János Ivanyos – József Roóz

A new approach in the assessment of the internal control systems applied in the public sector[1]

In our article, we will describe the new approach that supports the assessment of the operation of the internal control system. The significance and timeliness of the topic are justified not only by the recommendations of the audit profession such as the COSO frameworks, or INTOSAI GOV 9100: Guidelines for Internal Control Standards for the Public Sector, or the international regulations of financial reporting such as SOX, EU directives, etc. but also, the ever more pronounced appearance of the executive assessment and accounting obligations, which are already widely applied in the private sector, in the organizations of the public sector as well.

INTRODUCTION – APPLICATION OF INTERNAL CONTROL SYSTEMS

As is explained by the INTOSAI Guidance on Good Governance, i.e. by the introductory part of the GOV 9100 *Guidelines*, the assessment of internal control systems is a generally accepted standard for conducting the controls. The guidelines for the internal control standards built on the COSO model are on the one hand used by the managers of the organizations of public finances as an example for establishing a solid control framework for their entities, and on the other hand, these may be applied by the controllers of the public sector as a tool for assessing the internal control system.

Chart 1 helps overview the dimensions of the internal control system, as well as the related international (COSO, INTOSAI) recommendations and the guidelines published by the Ministry of Finance.

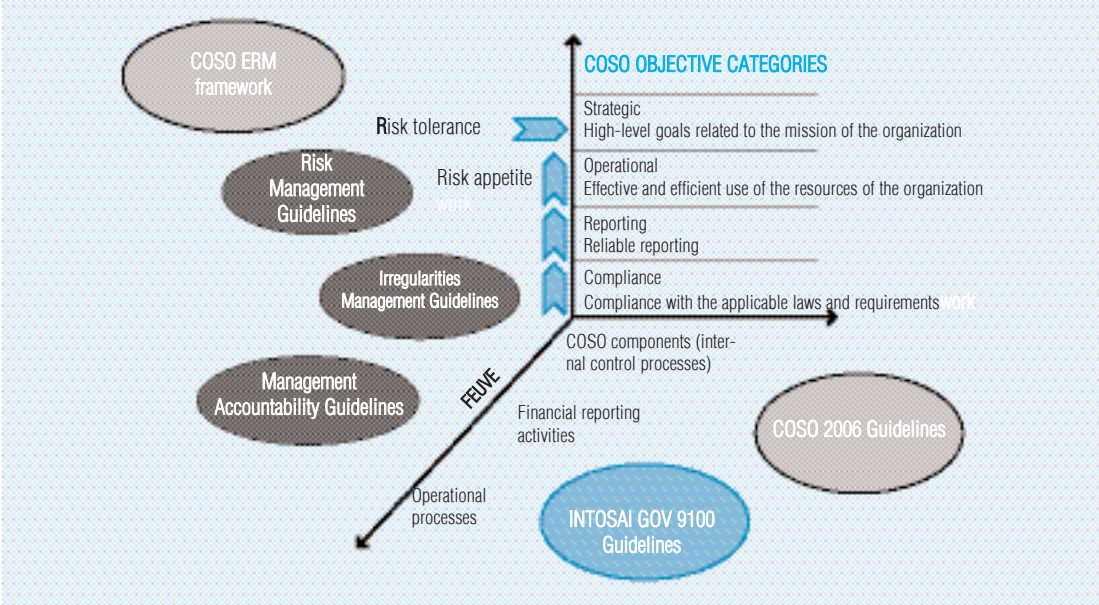
The "good governance" guidelines of the public sector can be traced back to the fundamental principles of responsible corporate governance in the private sector. In our article, we have only examined the roles of the internal control and risk management frameworks from among the wider correlations of good governance, as well as responsible corporate governance, in other words, we have analyzed to which extent the application of these contributes to obtaining an appropriate level of (reasonable) certainty as to how effectively and efficiently the given organization is able to realize its mission.

Internal control is a complex process both with regard to the public and private sectors, realized by the management and staff of an organization, and established for the definition of risks and for obtaining reasonable certainty. The purpose is that internal control supports the organization in

- complying with the relevant laws and regulations;

Chart 1

DIMENSIONS OF THE INTERNAL CONTROL SYSTEM AND THE RELATED INTERNATIONAL AND DOMESTIC GUIDELINES



- meeting its accounting/reporting obligations;
- the regular, ethical, economic, efficient and effective performance of the operational processes;
- the achievement of its strategic goals, including the protection of the resources of the entity from losses, improper use and damages.

In the following sections, we have described, as an example, those processes presented in the 2006 COSO Guidelines which are typical for the individual components with regard to the control system of financial reporting.

Control environment component

❶*Integrity and ethical values* – The values of integrity and ethical behavior are established, with special emphasis on the members of senior management, there is appropriate familiarity with the principles and in the course of the preparation of the financial reports, these are applied as fundamental norms of behavior.

❷*Supervisory body* – The supervisory body (Board of Directors, Board of Trustees or Supervisory Board) is aware of, and exercises the responsibilities related to financial reporting, as well as the relevant internal control system.

❸*Management philosophy and working style* – The philosophy and operational style of management contribute to the realization of an effective internal control system of financial reporting.

❹*Organizational setup* – The organizational setup of the entity supports the effective operation of the internal control system of financial reporting.

❺*Financial reporting competences* – The organization uses such persons who have the required expertise and experience in financial reporting and the related supervisory responsibilities.

❻*Authority and responsibility* – Both the managers and the staff have the appropriate authority and responsibilities for allowing the efficient operation of the internal control system of financial reporting.

❼*Human resources* – The human resource policies and practices are planned and introduced in such a

way that these allow the effective operation of the internal control system of financial reporting.

Risk assessment component

❶*The goals of financial reporting* – The managers define the goals of financial reporting with appropriate clarity and by applying sufficient criteria in order to allow the identification of the risks that may affect reliable financial reporting.
❷*Risks of financial reporting* – The organization identifies and analyzes the risks that may affect the achievement of the goals of financial reporting, and based on this, determines the method of risk management.
❸*The risk of fraud* – The possibility of fundamental misrepresentations arising from fraud should expressly be reckoned with in the assessment of risks affecting the achievement of the goals of financial reporting.

Control activities component

❶*Integration with risk assessment* – Measures are taken to handle the risks that jeopardize the achievement of the goals of financial reporting.
❷*Selection and development of control activities* – The control activities are selected and developed by taking into account the costs related to them, and their expected effectiveness with regard to the reduction of the risks that jeopardize the achievement of the goals of financial reporting.
❸*Policies and procedures* – The policies for reliable financial reporting are developed and communicated to the whole organization, the procedures stipulated in executive directives are executed.
❹*Information Technology* – IT controls are planned and introduced in order to support the achievement of the goals of financial reporting, where applicable.

Information and communication component

❶*Information in financial reporting* – Relevant information is determined, collected and applied, as well as distributed in such a way and by using such timing on each level of the organization that it could support the achievement of the goals of financial reporting.
❷*Information in internal control* – the information required for the operation of the other control components is defined, collected, applied and distributed in such a way and by using such timing that should allow the employees to perform their internal control tasks.
❸*Internal communication* – Communication allows and supports the understanding and implementation of the internal control goals and processes, as well as the personal tasks on each level of the organization.
❹*External communication* – The external partners are informed of the topics that affect the achievement of the goals of financial reporting.

Monitoring component

❶*Regular and individual assessments* – It is by relying on regular and/or individual assessment that management can conclude whether the internal control of financial reporting exists and works.
❷*Reporting of deficiencies* – The deficiencies of internal control are identified in due time and are communicated to the parties responsible for corrective measures, as well as to the management and the supervisory body, if necessary.

The sample processes that have been presented show that the components of the internal control system *(control environment, risk assessment, control activities, information and communication, monitoring)* appear as groups of processes that are parallel to each other and supplement each other, which ensure the efficient operation of the control system as a whole.

BACK TO THE BASES OF RISK MANAGEMENT!

Enterprise/Entity Risk Management, or ERM points beyond the risk assessment component of the internal control system. Focus is placed

on the risks that jeopardize the organizational level goals rather than on the risks inherent in the operational processes. In the following sections, we have highlighted those elements of risk management which primarily appear on the level of the organization (ERM) rather than on that of the operational processes (within the internal control system).

Setting of objectives

When the goals are defined, *the management* considers the strategy and the strategic goals of the organization. They determine the organization's *risk appetite*, i.e. what level of risks the management and the supervisory body (Board of Directors) regard as acceptable with regard to the strategy. Furthermore, *risk tolerance* is also defined, i.e. what level of deviance from the organizational goals is to be permitted on the given risk-bearing levels.

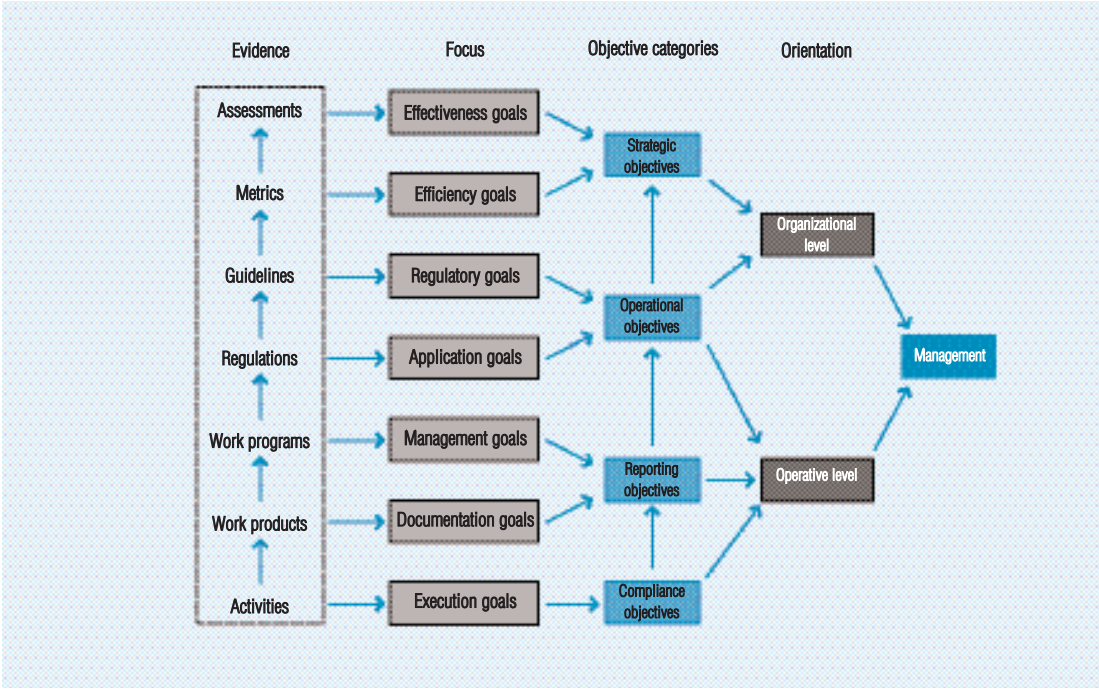
The goals defined for the organizational level or for the individual operational units and processes, as well as the allowed deviations from these should be supported by appropriate metrics (indicators).

The COSO ERM model, along with the incorporated control system, sets categories of objectives. In the case of the ERM, the *strategic, operational, reporting and regularity* objectives should be assessed through the realization of the goals of the operational units and processes, with regard to the organization, the integrated internal control system. Although different types of assessment (performance, financial or regularity) can be defined on the basis of the individual objective categories, it is easy to understand that the objective categories do not exist by themselves but are tied to each other *(see Chart 2)*.

According to the approach (also) represented by us, the objective categories are built on each other. *On the level of the operational processes*, the fulfillment of the compliance

Chart 2

INTERRELATED OBJECTIVE CATEGORIES



(regularity) goals ensures that the activities are performed according to the selected or prescribed requirements of risk management and the internal control system. The goals of reliable reporting (or accountability) assume the fulfillment of the compliance requirements, i. e. the risk-bearing level of the organization with regard to the operational processes can be determined by the indicators of the compliance (regularity) requirements.

As regards the operational units, the goals of efficient operation assume the fulfillment of the requirements of reliable reporting and regular execution. On this level, the risk appetite of the organization can be prescribed by the indicators of the requirements of reliable reporting and compliance (regularity).

With regard to the organization as a whole, the strategic goals broken down to the operational objectives defined for the level of the operational units assume the fulfillment of the requirements of efficient operation, reliable reporting and regular execution. As regards the organization as a whole, the level of risk-bearing can be characterized by the indicators of the operational, reporting and compliance requirements assumed in relation to the operational units, operational processes and activities.

As regards the risk management strategy of the organization, the level of risk-bearing can be described by the indicators of the requirements prescribed for the internal control system as a whole. Thus, a consistent organizational level risk management assumes that the operation of the internal control system of the organization can be described by the appropriate indicators. These indicators are also assigned a role in setting the objectives for the internal control system, since it is by using them that the risk tolerance for the level in question can be determined. It is the risk-bearing level of the next objective category that can be described by the control risk tolerance indicators of the lower-level objective category.

Identification of events

The identification of events contains those incidental external or internal events which may affect the strategy and the achievement of goals. It shows how the combination and interaction of the internal and external factors affect the *risk profile.*

From the aspect of organizational level risk management, it is not only the events (risks) of a negative impact that should be identified but also, the events of a favorable outcome, i.e. the opportunities. Although the COSO models do not describe the processes that support the utilization of the opportunities in detail, these represent the same level of importance for the operation of the organization as the traditional controls.

The general operational models, standards, frameworks, as well as the detailed operational (such as technological) requirements can also be used well for the identification of the potential events. It is by assessing the requirements prescribed by the control systems for the individual elements of the internal control system and the interrelatedness of the objective categories that we can obtain information on the events that were regarded as important by those who developed the control frameworks.

Integration of the internal control system into the risk management system

Neither the existence of risk management nor that of an internal control system in itself provides appropriate guarantee for the efficient operation of the organization. It is the risk responses given to keeping the impacts assessed on the basis of the identification of the external and internal risks or opportunities within the appropriate limit (risk tolerance), as well as the *results* of the control measures taken in order to implement these responses that we regard as the

guarantees for the efficient achievement of the goals of the organization in question.

In the assessment of the deviations and deficiencies, it is the consequences which go beyond the risk tolerance value and which potentially occur as a result of the deficiencies of the organizational level controls that support those operational processes which play a key role in the implementation of the organizational goals that should be taken into account. The assessment criteria can be illustrated by a traditional risk map as well *(see Chart 3)*.

Assessment, even if it is not subjective, is definitely individual. The significance of *individual assessment* is also supported by the fact that the consequences that go beyond the risk tolerance value may also arise from the inappropriate execution of the control measures taken to manage the inherent risk. However, it should also be taken into account that the key control process can only be developed appropriately, and its application can only be assessed properly if its relation to the implementation of the organizational level goals is measurable.

The integration of the internal control system into the risk management system means that the effectiveness of the operation of the internal control system should be measured by what extent the consequences of the affected operational process(es) remain within the prescribed risk tolerance limit.

A NEW APPROACH: THE APPLICATION OF THE ISO/IEC 15504 STANDARD IN THE ASSESSMENT OF THE PROCESSES OF THE INTERNAL CONTROL SYSTEM

COSO-based process assessment model

The ISO/IEC 15504 standard defines a two-dimensional process capability model for the assessment of processes. One of the dimensions, which is the process dimension, defines the processes and lists them in the different process categories. The other dimension is the *capability* dimension, which defines the set of

Chart 3

CONTROL DEFICIENCIES IN THE RISK MAP

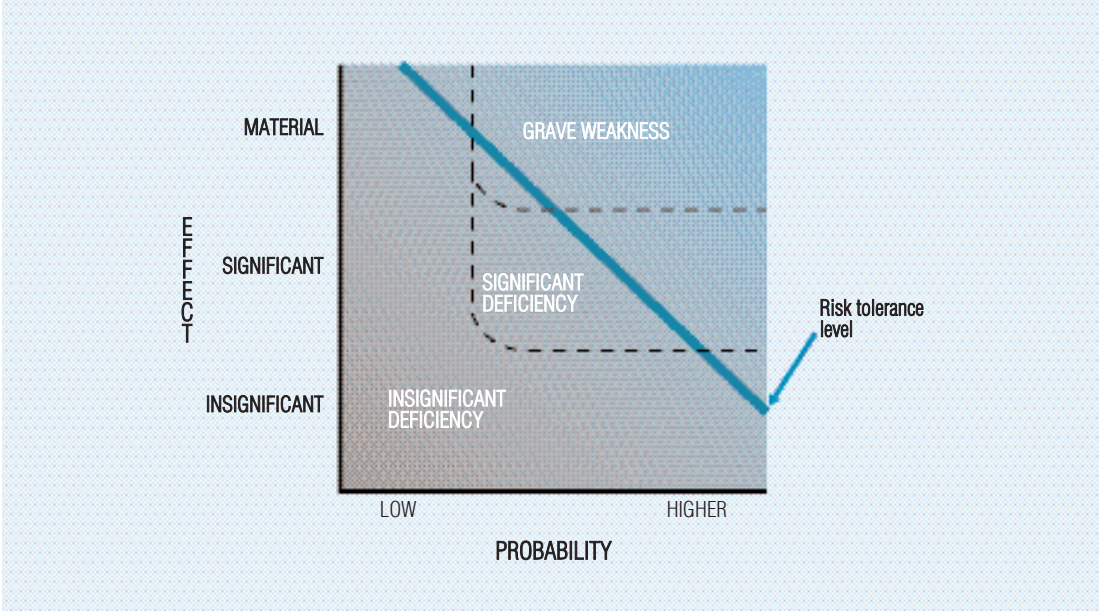
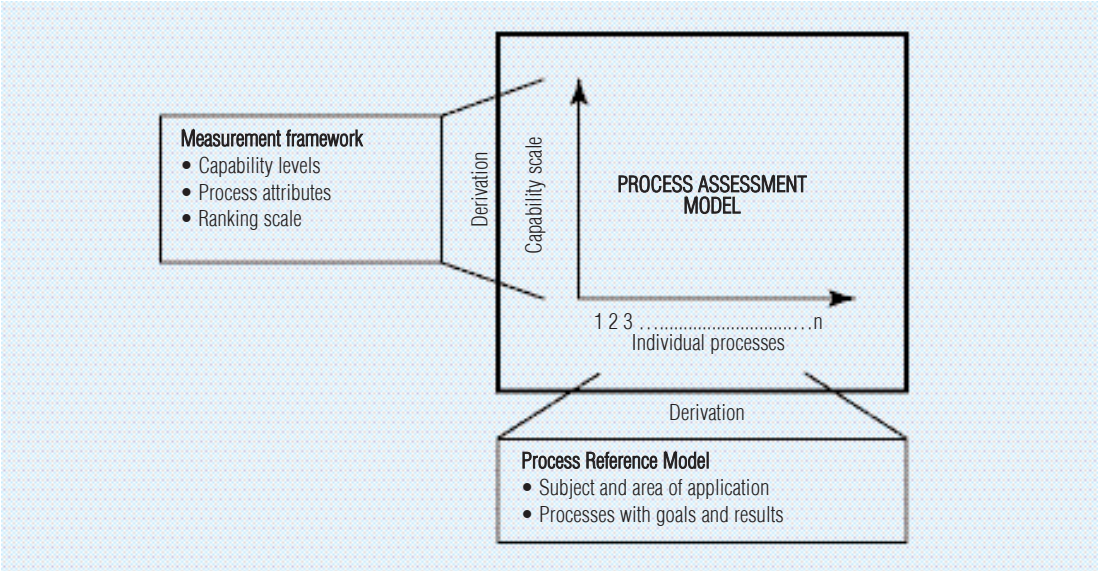


Chart 4

ELEMENTS OF THE PROCESS ASSESSMENT MODEL



process attributes grouped according to capability levels. It is the process attributes that provide the measurable characteristics of process capability *(see Chart 4)*.

It is required by the ISO/IEC 15504-2 standard that the process reference model (PRM) should contain the goals and results of the processes, as well as the definition of the conditions that are necessary and sufficient for the achievement of these.

The 2006 COSO guidelines define twenty fundamental principles that represent the basic conceptual processes that are related to, and are directly derived from the five components of the internal control *framework*. The individual principles are supported by the attributes that represent the characteristics related to the principles. It is stated in the guidelines that "although it is generally required that the individual attributes be present in the organization, it is possible to apply a principle in such a way that not all the listed attributes are present". According to the general criteria of assessing the internal control system, the attributes are treated as the "*process results creating the conditions necessary and sufficient for the achievement of the process goal*" described in the relevant principle.

Table 1 shows how the contents of the 2006 COSO guidelines can be used in PRM derivation.

The individual processes of the process assessment model are presented according to the *definition of the goal* (see the example in Table 1). These definitions of goals contain the individual functional goals related to the implementation of the process in a given environment. There is a list of specific final results linked to each definition of process goals, containing the positive results expected from the implementation of the process.

The fulfillment of a goal definition for a process means the first step in building up such a (level 1) process capability where the expected final results can already be observed.

The capability levels that make up the capability dimension of the process assessment model represent such a set of the process attributes as a compound result of which the capability of implementing the process in ques-

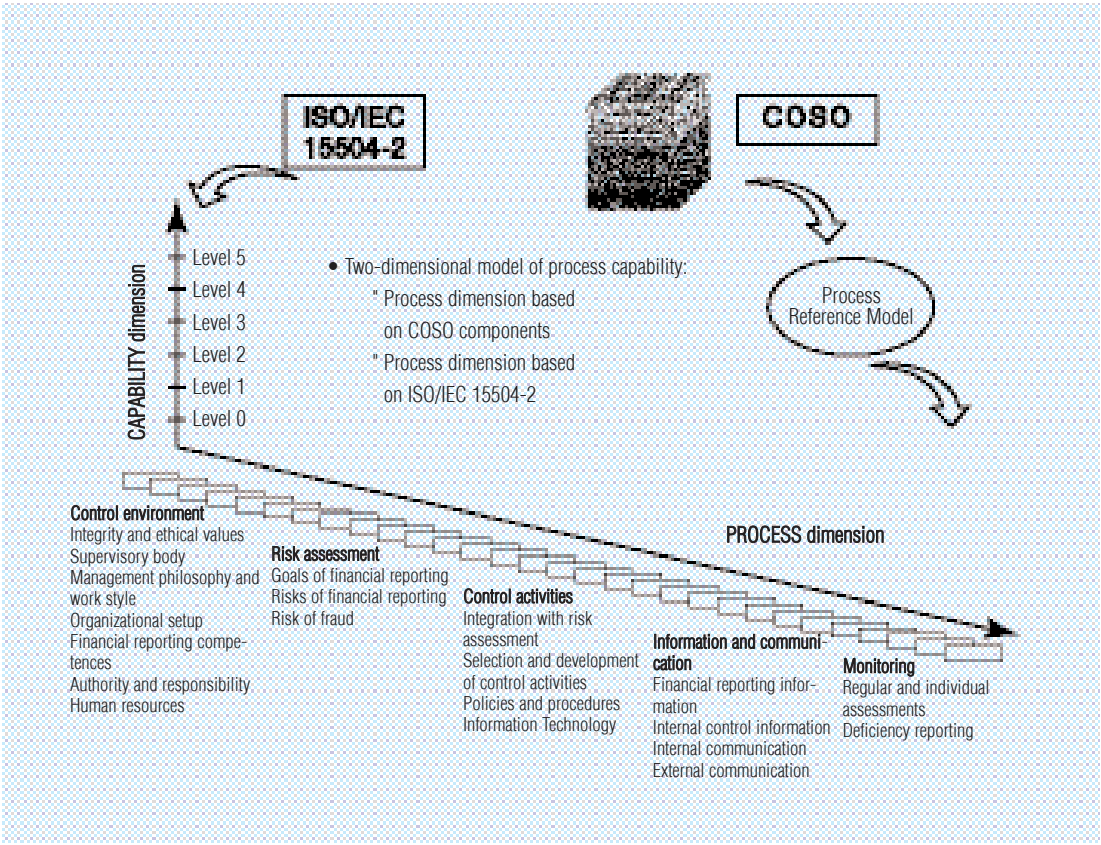
Table 1

EXAMPLE FOR A STANDARD PROCESS DESCRIPTION FROM THE 2006 COSO GUIDELINES

Process identifier	IFC.CE.IEV
Process name	Integrity and ethical values
Process goal	The values of integrity and ethical behavior are established, with special regard to the members of senior management; these principles are duly familiar, and are applied as fundamental norms of behavior in the preparation of the financial reports.
Process results	Results of the successful implementation of the IFC.CE.IEV process: ❶ clearly defined values – A clearly defined set of ethical values is developed by senior management, familiarity with which is ensured on each level of the organization; ❷ control of compliance – Processes are implemented for the control of compliance with the principles of integrity and ethical behavior; ❸ handling of deviations – Any deviations from the principles of integrity and ethical behavior are identified in due time, they are appropriately handled and corrected on the relevant levels of the organization.

Chart 5

PROCESS ASSESSMENT MODEL OF INTERNAL FINANCIAL CONTROLS



tion significantly improves. The capability to implement the process in question considerably improves from one level to another. The levels create a sensible route in the development process of either of the process capabilities and their definitions are contained by the ISO/IEC 15504-2 standard *(see Chart 5)*.

The process assessment model is based on the principle that the capability of a process can be assessed by presenting the achievement of the process attributes, on the basis of the evidence related to the assessment indicators.

There are two types of assessment indicators: the (general) process capability indicators, which relate to capability levels from 1 to 5, as well as the (specific) process implementation indicators, which exclusively refer to the 1. capability level.

There is such a set of process capability indicators belonging to the process attributes in the capability dimension which signals the extent of the fulfillment of the attribute in the process in question. These indicators refer to the significant activities, resources or results related to the fulfillment of the attribute goal in the process.

The levels of process capabilities and process attributes

In this measurement framework, the measuring of capabilities rests on nine process attributes (PA's) defined in the ISO/IEC 15504-2 standard. By using the process attributes, it can be defined whether the process in question has reached the required capability level. Each attribute refers to a predefined aspect of the process capability. The list of attributes within the capability levels does not suggest any sequence or ranking, it only serves their definitions.

ISO 15504 is built on a "continuous" model. This means that each process involved in the assessment can be independently assessed through the six-grade ranking scale of process capabilities *(see Chart 6)*.

LEVEL 0 – NON-EXISTENT PROCESS On this level, there is not any, or there is very little evidence as to whether the goal of the process is consistently fulfilled.

LEVEL 1 – PERFORMED PROCESS On this level, there is one attribute, that of *process implementation*, which shows the extent to which the process goal is fulfilled through the achievement of the predefined results of the process.

LEVEL 2 – MANAGED PROCESS On this level, there are two attributes, those of *managing implementation and handling the product of work*, which show to what extent the implementation of the process is governed, and how appropriately the work product resulting from the process is handled.

LEVEL 3 – DEFINED PROCESS On this level, there are two attributes, those of *defining the process* and applying the process, which show to what extent a standard process is maintained in order to support the application of a predefined process, and how successfully the standard process is applied in the achievement of the results of the process in question.

LEVEL 4 – PREDICTABLE PROCESS On this level, there are two attributes, those of *process measurement* and *process control*. These show the extent to which measurement results are used for the execution of the process to support the achievement of the appropriate process implementation goals for supporting the relevant organizational and operational goals, and the extent to which the process is managed by quantitative tools for achieving a stable process with appropriate capabilities and predictable within the predefined limits.

LEVEL 5 – OPTIMIZING PROCESS On this level, there are two attributes, those of *process innovation* and *process optimization*. These show the extent to which the changes in the process are determined by the analysis of the common

Chart 6

LEVELS OF PROCESS CAPABILITY

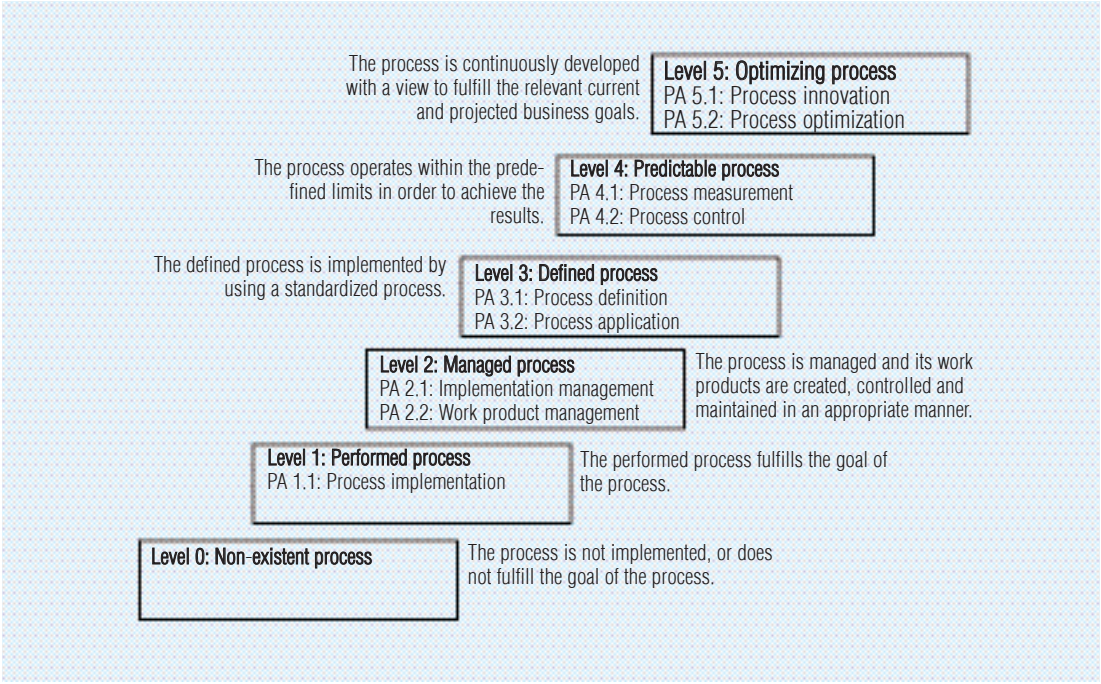
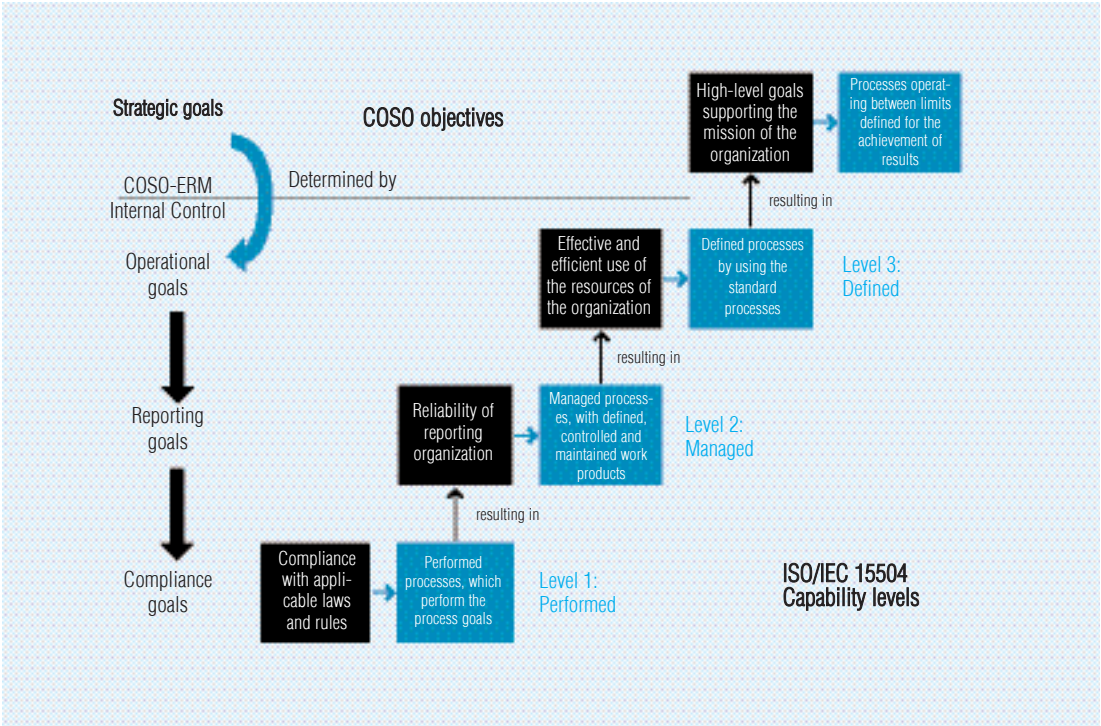


Chart 7

CAPABILITY LEVELS IN ISO/IEC 15504 AND THE COSO OBJECTIVE CATEGORIES



reasons for the fluctuations in implementation, as well as the examination of the innovative approaches used in process definition and application, and the extent to which the changes exert an actual effect in the definition, management and implementation of the process that will achieve the relevant process development goals.

The fulfillment of a capability level requires that all the attributes below it should be completely (minimum 85 percent) fulfilled and the attributes of the level in question should at least be *roughly* (minimum 50 percent) met.

The capability levels of the management and control processes

The 1. and 2. level process attributes of the measurement framework of the ISO/IEC 15504 standard described above focus on the case or activity aspects of the processes, while they concentrate on the aspects of the organizational unit from the 3. level onwards. By using this observation, it is easier to understand how COSO's internal control system and ERM's framework fit with the above-described assessment model. Besides the control and risk management components and objective categories, the third dimension of the control framework is represented by the operative processes that describe the operational units and activities, while in the ERM, the third dimension also including the level of operational units is the organizational setup.

In the ISO/IEC 15504 process assessment model, the target process profiles define that level of the selected process capability which is found suitable by management (or the party who ordered the assessment) for the risk appetite and risk tolerance of the organization.

Chart 7 shows the derivation applied between the capability levels and the objective categories of COSO, i. e. how the process capability levels can be applied as the scorecards for the objective categories of the COSO model.

LEVEL 1 – COMPLIANCE (PERFORMED PROCESS) There is an internal control process in place and all the predefined results are achieved in accordance with all the relevant external and internal regulations.

The relevant operational activities should be examined on the 1. level from the aspect of whether they prove the existence of the *results of the internal control processes.*

LEVEL 2 – RELIABLE REPORTING (MANAGED PROCESS) The above-described *performed process* has already been implemented on this level in a managed (planned, monitored and corrected) form, the work products are properly developed, controlled and maintained.

Besides the fulfillment of the requirements of the 1. level, the internal control process is managed and fulfills the goals of reliable reporting (management accountability).

On the 2. level, the relevant operational activities should be examined from the aspect of whether the implementation management and work product handling *indicators related to the internal control processes* can be assessed.

LEVEL 3 – EFFECTIVE OPERATION (DEFINED PROCESS) The above-described *managed process* has already been implemented on this level by applying the predefined process that is capable of achieving the process results.

Besides fulfilling the criteria of the 1. and 2. levels, the internal control process has been integrated into the operational processes on the level of the operational unit and fulfills the goal of "effective and efficient operation" (through the regular, ethical, economic, efficient and effective execution of the operational processes).

On the 3. level, the relevant operational activities should be examined along with the guidelines and procedures relevant for the given level

of the organization from such an aspect whether the process definition and process application *indicators* related to *the organizational level regulation of the affected operational processes* can be assessed.

LEVEL 4 – STRATEGIC GOALS (PREDICTABLE PROCESS) The above-described *defined process* works within the framework defined on this level with a view to achieving the process results. Besides the fulfillment of the criteria of the 1., 2. and 3. levels, the internal control process was incorporated into the system of organizational risk management and, in harmony with the mission of the organization and supporting the latter, it contributes to the fulfillment of the strategic objectives of the organization.

On the 4. level, the key controls must be examined from such an aspect of how they are applied for the strategy and the organization as a whole, and organizational level risk management should be looked at from the perspective of whether the process measurement and process control *indicators related to the realization of the goals of the organization* can be assessed.

POSSIBILITIES OF APPLYING THE NEW APPROACH

In the ISO/IEC 15504-4 standard, the processes and the methods of applying of Process Improvement, i.e. PI, and Process Capability Determination, i.e. PCD are described, and guidance is given for the following:

- use of process assessment,
- selection of process reference model(s),
- setting of target capability,
- definition of assessment input,
- definition of process-related risks from the assessment output,
- steps of process improvement,
- steps of determining process capabilities,
- comparability of the analysis of assessment outputs.

In the context of process improvement, process assessment provides a tool for the characterization of the organizational unit with regard to the capability of the selected processes. The analysis of the result of an appropriate process assessment in the light of the goals of the organizational unit determines the strengths, weaknesses and risks regarding the processes. This, in turn, helps define whether the processes contribute to the achievement of the organizational goals, and whether they facilitate improvement.

The targeted capability levels and attributes of the internal control system can be interpreted as the indicators of the operational goals related to the control system and the relevant risk tolerance, from the aspect of process improvement.

The determination of process capabilities deals with the analysis of the results of one or several relevant process assessments, in order to define the strengths, weaknesses and risks related to the operational activities by using the processes selected within a given organizational unit. A determination of process capabilities may provide fundamental input for the regularity control and the supervisory review. In the determination of process capabilities, however, the risks related to the process are also taken into account.

With regard to the internal control system, the capability levels examined (required) in relation to the determination of process capabilities, as well as the attributes thereof can be regarded as the indicators of the risk tolerance with regard to the requirements of achieving the higher objective category.

Analysis of the risks related to the control process

By *control risk,* we mean the risk of that the individual processes of the control system or the individual control activities do not achieve

the planned effect, i.e. the keeping of the residual risk within the desired range (risk tolerance level).

Comprehensive enterprise risk management (ERM) takes all the strategic, performance, reporting and regularity goals into account but, with regard to the application area of the risk assessment of internal control (regarding the processes), is limited to those material weaknesses which are not prevented or disclosed by internal controls in time. At the same time, however, the inherent operational and control risks are definitely not independent from each other, and the decisions on the risk appetite (the acceptance of the risk-bearing levels) and risk tolerance (the acceptance of the deviations from the organizational and operational goals) significantly affect the acceptance of the levels of control risks.

The risk assessment methodology to be presented can be generally applied for the use of all the assessment results of operational and control processes described in accordance with the requirements of the ISO/IEC 15504-2 standard. The capability determination applied for the operational processes may be suitable for defining the indicators of the risk tolerance level even without the framework of the internal control system.

The *probability* of the occurrence of the problem arises from the extent of the deviations of the process attribute and the capability level according to occurrence.

> *The deviations of the capability levels can be categorized as follows.*
> NONE – There are no major or minor deviations.
> LOW – There is no deviation on the 1. level, there are only minor deviations on the higher levels.
> SIGNIFICANT – There is a minor deviation on the 1. level, or a major deviation on a higher level.
> MATERIAL – There is a significant deviation on the 1. level, or more than one major deviation on a higher level.

The risk related to the process depends on both the *probability* of the occurrence of a problem arising from an identified deviation and the potential *consequence*. The consequences usually depend on the capability levels according to the place of the deviation.

A high risk arises from the material deviation of the lower capability level as described in *Table 2.*

If the risks are identified on several capability levels, the highest risk value should be regarded as the risk related to the process.

Table 2

RISKS ALLOCATED TO CAPABILITY LEVELS

CONSEQUENCE	PROBABILITY		
It is indicated by the capability level of the place of the deviation	It is indicated by the extent of the deviation of the capability levels		
	Low	Significant	Material
5 – Optimized	Low risk	Low risk	Low risk
4 – Predictable	Low risk	Low risk	Medium risk
3 – Defined	Low risk	Medium risk	Medium risk
2 – Managed	Medium risk	Medium risk	High risk
1 – Performed	Medium risk	High risk	High risk

Table 3

EXAMPLE FOR RISK ASSESSMENT RELATED TO INTERNAL CONTROL PROCESSES

IFC.RA.FRO - Goals of financial reporting

	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**	–	–
Deviation of the process attribute	–	**Major**	**Minor**	–	–	–	–
Deviation of the capability level	–	**Significant**		–		–	
Risk of the capability level	–	**Medium**		–		–	
Process risk	**Medium**						

Based on the above-described approach, the following must be defined by the risk analysis: the risks arising from which process or processes mean a material control deficiency, or a material (grave) weakness of the control system. In *Table 3*, we have described how the goal and the process profile that contains the assessed capability levels can be applied for determining the risks inherent in the control process.

In the control risk classification of the control processes assessed as described above, low risk means an immaterial *deficiency* within the risk tolerance level; while medium risk suggests a *material deficiency* that exceeds the risk tolerance level. High risk means a material (grave) weakness in the control system. This means that the risk assessment system presented above is suitable for providing objective support to the traditional control risk classifications (illustrated in Chart 3).

The control risk assessment based on ISO/IEC 15504-4 provides a practical tool for assessing *the effectiveness of the operation of controls* as well, i.e. for concluding whether the assessed capability profiles provide reasonable evidence for achieving the related organizational goals. For example, the low risk classifications established in relation to the control processes mean *an acceptably low level of probability* of that the material/financial types of mistakes or defaults, or any significant losses are not prevented or disclosed in time during business as usual.

In the example shown above, we applied the approach of comprehensive enterprise risk management (ERM) with regard to the internal control system:

- for the preliminary definition of the risk appetite (risk tolerance level) by applying the capability profile of the processes of the internal control system;
- for the definition of risk tolerance with regard to the key control processes;
- for linking the measurements of operational effectiveness (risk tolerance) to the process attributes;
- for risk assessment by comparing the targeted and measured process attribute values of the internal control system;
- for determining the effectiveness of establishing and operating the internal control system through defining the level of achieving the target capability profiles and the risks arising from the deviations.

Control of the EU Structural Funds

Although the Structural Funds are part of the Community budget, the method of spending them is based on the common responsibilities of the European Commission and the governments of the member states:

- it is the Commission that negotiates the development programs proposed by the member states, and approves these, as well as allocates resources;
- it is the members states and their regions that manage the programs, as well as execute, control and assess these by selecting the tenders;
- it is the Commission that takes part in the monitoring of the programs, makes available and pays the approved expenses and controls the established control systems.

The control of the (operational and financial) control systems can be performed by the European Commission and/or the relevant member state (in Hungary, the Government Control Office). The definition of the process capability of the controls is applicable to both cases.

In its opinion No. 2/2004 (Official Journal of the European Union No. C 107/2004), the European Court of Auditors developed a proposal for the Integrated Internal Control Framework, which contains what we call the "*single audit model*". The single audit concept has no generally accepted definition but it fundamentally determines that the internal control systems should be based on a chain of control procedures, in which the different levels of internal audit institutions cooperate.

The single audit approach rests on common achievements and the prioritization of their cost-efficient principles and aims to minimize overlaps in the control efforts and to maximize the effectiveness of controls with a predefined level of available resources. The sharing of well-defined and documented control data with others may enhance the reliability of controls on each level of the chain. The assessment of cost-efficiency formalized on the individual levels allows stating that the applied controls have optimized the error risks remaining in the basic transactions.

Further development of the systemic control method

According to the traditional interpretation, systemic control is defined by the already existing systems and the related controls. This approach assumes that the existing systems cover all the risks and the method often relies on "internal control questionnaires": these are such uniform documents which are applied in the execution of the individual controls.

The use of capability profiles lends an effective tool to management in the identification, understanding and management of control risks. If they reach the attributes of level 4 with regard to the selected control processes, management will be able to introduce and apply the principles of risk management in a cost-efficient manner.

The assessment model that contains both the process and the capability dimensions does not only focus on the use of the "internal control questionnaires" and the checklists but also takes the relevant assessment indicators into account. The observance of the standard requirements of the assessment process under the standard ISO/IEC 15504 helps implement this highly developed assessment method into the internal and external control procedures that apply varying standards in each sector.

* * *

The approach described in the article with the support of the readers of the journal Pénzügyi Szemle (Financial Review) can on the one hand be used by the managers of the public finance organizations in the establishment, improvement

of their internal control systems, as well as the presentation of effective operations, on the other hand, it can be used as a tool for the assessment of the internal control systems under review by the controllers of the public sector. A uniform application in the widest possible scope, i.e. one that is compliant with the international process assessment standard, may contribute to ensuring transferability between the various international and national management and control systems and the individual levels thereof, thus to the implementation of the "single audit approach" proposed by the European Court of Auditors, as well as to increasing cost efficiency, which has become ever more important in the public sector, as a result of the global crisis.

Notes

[1] The authors of this article have been involved in the development of the methodology related to the assessment of internal control systems, as well as the development of the related Hungarian and international training programs since 2005. In the period between 2005 and 2007, the international and Hungarian training and examination system based on the European Qualifications Framework ('skills card') entitled "Internal Financial Control Assessment" was established with the support of the European Union's Leonardo da Vinci Program and with the participation of the Hungarian, Spanish, Belgian, Irish and Romanian partners who took part in project number L-B-013/2005. From 2008 onwards, the common, i.e. English, Spanish, German, Romanian and Hungarian terminological and ontological model of the international training has been developed in the framework of a new support contract. This has been applied in training since late 2009. The findings of the international projects managed by the Budapest Business School and professionally coordinated by Memolux Kft have been disclosed on an ongoing basis and they have been discussed at reputed professional symposia and international conferences. Of these, we can highlight the presentations held by Gejza Halász, the Hungarian member of the European Court of Auditors and those given by the president of this organization Vitor Caldeira in Budapest in September 2007 at the international professional conference entitled "The Role of Internal Financial Controls in the Public Sector", which was supported by the State Audit Office (ÁSZ) of Hungary.

Literature

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)

INTOSAI GOV 9100 (2004): Guidelines for Internal Control Standards for the Public Sector

ISO/IEC 15504-1:2004 Information technology – Process assessment – Part 1: Concepts and vocabulary

- ISO/IEC 15504-2:2003 Information technology – Process assessment – Part 2: Performing an assessment
- ISO/IEC 15504-2:2003/Cor 1:2004
- ISO/IEC 15504-3:2004 Information technology – Process assessment – Part 3: Guidance on performing an assessment
- ISO/IEC 15504-4:2004 Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination
- ISO/IEC 15504-5:2006 Information technology – Process Assessment – Part 5: An exemplar Process Assessment Model

European Court of Auditors: Opinion No. 2/2004 of the Court of Auditors of the European Communities on the 'single audit' model (and a proposal for a Community internal control framework) (Official Journal of the European Union C 107/2004)