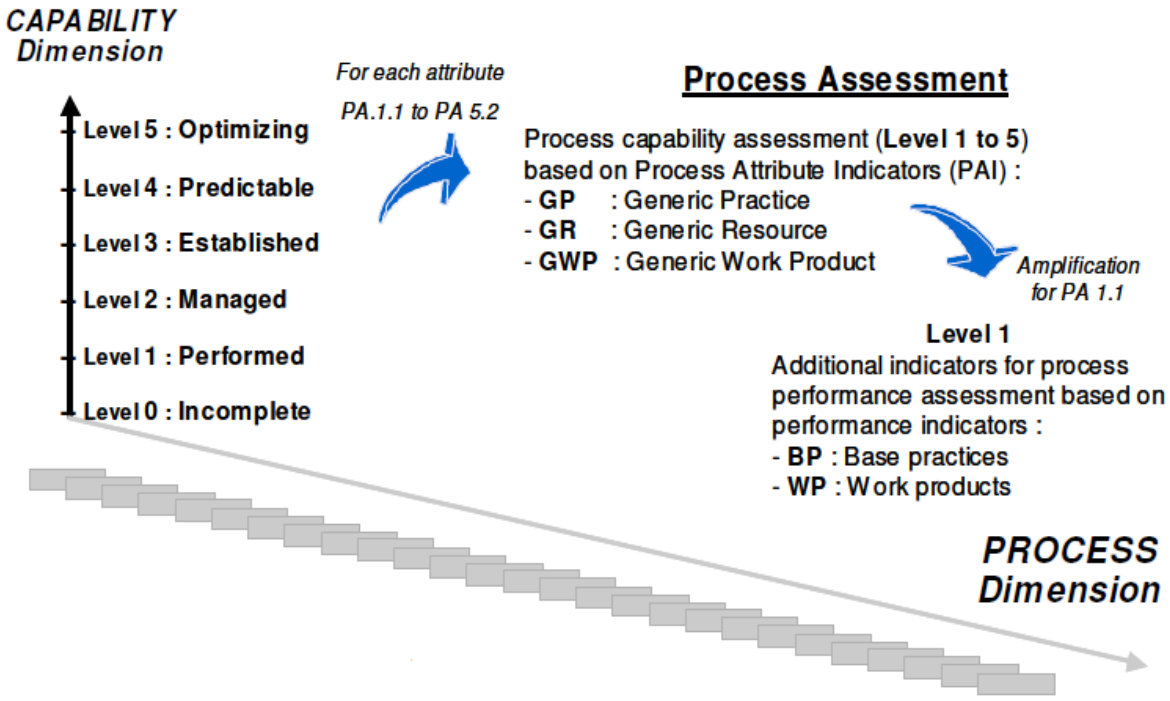


Figure 7: Assessment indicators of ISO/IEC 15504

3. Implementing Measurement Framework

3.1 COBIT Performance Measurement

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 8 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:

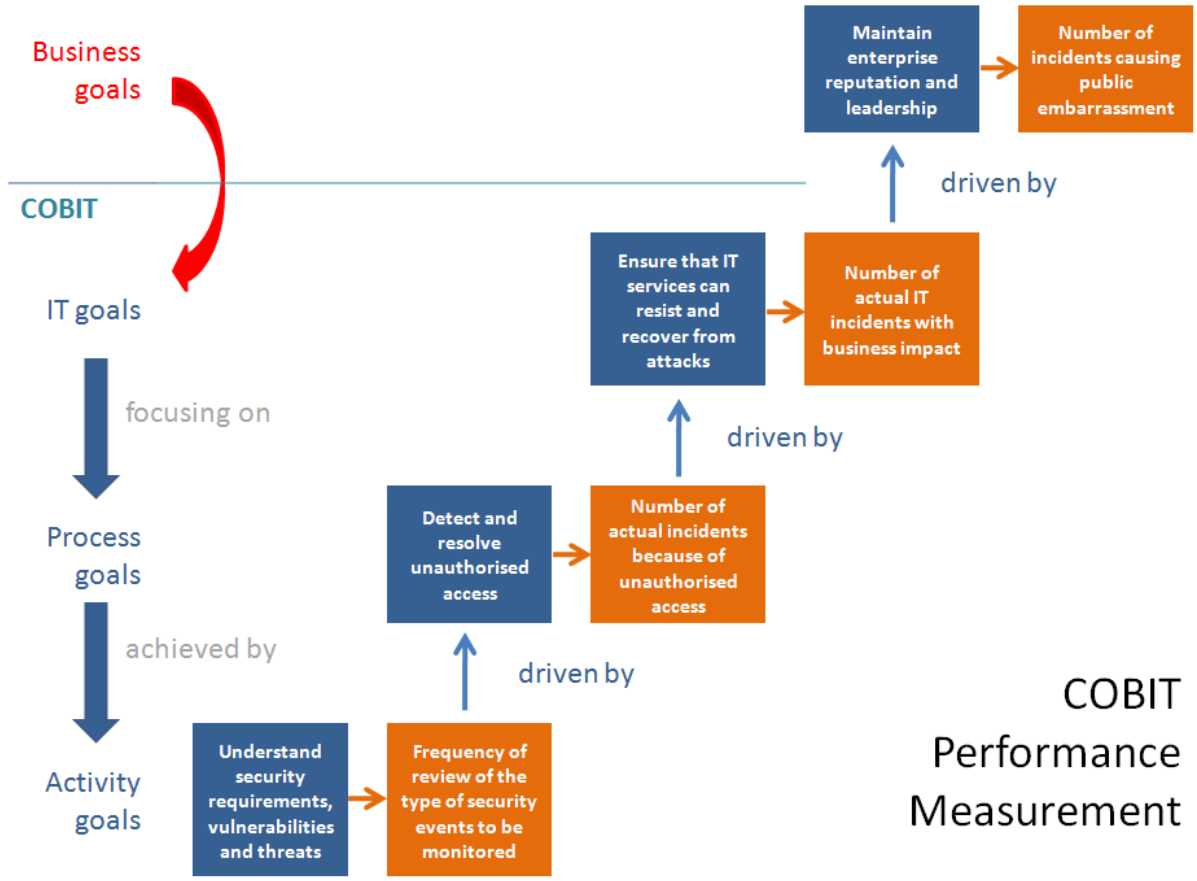


Figure 8: Example of linking different levels of goals and metrics in COBIT

3.2 Setting Objectives: Risk Appetite and Risk Tolerance

In 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.

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 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 evidential that these categories can exist only in interconnection. Next Figure presents how the interconnection of these objective categories can be underlined by ISO/IEC 15504 capability levels using the "outcome measures - performance drivers" relations from COBIT performance measurement concept.

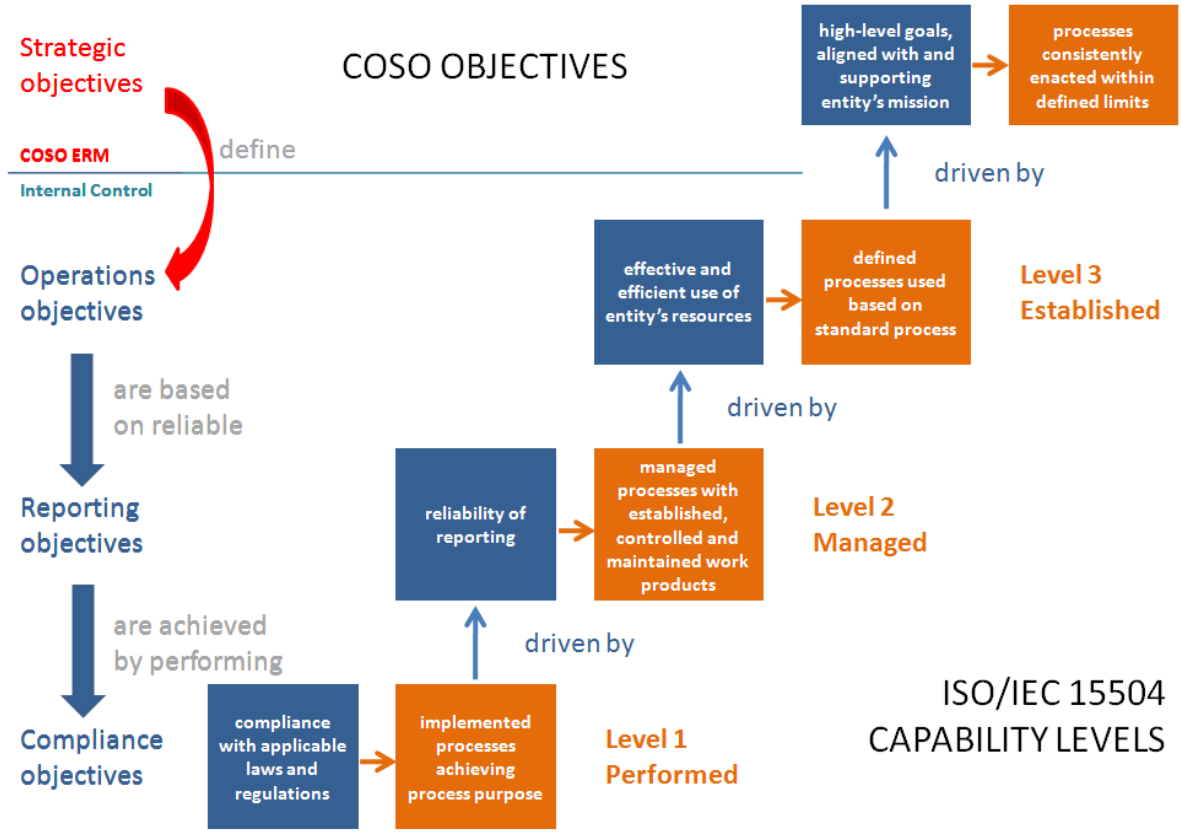


Figure 9: Measurement of COSO objectives by ISO/IEC 15504 capability levels

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 internal or IT controls. Objectives of reliable operation – like *achieving goals of reliable reporting or IT operation* - presume the fulfilment 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.

The objectives of the effective and efficient operations *related to operational units* (achieving *business goals*) presume the fulfilment of reliable reporting and compliance requirements. At this level, the entity's risk appetite can be prescribed by using the indicators of reliable reporting and compliance 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 requirements for operational units, processes and business activities.

Notice the consequence of *adapting risk management on internal or IT 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 internal or IT control system requirements.* So the consistent enterprise risk management presumes that the operation of internal or IT control system of the organization is measurable by adequate indicators. These indicators play roles in setting objectives regarding internal or IT 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 8.

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 internal or IT 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 10 identifies the applicability of the capability levels for the assessment of the COBIT-based IT control systems:

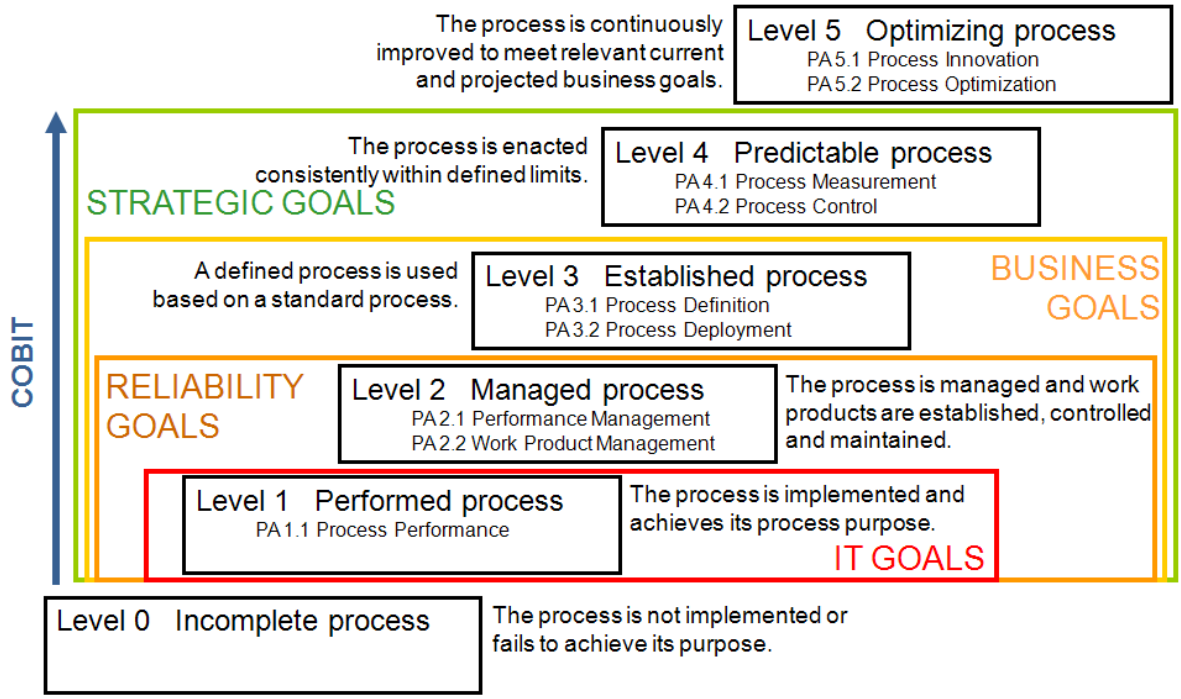


Figure 10: ISO/IEC 15504 capability levels for assessing COBIT-based IT control systems

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. 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.

3.3 Governance Context of Capability based on COSO Frameworks

The 0-2 capability level attributes are focusing on the instance or activity views 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 also helps to understand how the COSO Internal Control and Enterprise Risk Management (ERM) frameworks fit into the capability assessment model. As shown in Figure 11, the third dimension of the Internal Control framework is the Unit/Activity, while in ERM this is expanded into the corporate structure.

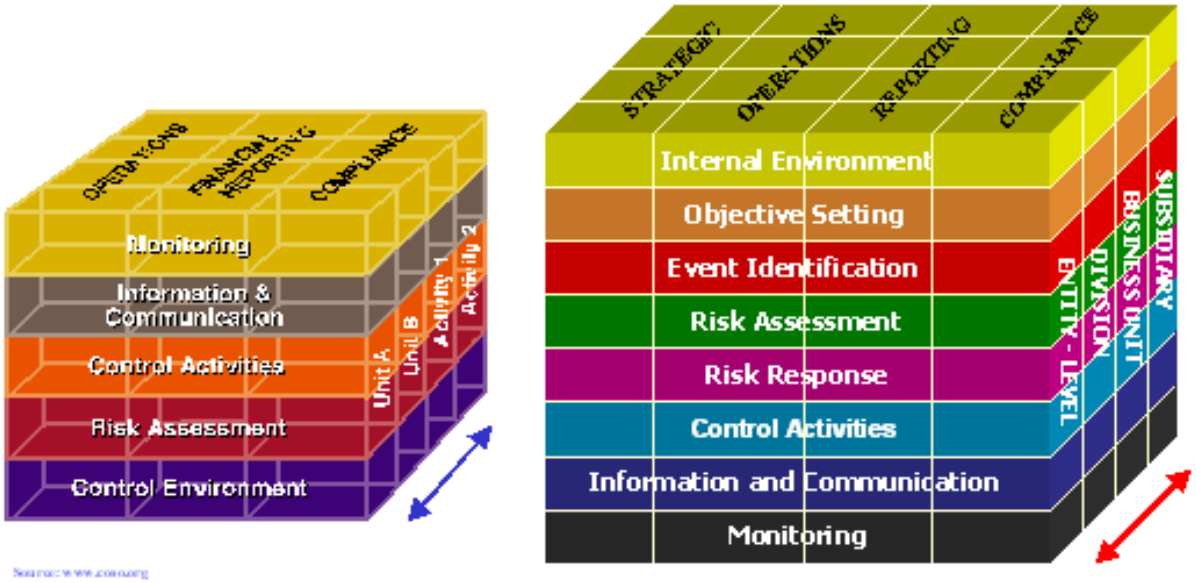


Figure 11: Activity (Instance) and Entity (Corporate) views within the dimensions of the COSO frameworks

Figure 12 shows that while the COSO Internal Control components are formulating 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.

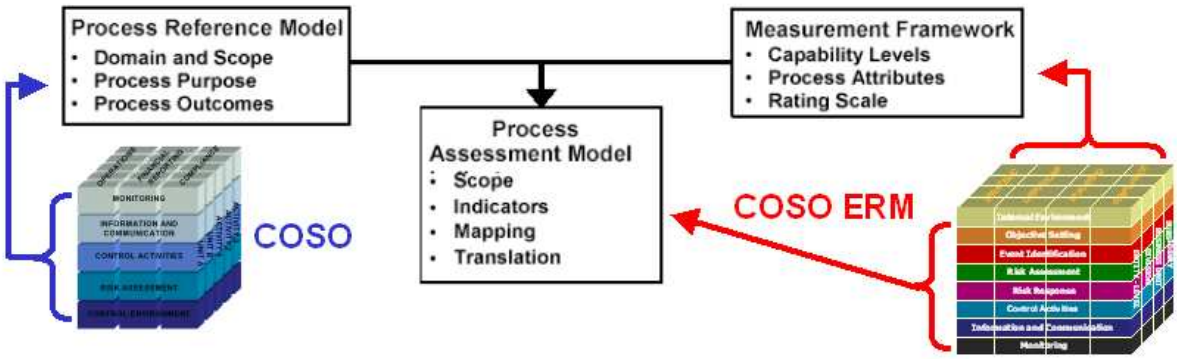


Figure 12: ISO/IEC 15504 process assessment and the COSO frameworks

Mapping and applying the main objective categories of the COSO Internal Control and ERM frameworks into the capability dimension of the ISO/IEC 15504 measurement model 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 13 identifies the applicability of the capability levels to the COSO main objective categories:

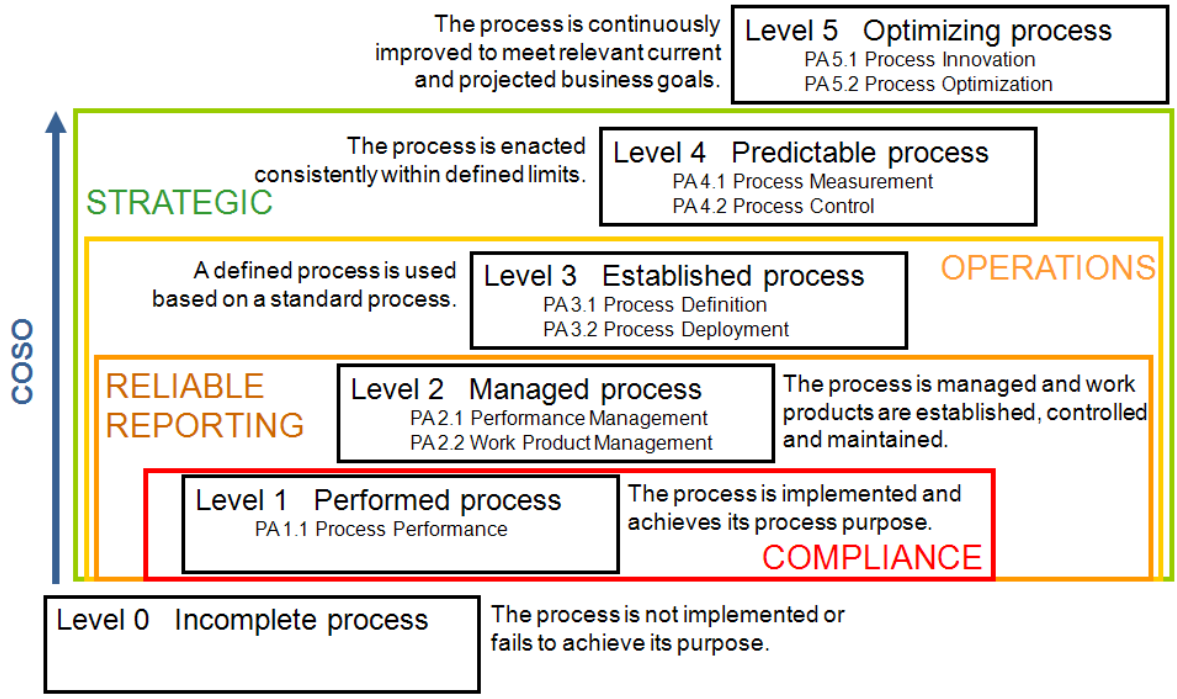


Figure 13: Mapping ISO/IEC 15504 capability levels to COSO objective categories

Figure 14 presents the general concept of how the ISO/IEC 15504 capability measurement is applicable for assessing governance systems implementing the most acknowledged control frameworks such as COSO and COBIT. 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

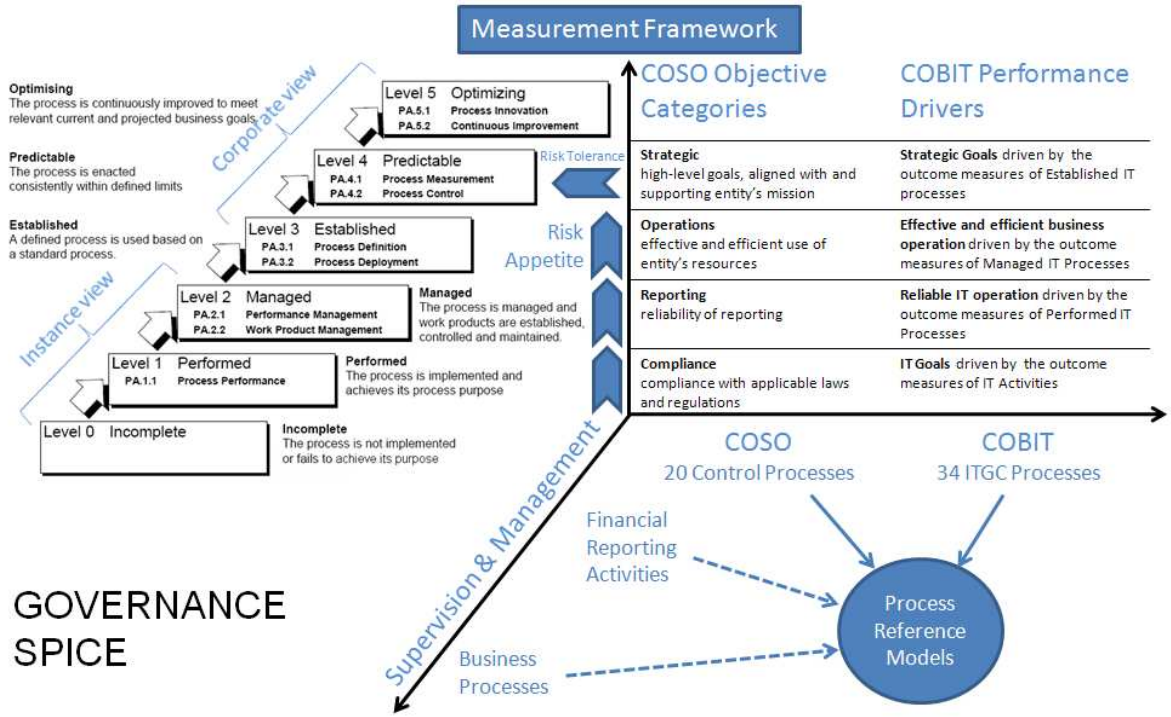


Figure 14: Assessing COSO and COBIT based governance systems

In the following parts we use the proposed Internal Financial Control Assessment Model for presenting business context of process capability. The process dimension of the proposed assessment model adopts the process definitions based on the twenty COSO 2006 Principles.

3.4 Achieving "Compliance" Objective at Performed Process (Level 1)

The achievement of the process performance attributes represents that the management has good understanding of the basics of the control requirements and the business activities are managed by keeping in mind the selected control framework(s) in an ad hoc base. There are evidences of achieving control process purpose, however not in a *managed* way.

At level 1 the internal control process exists and provides *reasonable assurance* to the achievement of all defined outcomes complying with the relevant external and internal regulations. At level 1 the (financial reporting) activities should be investigated, whether they proof the fulfilment of *purpose* and existence of the *outcomes* of the internal financial control process contributing to the *compliance objectives* of financial reporting (activities and controls).

Compliance objectives may refer to internal and external regulations or requirements. The description of internal financial control process - by the purpose statement and the outcomes - sets criteria for compliance with the relevant internal control framework (COSO) and contribute to the compliance with the regulatory requirements for internal controls over financial reporting (if applicable, like SOX or Basel II).

The level 1 assessment results are mainly usable in further process improvement context. Achieving Compliance objectives of all (relevant) 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 compliance of financial 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.

3.5 Achieving "Reliable Reporting" Objective at Managed Process (Level 2)

This level represents that the Performed control process (already achieving compliance to COSO process requirements 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 reporting* is evidenced in a traceable way (evidences are sufficient and suitable for external bodies).

Besides Level 1 achievements, the internal control process is managed and provides *reasonable assurance* to the achievement of the reliable reporting objectives. At level 2 the (financial reporting) activities should be investigated, whether the *performance management and work product management indicators* related to the internal financial control process are assessable as outcome measures of the *reliability objectives* of financial reporting (activities and controls).

Management of internal financial controls might be additionally evaluated by considering other relevant sources (like Corporate Governance Codes, Audit Standards, Recommendations and Guidelines).

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 COSO control processes). Moreover, the performance and work products of the financial 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 finance related business activities.

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

3.6 Achieving "Effective and Efficient Operation" Objective at Established Process (Level 3)

At this level the Managed process (already achieving compliance and reliable 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 internal control process is built into the operational processes and provides *reasonable assurance* to the achievement of the *objectives of "Effectiveness and efficiency of operations"*.

At level 3 the (financial reporting) activities should be investigated together with the organizational/entity level policies and procedures; whether the *process definition and process deployment indicators* are assessable as outcome measures of the *operational effectiveness and efficiency* objectives of financial reporting (at corporate levels).

Standardization is necessary for supporting measurement of operational effectiveness and efficiency, when evaluation is based on predefined comparable information.

The internal financial control process will better support the achievement of effectiveness and efficiency goals of operational units (effecting financial reporting objectives), if its design is based on Policies and Procedures consistent with the corporate structure and the entity's *risk appetite*.

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 context to the process dimension, level 3 type assessment of the full set of financial 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 COSO based Process Reference Model(s) 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 COSO process requirements) and reliable reporting objectives. For example level 3 monitoring processes enhancing internal audit functions have real additional value for any type of organizations targeting lower capability levels for other financial 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 financial control processes into operational processes. Too complex scope and excrescent 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 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.

3.7 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 internal control process is incorporated into the enterprise risk management system and provides *reasonable assurance* to the achievement of the *strategic objectives* relating to high-level goals, aligned with and supporting the entity's mission.

At level 4 the key controls should be investigated as an entity level key control (how applied in strategy setting and across the enterprise) within the entity level risk management, whether the *process measurement and process control indicators* are assessable as outcome measures of assurance regarding the entity's *strategic objectives* of financial reporting.

Setting of level 4 target capability presumes that the concerning financial 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 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 finance 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.

3.8 Evaluating Key Controls through the Supporting Internal Financial Control Processes

In case of extending the process dimension of the Process Assessment Model (based on the ISO/IEC 15504 requirements) by key controls as referred in context of the level 3 process capability, more practical advantages of applying ISO/IEC 15504 appear.

The key controls operating at *entity*, *intermediate* or *activity levels* having either *direct* or *indirect relationship* to the risk of material misstatement (as presented by the related IIA professional guidance */5/*) can be described by *purpose and outcome statements* of conformant process definitions. Outcomes should be identical and unique for all processes, which help avoiding unnecessary overlaps of key controls' objectives (in their documentation and test procedures). Outcomes (key control objectives) can be identified by the *relevant financial assertions* connected either to the significant accounts or to the material transactions flowing into the significant accounts.

Implementing a comprehensive set of internal financial control processes from the COSO based Process Reference Model contributes to the achievement of all process attributes up to level 4 at an entity level key control. The process performance (level 1) indicators, such as *base practices* and *work products* of the supporting internal financial control processes provide persuasive information for level 4 assessment of the key control processes.

4. Evaluating 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 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.

4.1 Setting Target Capability

The sponsor should determine which processes from the selected Process Reference Model(s) 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). Table 1 presents example target and assessed process profiles for 5 selected sample Internal Financial Control processes:

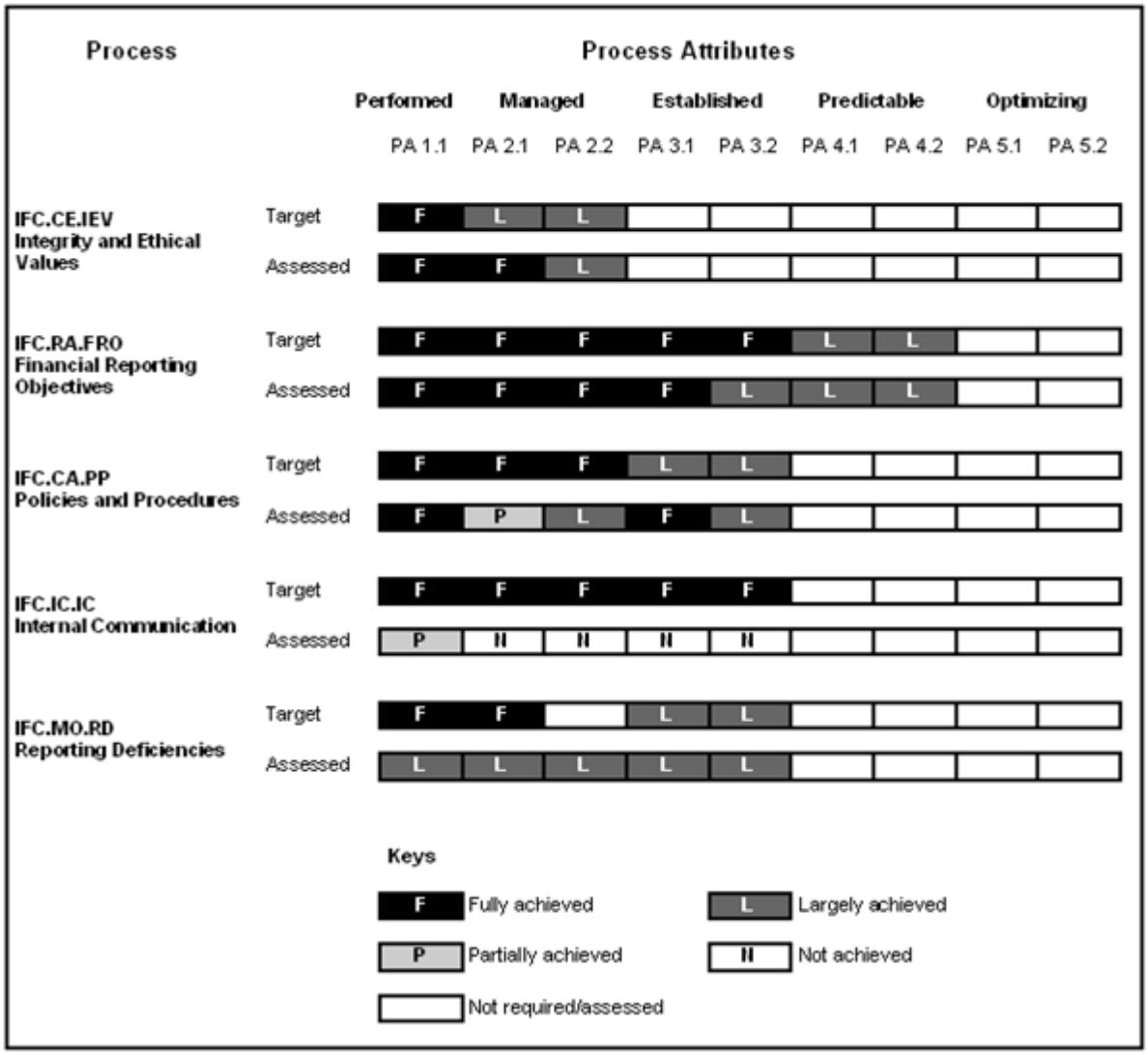


Table 1: Example target and assessed process profiles

4.2 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 achieved, 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 just 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.

4.3 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 *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 Table 2, the high risk arises from a major gap at lower capability levels.

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

Table 2: 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.

While the gaps between target and assessed profiles indicate the effectiveness of control design, the control process related risk measures the effectiveness of control operation, as shows the extent of risk that material loss or deviation from business objectives cannot be prevented or detected in time by the normal operation. Audit literature identifies ranking of control deficiencies concerning their business impact:

- *Control Deficiency*: Controls are not in place, or inadequate, or not being used
- *Significant Deficiency*: Deficiency in a significant control, or aggregation of deficiencies that could result consequential impact
- *Material Weakness*: Significant deficiency or an aggregation of significant deficiencies that preclude the entity's internal control from providing reasonable assurance that material misstatements or any major "loss" will be prevented or detected on a timely basis by employees in the normal course of performing their assigned functions

High risk measure of internal control process represents reportable Material Weakness of the control system.

Based on the presented approach risk analysis shall determine which process or processes represent the greatest degree of risk. Tables 3-5 present examples of Internal Financial Control related risk assessment using example process profiles from Table 1, 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						

Table 3: Internal Financial Control related risk assessment example - 1

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						

Table 4: Internal Financial Control related risk assessment example - 2

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						

Table 5: Internal Financial Control related risk assessment example - 3

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.

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 financial control processes is theoretically explainable if the inherent risk of the financial reporting

activities with their related business 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 requirement to assess control procedures against reliability objectives.

In more complex environment (featured by business type, size, sectoral regulations, etc.) the continual improvement of the governance and business administration processes is desirable. Assessing the integration of internal controls with business operations is necessary, when not only the reliability, accuracy and availability of the (e.g. financial) information are critical, but the effectiveness conclusion on the related operational processes or activities is also required. Assessing internal 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, and specific public service companies managing public funds.

5. Benefiting ISO/IEC 15504 Assessment Results

5.1 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 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.

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. *SAS 70 Audit:* A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of SOX make SAS 70 audit reports even more important to the process of reporting on effective internal controls at service organizations.

3. *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.

4. *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 is applicable for both.

5. “*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.

5.2 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 2110 of the International Standards for the Professional Practice of Internal Auditing [6]:

The common interpretation of ISO/IEC 15504 capability levels and COSO objectives showed in Figure 13 provides an innovative method for internal auditors to implement the 2110: 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.

Relevant guidance of internal audit engagements can be found in the The IIA's International Professional Practices Framework [7].

5.3 Monitoring Internal Controls

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 controls in the following aspects:

- Providing Assessment Model for internal control components and key controls 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 and risk management 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.

5.4 Systems based Audit Approach

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 [8]:

- *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 IC and 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 internal control processes and key controls, 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.

5.5 Applying Organizational Maturity Model for Internal Controls

Organizational maturity is the extent to which an organization consistently implements processes within a defined scope – derived from the specified Process Assessment Model(s) - that contributes to the achievement of its business goals. The new part of the ISO/IEC 15504 standard defines a measurement framework for the assessment of organizational maturity. Within this measurement framework, each level of organizational maturity is characterised by the demonstration of achievement of specified levels of process capability in process sets drawn from the specified Process Assessment Model.

In case of completing the basic process set of the Internal Financial Control Process Assessment Model (based on the ISO/IEC 15504 requirements) by key controls more practical advantages of applying ISO/IEC 15504 appear.

The key controls operating at *entity*, *intermediate* or *activity levels* having either *direct* or *indirect relationship* to the risk of material misstatement) can be described by *purpose and outcome statements* of conformant process definitions. Outcomes should be identical and unique for all processes, which help avoiding unnecessary overlaps of key controls' objectives (in their documentation and test procedures). Outcomes (key control objectives) can be identified for example by the *relevant financial assertions* connected either to the significant accounts or to the material transactions flowing into the significant accounts.

The key control processes - defined based on the ISO/IEC 15504-2 requirements - can be added to the *basic process set* for the organizational maturity model ensuring the achievement of level 1 (*basic*) maturity. The basic process set should include a minimum set of key control processes, together with additional and optional processes determined by the organizational context for the assessment.

The new organizational maturity concept can be used for further developing internal control evaluation tools, for example defining element(s) of the extended process set ensuring the achievement of the level 4 (*predictable*) organizational maturity in order to establish and maintain the quantitative understanding of the performance of the organization's key control processes through measurement and the use of appropriate quantitative techniques to ensure that performance of the organization's implemented key control processes support the achievement of the organization's relevant business goals.

The organizational maturity concept with its customization options such as definition of basic and extended process-sets including the minimum, *additional* and *optional* categories determined by the organizational context for the assessment, provides wider applicability of the ISO/IEC 15504 standard in new domains, such as IT management, internal controls and enterprise risk management, where relevant processes are assessed through different governance views or dimensions.

5.6 Evaluating Effectiveness of Internal Controls

Effectiveness conclusion is based on whether the implemented key controls (together) provide reasonable assurance that the organization achieves its business objectives within tolerable limits. The level of assurance depends on the risk-taking philosophy of the organization, however in case of internal controls over financial reporting, the regulatory and accounting requirements force executive and financial management minimizing those risks that *may* cause *material* misstatements in financial reports and other disclosures. The accounting and auditing literature provides detailed guidance on materiality issues, however materiality can be easily understood by simply applying the risk tolerance terminology of risk management: any deviation exceeding the pre-set tolerable limits regarding objectives should be considered as material.

Developing and assessing the necessary and sufficient set of key controls should follow risk-based and top-down approach. Effective design and operation of the internal control system presume that all risks, which can have material (more than significant) effect on business objectives, are responded in a cost effective way, so the applied set of key controls ensures that the probability of a material deviation from objectives (like misstatement in financial report) is remote or the consequence of a control deficiency (even considered its cumulative effect) remains within tolerable limits.

The key controls are operating at entity, intermediate or activity levels, and can have either direct or indirect relationship to the risk of material error. The outcomes of the 20 internal financial control processes of the COSO based Process Reference Model provide evidences that key controls are designed by applying risk management and internal control principles and also indicate that key controls are operating at predictable (level 4) capability. Furthermore, some of the 20 internal financial control processes can be also implemented as entity-level key controls based on circumstances.

ISO/IEC 15504 conformant process assessment includes not only traditional testing of key 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 proposed ISO/IEC 15504 based Control Risk Assessment provides practical tool for judgement about the *effectiveness of control operation*, whether the assessed process capability profiles of the key controls constitute reasonable assurance concerning achievement of related business objectives, such as the (low) control process related risk levels represent remote likelihood that material errors in financial statements and disclosures will not be prevented or detected on a timely basis.

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 the 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 understood 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 integrated "Governance SPICE Assessor" and "Internal Financial Control Assessor" Skill Cards 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.

See more details at http://www.training.ia-manager.org/ or contact to ivanyos@memolux.hu.

Key References

[1] 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 TR 15504-7:2008 Information technology -- Process assessment -- Part 7: Assessment of organizational maturity

[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] COBIT - Control Objectives for Information and related Technology,
COBIT 4.1 © 2007 IT Governance Institute. www.itgi.org

[4] Key Controls: The Solution for Sarbanes-Oxley Internal Control Compliance, Vorhies,J.B, The IIA Research Foundation, 2004

[5] SARBANES-OXLEY SECTION 404: A Guide for Management by Internal Controls Practitioners, The Institute of Internal Auditors, 2nd Edition, January 2008

[6] The Institute of Internal Auditors (The IIA): International Standards for the Professional Practice of Internal Auditing, 2009

[7] International Professional Practices Framework (IPPF), The IIA Research Foundation, 2009

[8] Risk based internal auditing - an introduction, David M. Griffiths, 30 January 2006

Additional Resources for Internal Financial Control Assessor Trainings

[A] COSO-based Process Reference Model and Process Performance Indicators (under COSO Copyright)

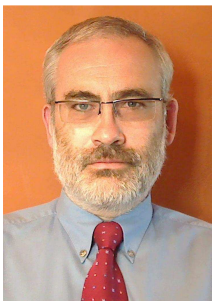
[B] Glossary of Internal Financial Control Assessment

[C] Skill Card – Governance SPICE Assessor

[D] Skill Card – Internal Financial Control Assessor

[E] Level 2-4 Indicators for Internal Financial Control Assessment

Author's short biography



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 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).

He was 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 the leader of the Governance Working Group and a founding member 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.

Contact info: János Ivanyos
Memolux Ltd.

Erzsébet királyné útja 125.
1142 Budapest
Hungary

Tel: +36 1 4607403
Fax:+36 1 4607493
e-mail: ivanyos@memolux.hu

www.training.ia-manager.org