János Ivanyos – Éva Sándor-Kriszt

Risk Management Measurement and Evaluation Methods Based on Performance Indicators

Abstract: In recent years, audits of the State Audit Office of Hungary have detected numerous compliance and operational deficiencies in relation to the risk management practices of public sector institutions. This article presents a number of approaches and audit methods which, besides helping to meet compliance requirements, provide assistance in implementing and operating effective risk management. Under the international projects launched by the Budapest Business School with a view to facilitating the application of the ISO 31000 risk management standard, a number of methods have been developed to enhance the governance capability of organisations and ensure its objective assessment. They offer guidance for determining the risk criteria indispensable for the implementation of effective risk management, including adequate risk acceptance levels. The proposed performance indicators for the governance process of enterprise risk management are equally applicable to public and private sector organisations and enterprises. Receiving the title "Budapest University of Business Administration" on 1 January 2016, Budapest Business School provides an adequate training framework for acquiring risk management methods.

Keywords: risk management, governance capability, risk acceptance, effectiveness, performance indicators
JEL codes: G32, G34, D81, D61, D23

Heads of budgetary institutions subject to Act CXCV of 2011 on Public Finances (Áht.) – a regulation aimed at establishing the guarantees for maintaining the balance of public finances and for the transparent, efficient and controllable management of public funds –, of the asset management organisations established by budgetary institutions and, since 2014, heads of any other organisations of the government sector, including selected public companies, are required, pursuant to Government Decree No. 370/2011 (XII. 31.), to develop, operate and enforce at all levels of the organisation – in accordance with the methodological guidelines issued by the Minister in charge of public finances – an internal control system, and to submit a statement at least once a year evaluating the quality of the internal control system of the organisation.

Legal compliance requirements pertaining to Hungarian public finances and the guidelines recommended for application (*Ministry for National Economy,* 2012) essentially define risk management as a part of the internal control system[1]. In line with international trends, control-oriented risk assessment, as a key element in the planning of risk-based auditing, has become a cornerstone of public sector risk management regulation. Precisely with these compliance criteria in mind, institutions strive to enforce its principles even in their internal policies.

E-mail address: ivanyos.janos@uni-bge.hu

Recent periods have seen the publication of several articles and studies dedicated to the theoretical, regulatory and control issues of public sector risk management (Domokos et al., 2015), (Vasvári, 2015). These papers brought into focus an important problem: despite the remarkable accumulation of methodological knowledge and experience over the past 10 years, there are striking differences between the level of development – as per compliance criteria – of the organisational rules of risk management systems and the quality of the actual application of risk management at the vast majority of the entities audited by the State Audit Office of Hungary. Audit experiences gained with respect to the organisations of the central subsystem during the audit of the 2013 final accounts "found that in both the institutions and the organisations of institutional titles, risk management was the element of the internal control system where the greatest number of deficiencies was encountered". While risk management regulations were rated, based on the SAO's audit method, "compliant" at 87.4 per cent of the audited entities, only 29.1 per cent of the organisations received the same rating for risk management activity. The audit also found that, although correlation was observed between the size and rating of the audited organisations, it was medium-sized organisations that least complied with risk management requirements.

With respect to risk management systems implemented in the local government subsystem of public finances, the results were even more dismal both among the local governments completing the questionnaire of the integrity survey and among those selected for the audit on the basis of risk considerations. The audit findings regarding the financial management and operation of public higher education institutions were similarly unfavourable in the period of 2009–2013 (State Audit Office of Hungary, 2015). According to the audit results, barely more than one third of the audited public higher education institutions were found compliant with respect to the design and operation of the risk management system. Although the vast majority of institutions had an internal risk management policy, nearly one third of the institutions failed to update it. It is even more worrisome that less than one third of the institutions "took actions to eliminate the factors that jeopardise the achievement of the organisation's objectives and to minimise risks".

While lacking the necessary professional capacity may be a justification for municipalities of smaller settlements, obviously, this argument cannot be accepted in the case of public higher education institutions. The question rightfully arises: what is it that impairs legal compliance beyond the formulation of internal regulations? Is legal compliance sufficient in itself to implement successful risk management across the public sector?

Below we seek answers to the following questions: how can public sector institutions enhance their risk management systems besides satisfying compliance requirements? Which performance indicators can be used, besides compliance, to gauge effectiveness?

A NEED TO SUPPLEMENT COMPLIANCE CRITERIA

Control-based risk management expectations developed by professional audit organisations focus primarily on compliance criteria and are cited and prescribed by binding regulations and mandatory guidelines applicable both to the financial sector and the public sector as part of the "lines of defence". At the same time, originally developed for listed companies with a primary focus on supporting the reliability of financial statements, COSO models, as well as the internal control stand-

ards and guidelines that are based upon them, limit risk management to the context of developing and auditing the controls required for running the organisation. This is reflected in the widely applied interpretation of risk that describes risks as the negative effects of potentially arising events and, by assigning preference to risk mitigation, concentrates on reducing the probability (or frequency) of such events and/or alleviating the effects (consequences) thereof. This approach, however, fails to address risk management aimed at achieving positive outputs. According to a broadly accepted attitude in the public sector:

"Any possible positive yield of taking risks is – in contrast with the private enterprise domain – minimal in the public sector. Particularly when achieving goals that do not appear in the legal regulation has no "reward" (Domokos et. al, 2015).

At the same time, besides the criteria of compliance with legislative objectives, other angles should also be considered. Indeed, the public sector covers a fairly broad spectrum of organisations; institutions operating in the central and local subsystems of public finances are far from being homogenous in terms of institution type and size, supervisory and ownership structure, social/economic duties and regional dimensions with respect to the objectives specified in legislation applicable to the given professional field (such as the higher education act in the case of universities and colleges).

Not only certain policy areas (such as healthcare or education), but institutions operating within the framework set by the shared legislative objectives (e.g. in higher education) compete with each other in reality; at the very least, they compete for funding. If it was true that the achievement of a better ranking (position) has no "reward" – in the form of better financial conditions, professional recognition, "customer" satisfaction, rewarding of excellence, etc. –, this obvious, frequently seen competition – which is rather fierce among the top-ranking institutions – would not even exist. This, however, would not even be desirable as incentives for the best possible (or at least continuously improving) performance of the public sector serve broad social interests. Without the promise of a positive reward of risk-taking, public sector institutions could not be expected to have an intrinsic need for innovation and continuous development.

Accordingly, there is every reason to expect public sector institutions to put in place, besides the general statutory objectives, individually defined strategic and organisation-level operating objectives in the given time and space, in particular, with respect to effectiveness (utility) and efficiency (i.e. the optimal use of resources).

For instance, the objectives and tasks defined in the Organisational and Operational Regulations of the Budapest Business School (BGF, 2015) go beyond the objectives set forth in the statutory provisions applicable to higher education and adult training. Indeed, in addition to the main objective – i.e. maintaining the position achieved in tertiary-level specialist training ("to be an attractive business school in the field of economic and social sciences and the related disciplines both for the community and internationally") –, there is a need to enhance the quality of training continuously by ensuring the overarching autonomy of education, supporting the individual development of educators and students, providing continuously updated training materials and curricula that ensure an adequate balance between time-tested and up-to-date theoretical and practical knowledge, and by enhancing liaison with the domestic and international academic community. Accordingly, risks should be identified, assessed, accepted and addressed in accordance with the organisational and operational objectives that are intended to support the achievement

of these strategic goals, based on compliance with legislative requirements and high-level public administration expectations.

In our view, it is not the negligible positive reward of risk-taking that is reflected in the risk aversion so typical of public sector institutions, but the dissuasive force of the control system of public finance administration. At the same time, this does not necessarily imply a positive attitude if it also obstructs development, limits the likelihood of positive outcomes, unreasonably increases lead times or entails significant additional expenditures. The risk management literature has been long aware of and thoroughly analysed the contradiction between "business" oriented (safety-seeking) and "venture" oriented (risk-seeking) behaviours within corporate governance (Farkas and Szabó, 2005).

With the attributes of all other external factors unchanged over time and space, the optimal combination or proportion of "business" oriented and "venture" oriented attitudes is defined by governance objectives aligned with the specific organisation's goals in accordance with its desire to change or retain its position in the current competition. However, a protracted dominance of either attitude (which is described in the literature as the "apathetic" and "adventurous" states) jeopardises the achievement of both specific organisational objectives and reasonable business objectives, including the case of public sector institutions. It is also important to note that taking higher risks – for example, in the context of developments, innovation or the introduction of a new product or technology – is not the opposite of regular financial management, although on such occasions the altered effect of external and internal uncertainty factors calls for a higher professional quality of economic and legal administration. Naturally, this is also true to the lower and higher institutional levels of governance.

Keeping in mind the most comprehensive, efficient and reasonably expected achievement of specific organisational goals, managers view risk-taking as a natural concomitant (indeed, integral part) of day-to-day decision-making and governance activities, especially when they are forced to prioritise or choose from conflicting alternatives along the lines of the pre-defined objectives. Consequently, they perceive compliance with risk management policies developed or expected "irrespective" of specific organisational objectives and the functioning of the implemented governance system primarily as an extra administrative burden. As such, understandably – and especially in the absence of sanctions –, they either ignore risk management regulations or, as a best case scenario, they allocate compliance with the regulations to organisational frameworks less likely to "disturb" the daily work. As a result, "compliant" risk management may become an exercise in mostly ex post documentation completely separated from actual decision-making and governance functions that follows the audit cycles rather than the time horizon of organisational goals or any changes in circumstances. All this may lead to the devaluation of the role and function of mandatory risk management and the emergence of a negative general perception among staff members.

The "added value" of exclusively compliance-oriented risk management is also questionable from the perspective of external stakeholders. Recent decades have seen – nearly in all sectors and organisation types both on a global and local scale – a wide array of governance scandals and organised abuse, attempts at cooking the books or manipulating disclosures, various forms of corruption, the erosion of ethical standards, etc. This suggests that meeting legal compliance requirements does not guarantee the prevention of catastrophic (environmental, economic and social) failures

or even the achievement of organisation-specific goals in itself.

In numerous cases, we do not necessarily find a direct correlation between the quality of legal compliance and the state of individual success factors, as demonstrated by the compliance deficiencies identified at a number of leading Hungarian higher education institutions. Even the few Hungarian universities regularly selected to several international top lists (as different and dubiously compiled as they are) include institutions where the design and operation of the risk management system did not comply with legal provisions in the period of 2009–2013 audited by the SAO. It is an open question as to how to measure the extent to which a corrective or improving action (such as the addition of a risk management chapter to an internal control manual) or a lack thereof during the review period correlates with the previous or current prestigious ranking of the specific higher education institution in Hungarian or international top lists or with the existence and elimination of financial management irregularities.

ADDITIONAL CRITERIA OF RISK MANAGEMENT QUALIFICATION

Traditional compliance audits judge the effectiveness of risk management on the basis of whether all components of a model (such as COSO ERM) are "present" in the organisation's operations and whether their functioning provides "reasonable assurance" regarding the achievement of specific objectives. In our opinion, based on the application of the effectiveness criteria of the ISO 31000 risk management standard (ISO, 2009)[2], effectiveness can be best determined by answering the following three questions (Ivanyos and Sándor-Kriszt, 2015).

- Does the organisation have an up-to-date, accurate and comprehensive (i.e. covering all operational and organisational levels) interpretation of risks?
- Do all external and internal stakeholders understand and accept the levels and limits of risk appetite applied by the organisation (risk criteria)?
- Are the risks of the organisation within the limits of the prescribed criteria?

Answering these questions goes beyond the scope of statements pertaining to the regularity of the design and operation of the internal control system. Indeed, the answers provided cannot even be verified based on pre-defined audit questionnaires due to the differences between organisation-specific objectives and their time horizons, the established organisational frameworks, the position of individual organisations in space and their linkages, and the organisations' roles in administrative, production, service provision, sale and utilisation chains. At the same time, by asking these questions managers may better grasp the tasks related to risk management, while keeping in mind the time and space considerations and changes of the organisation's external and internal linkages.[3]

Governance activities and capabilities implemented at the organisational and operational levels support the effectiveness of risk management. Implementation of the recommendations of the applied risk management models or approaches cannot be evaluated and verified directly but only by examining the extent to which they are embedded in the governance and control of operational processes, the planning, decision-making and review procedures of the organisation, the comprehensive governance policies and the record-keeping systems of the organisation. Based on this, the quality of risk management can be better captured by assessing the governance capability of an organisation[4] (Ivanyos and

Roóz, 2010) rather than by strictly examining "compliance" with the components of a general risk management or control model.

Governance capability is an attribute of the operation of an organisation, which indicates the extent to which the governance system supports the execution of key processes aligned with organisational goals. The definition and improvement of governance capability are important tools that facilitate the enhancement of the frameworks of the governance system, the fullest possible integration of risk management into the decision-making and execution processes of the organisation, and the increased efficiency of supervisory and audit activities.

The quality of individually developed (customised) risk management can also be measured against a number of model-independent attributes, the deficiencies of which jeopardise the adequate enforcement of effectiveness criteria. Based on the recommendations of the ISO 31000 risk management standard, the attributes supporting the effectiveness of risk management and improving performance can be summarised as follows (Ivanyos, 2015):

- continuous improvement of risk management;
- comprehensive regulation of personal accountability for risks;
- application of risk management during the implementation of all decision-making procedures;
- continuous communication with stakeholders;
- full integration into the governance system of the organisation.

Deficiencies in the continuous improvement of risk management typically arise from delays in – or the absence of – senior officers' responses to changes and problems affecting the governance framework encompassing the organisational and operational levels, in particular, the monitoring and review activities assigned to governance roles, or from the inadequate or untimely provision of the required resources, which often convey messages in conflict with the announced risk management policy.

Risk management activities should not be ad hoc; they should be performed consistently, in accordance with the job description rules governing all other duties. In addition to the clear and straightforward definition of the rules of mandate and responsibility, wherever possible, performance criteria should be also prescribed and used directly as a measure for evaluating the performance of risk management. Besides having the rules of responsibility formally accepted, it is important to ensure that the rules are clearly understood, to provide the required training opportunities, and to share good examples and best practices with the stakeholders.

Upon making decisions, risks are obviously considered at each organisational and operational level, and accordingly, a more or less formalised risk management process (or risk acceptance) will take place. The fact and extent of the implementation of risk management can be monitored by way of the documentation of the decision-making procedure. The preparation and decision-making steps of important decisions may involve all elements of risk management (e.g. those prescribed by the regulation), and decision-makers may evaluate the adequacy of the implementation of risk management which could influence the decisions made.

The method and level of risk management applicable during specific decision-making procedures should be planned and, as appropriate, specified in a separate policy, aligned with a governance framework that is developed – individually – and reviewed on a regular basis for the organisation as a whole. At the same time, it should be remembered that the mere fact of regulation or documentation

will not suffice in itself; adequacy can only be considered in the case of implementation in all decision-making procedures at all organisational and operational levels, including at custom-tailored capability levels. Another important aspect to consider is to ensure that the application of risk management procedures is not prescribed with a view to restricting the decision-making powers of the given organisational or operational level, but in order to facilitate sound and good decisions with the assistance of the risk management toolkit.

Risk management is built on continuous communication, dialogue and consultation with external and internal stakeholders. From the perspective of the operation of the organisation, multidirectional communication ensuring that even the potentially conflicting objectives and angles of stakeholders are considered is an important element and organic part of risk management, which is indispensable not only in identifying and evaluating risks but also in planning risk management measures, monitoring execution and reviewing the results. If the stakeholders do not recognise or accept each other's risk levels, measures taken on the basis of criteria pertaining to the same risk without coordination with the various stakeholders may mutually neutralise one another or at the very least, may jeopardise the achievement of the effect desired by either party.

As the prescribed and the implemented risk management procedures may differ from one another, in relation to the governance of individual organisational and operational levels, the stakeholders, as well as the method and frequency of liaison may also be different. For example, the contractual delivery of a specific order, the provision of a public service or the implementation of a major investment project necessitates different risk definitions and presentations and different types of dialogues with the required partners, staff members, senior officers, authorities, creditors and households, in function of the specific circumstances regarding work conditions, financing, profitability and household demand.

Developing the governance system and its processes should provide an optimal framework for the achievement of organisational objectives. Even with respect to the effect of uncertainty on organisational objectives, i.e. risks, the task is to create optimal organisational frameworks and to integrate risk management into organisational and operational processes. In this regard, it is the actions and the statements of managers playing a role in risk management that reflect the weight and role they assign to risk management in the control system, based on what they consider necessary and sufficient to achieve organisational objectives.

DEFINITION OF RISK LEVELS

In accordance with the ISO 31000 standard, risk is interpreted as the effect of uncertainty on our objectives, which can be a positive and/or negative deviation from what is expected. This definition is far broader than the traditional (control-based) approach that applies the product of the probability and effect of negative events. Consequently, risk management should not concentrate on reducing the probability and/or more or less predictable effect of "inherent" (or seemingly inherent) risk factors; instead, it should consider the significance of the effect of the "persisting" (factual but hard-to-measure) uncertainty on the objectives, based on the best information available. This approach is also supported by the fact that it is precisely not the high probability events that cause the most severe damages, but inadequately considered changes of circumstances, as well as rare or unpredictable (chain of) events that trigger/intensify each other.

These events would not even be considered a significant risk if examined as the product of probability and effect.

According to the ISO 31000 standard, in order to assess the significance of risks the organisation needs to define risk criteria aligned with the values, objectives and resources of the organisation. These criteria may derive from legal or other requirements undertaken by the organisation, and the factors to be considered in defining them are the following:

- nature and type of possible causes and effects;
- the manner in which the probability of the event is defined;
- space and time horizon of the frequency and consequence of the event;
- definition of risk levels;
- possible risk limits;
- definition of the combined effect of recurring or parallel risks;
- opinion of stakeholders.

It is the task of the senior management responsible for the strategic governance of the organisation to define the governance objectives that provide a framework for the internal correlations of risk management processes at the operational and organisational levels of the organisation. This is the basis on which the risk criteria to be applied by risk management can be developed as part of the tasks and within the competence of the senior officer responsible for the implementation of risk management.

Governance objectives link organisational objectives to operational and organisational level capabilities as shown in *Figure 1* in such a way that they ensure that the stance and instructions of management remain within the governance frameworks that define the needs of the stakeholders and the expectations of the environment. As such, governance and supervisory bodies should be aware of and competent to decide the extent to which the comprehensive corporate governance system meets the expectations of stakeholders.

According to the COSO ERM framework that applies the traditional definitions of risk levels, risk appetite (or willingness to take risks) shows the risk still acceptable for management and the supervisory body with respect to strategy, while risk tolerance indicates the acceptable deviation from organisational objectives at the specific risk appetite level.

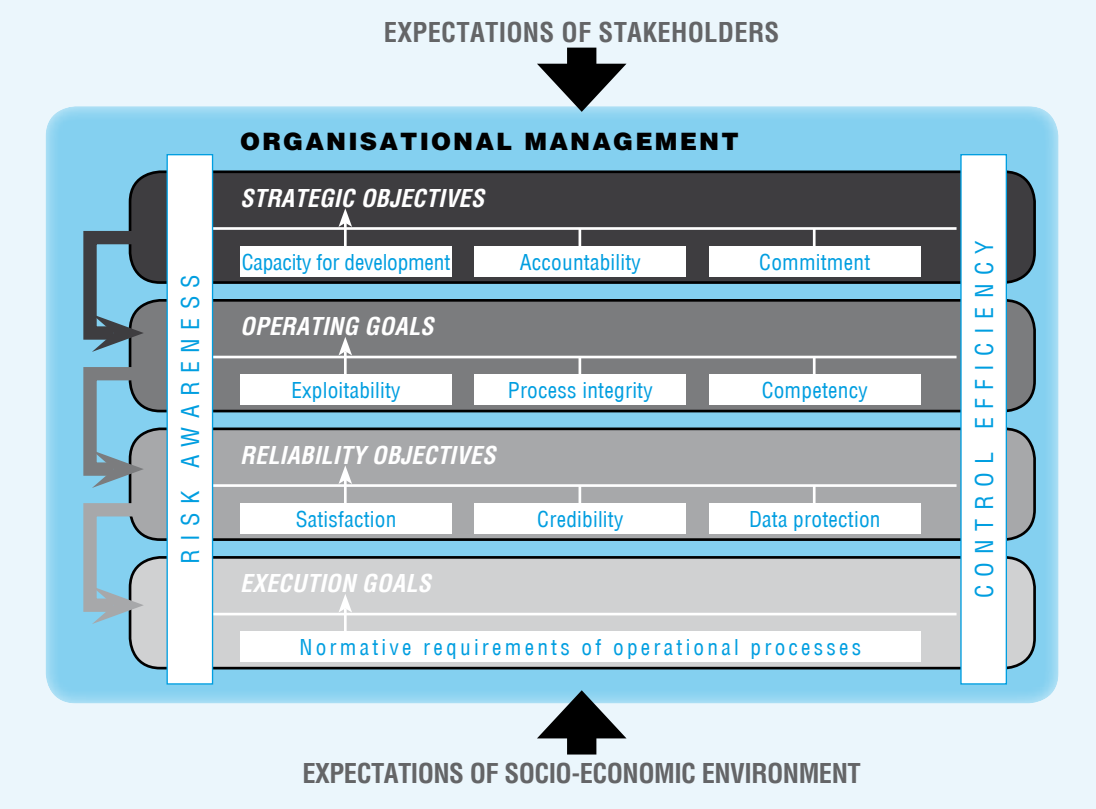
Risk appetite and risk tolerance levels need to be aligned with operational and organisational objectives and the relevant management responsibilities (it should be noted that the ISO 31000 standard does not use the terms risk appetite and risk tolerance and even the traditional risk management literature fails to provide a consistent interpretation of "tolerance"). This can be implemented effectively by applying risk criteria designed in view of the approved risk management policy and the external and internal correlations considered in establishing the risk management frameworks integrated into the control system on the one hand, and of the external and internal and time and space considerations defined by the risk management process organically integrated into the governance of individual operational and organisational levels on the other hand.

The ISO 31000 standard emphasises the responsibility of the CEO/Board in the design and effective operation of the risk management system. This includes the continuous maintenance of a strong commitment on the part of the organisation's management, and the strategic planning and enforcement of commitment at all levels of the organisation. In this context, the CEO/Board

- defines and approves the risk management policy;
- ensures the harmony between organisational culture and the risk management policy;

Figure 1

CONNECTION OF GOVERNANCE OBJECTIVES TO THE OBJECTIVES OF ORGANISATIONAL AND OPERATIONAL LEVELS



Source: own editing

- defines the performance indicators of risk management in line with the organisation's performance indicators;
- aligns risk management objectives with the strategy and objectives of the organisation;
- ensures legal and regulatory compliance;
- allocates accountable responsibilities to the relevant levels of the organisation;
- ensures the availability of the resources required for risk management;
- communicates the importance and benefits of risk management to all stakeholders;
- ensures the continuous applicability of the risk management framework.

Although the definitions and the terminology of COSO are different from those applied by the ISO 31000 standard, the document issued by the Commission in 2012 (*COSO,* 2012) also provides guidelines regarding the definition, application and presentation of risk appetite and willingness to take risk.

"Risk appetite:

- *strategic and is related to the pursuit of organizational objectives;*
- *forms an integral part of corporate governance;*
- *guides the allocation of resources;*
- *guides an organization's infrastructure, supporting its activities related to recognizing, assessing, responding to, and monitor-*

ing risks in pursuit of organizational objectives;

- *influences the organization's attitudes towards risk;*
- *is multi-dimensional, including when applied to the pursuit of value in the short term and the longer term of the strategic planning cycle; and*
- *requires effective monitoring of the risk itself and of the organization's continuing risk appetite."*

The difficulty with applicability lies in the fact that, while application of the relevant indicators cannot be a problem for risk tolerance as they may well coincide with financial and other performance indicators capturing the effectiveness of the operation of the organisation, the indicators cannot be directly interpreted as measures of risk appetite.

However, if the performance indicators pertaining to the design and maintenance of the risk management framework – as integrated into corporate governance – are considered to be the attributes describing the organisation's risk appetite levels, then comparing the governance processes designed and operated in accordance with the expectations of the environment and the operational goals of the organisation to the best practices known by the environment may serve as a natural measure. The more comprehensive and exhaustive the planned implementation of best practices and the higher the capability level, the lower the risk that may arise with respect to the given governance process and jeopardise the achievement of organisational objectives.

Thus, risk appetite may be defined by the selection of best practices that support the capability levels corresponding to the organisational objectives of operational and governance processes.

Realistically defined, specific organisational and operational objectives, however, also determine the costs that the organisation has the capacity to bear in the course of optimal operation. Accordingly, in defining individual risk appetite levels, management needs to consider the costs entailed by the reduction of the risks' potential negative effect. Definition of the actual and expected costs of the applicable governance practices is another necessary condition of determining the risk appetite levels corresponding to the organisational objectives pertaining to various time horizons and operational areas. *(See Figure 2)*

PERFORMANCE INDICATORS TO BE CONSIDERED IN EVALUATING THE GOVERNANCE OF RISK MANAGEMENT

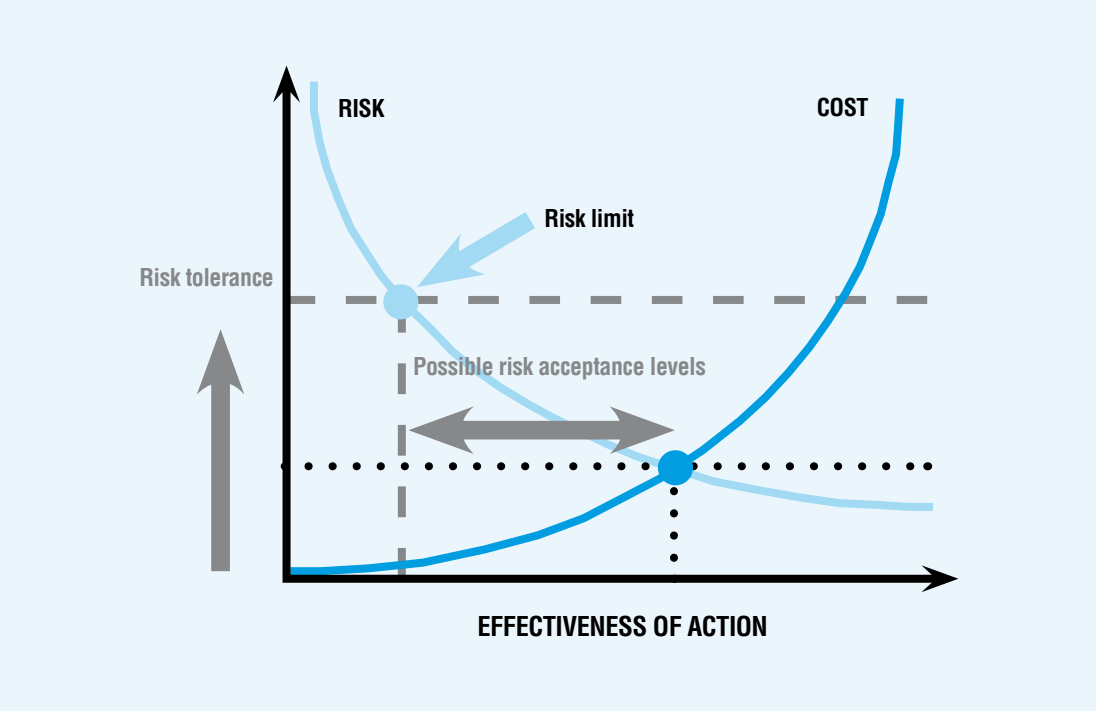
The fundamental principles of organisational risk management are the same for all organisations pursuing independent operations. However, the range of the related governance practices and the capability levels of the governance processes implementing them could exhibit significant differences. Organisations may pursue extensive value-generating activity even without implementing formalised risk management practices. Changes in the stakeholders' expectations, the business environment or the relevant legislative provision, however, may call for a stronger and more clear-cut risk management framework, while developing a risk management system may pose a challenge even for more mature organisations.

The governance of risk management is understood as the management's efforts to select governance practices relevant to the achievement of organisational objectives and to apply them in accordance with the risk appetite levels, expended in the context of enhancing the governance system and making it more efficient.[5]

Risk management should involve risk criteria capable of measuring the effectiveness of governance practices – as risk management

Figure 2

UTILITY AND EFFICIENCY CONSIDERATIONS OF RISK ACTIONS IN DEFINING RISK APPETITE LEVELS



Source: own editing

actions – that support the achievement of organisational objectives and the availability and efficient use of the required resources. Accordingly, the selection and application of governance practices supporting risk management should be examined from the perspective of the extent to which they cover all governance objectives and all operational and organisational levels of the organisation.

In order to determine the scope of risk management governance, there is a need to identify the risk criteria (risk tolerance and risk appetite levels) applicable to the governance objectives used. Bearing in mind the typical space and time horizons of the organisational and operational goals covered by the scope of risk management, the "utility" and "efficiency" criteria of governance objectives can be developed as follows:

- Definition of risk appetite levels by the capability levels of the governance processes supporting corporate governance.
- Definition of risk tolerance by the deviation from the organisational and operational objectives applied at the given level of the governance system.

In order to ensure risk optimisation, the following performance indicators may be used to measure the risk criteria[6]:

- degree of achievement associated with the capability attributes of governance processes with the application of a common rating scale (process profiles under the ISO/IEC 15504 standard); and
- control limits interpreted in accordance with the space and time horizons of organisational and operational objectives.

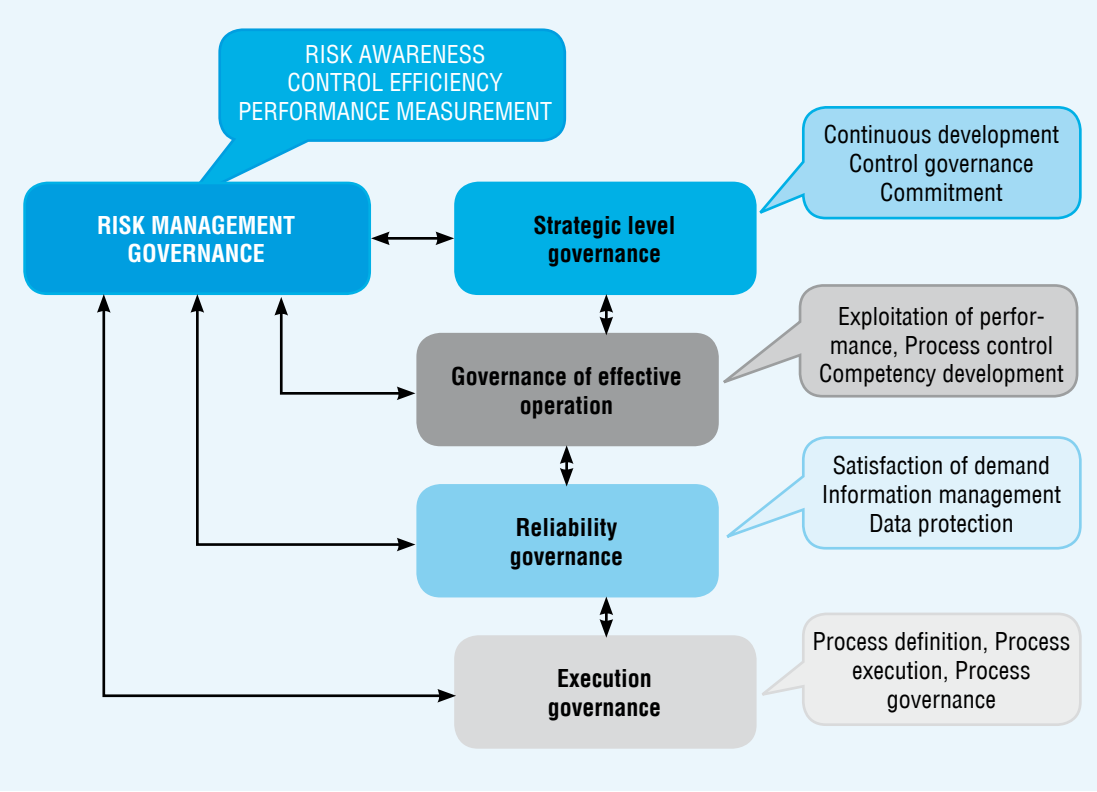
Similarly, in relation to the governance

objectives of risk awareness and control efficiency that support the governance of risk management, a number of risk criteria should be in place capable of measuring the effectiveness of governance practices – as risk management actions – that support the achievement of organisational objectives and the availability and efficient use of the required resources. However, these organisational objectives and resource requirements should derive from the objectives applied by the governance system. Accordingly, the selection and application of governance practices supporting the governance of risk management should be examined from the perspective of the extent to which the "utility" and "efficiency" indicators described above cover all governance objectives and all operational and organisational levels of the organisation. In other words (reiterating the first criterion of the effectiveness of risk management): does the organisation have an up-to-date, accurate and comprehensive (i.e. covering all operational and organisational levels) interpretation of risks? *(See Figure 3)*

Attributes (as prescribed by the ISO/IEC 15504 standard) of the set of governance practices applied and selected from recognised benchmark models and the targeted process capability levels constitute the risk criteria against which the governance of risk management can be measured. Residual risks can be inferred from the process attribute gaps be-

Figure 3

GOVERNANCE OF RISK MANAGEMENT AND GOVERNANCE PROCESSES SUPPORTING THE ACHIEVEMENT OF THE OBJECTIVES OF INDIVIDUAL ORGANISATIONAL AND OPERATIONAL LEVELS



Source: own editing

tween the target and assessed (actual) capability profiles.

The performance indicators of risk management governance[7] are the following.

▸In relation to the governance process of risk awareness:

- management defines the governance objectives and risk criteria of corporate governance (risk tolerance and risk appetite levels);
- risk assessments that consider the time horizon of governance objectives and the risk criteria (risk tolerance and risk appetite levels) are regularly executed;
- risks affecting the objectives of corporate governance are considered in designing the control activities upon which all management statements (reports) regarding the control system are based.

▸In relation to the governance process of control efficiency:

- management ensures the maintenance of adequate organisational structure and reporting routes;
- supervisory activities ensure the periodical review of the effectiveness of the internal control system;
- management examines control deficiencies and takes the required steps.

▸In relation to the performance measurement based on quantitative indicators:

- processes or process elements relevant and significant for the achievement of organisational objectives are selected for performance measurement;
- measures and analysis techniques are developed and maintained for the performance measurement of processes or process elements;
- process execution data are collected and analysed by statistical or other quantitative methods that ensure the understanding of the deviations between the occurrences of selected processes or process elements;
- ad hoc causal factors triggering the deviations of process execution are defined by using the results of the data analysis;
- corrective and preventive measures are taken in order to take account of the ad hoc or other causal factors triggering the deviations; and
- the execution of the selected processes or process elements is monitored and checked with a view to developing stable, functional and predictable processes and keeping within the limits of control thresholds.

Existing governance and control frameworks offer a wide array of application sets regarding the recognised best practices that support the results listed above. At the same time, not all of them are necessarily required for achieving the specific goals of the organisation. When presenting executive statements, management should only select practices which have an obvious relevance to the "utility" and "efficiency" objectives of the given operational level. In relation to risk management governance, these objectives are the following: definition and application of risk appetite levels, as well as risk tolerances to be adhered to at the operational and organisational levels covered by the scope of the governance system.

For thoroughly informed decisions, management should develop and apply the "utility" and "efficiency" indicators considered relevant to governance practices. Where there are significant gaps between the actual (measured) values and the expectations (risk appetite) of management, the practice concerned should be re-designed or corrected. Where the actual indicator values are known and deemed satisfactory with respect to the risk appetite, the application practice can be considered as an executive statement.

Based on quantitative indicators, performance measurement provides a tool for man-

agement for the application of the "utility" and "efficiency" indicators determined by the governance system. Values exceeding the prescribed control threshold signal the necessity of corrective and/or remedial actions supporting the better (safer) achievement of organisational objectives. Since all control and other risk management measures should be considered in relation to organisational objectives, the "utility" and "efficiency" indicators measuring governance practices have a number of different functions. On the one hand, they indicate the level of residual risk relative to the risk appetite level; on the other hand, by the application of control thresholds as a measure of risk tolerance, they create a link between governance objectives and organisational and operational objectives. The rating of the capability attributes of the processes related to governance objectives through risk management governance serves as an indicator to measure the risk tolerance levels prescribed for the individual governance levels of the operation and the organisation.

CONCLUSIONS

In the article we attempted to define, going beyond legal compliance considerations, the effectiveness aspects of organisation-level risk management criteria on the basis of solutions devised – in the context of projects implemented with the support of the European Commission under the direction of the Budapest Business School – for the development and performance measurement of corporate governance. We recommended the presentation of the effectiveness of risk management and the application of assessment (assurance) and process improvement (consulting) methods allowing for the comparability of results based on objective indicators. Governance processes that can be developed – based on existing benchmark models – in the context of governance capability assessment and corporate governance can be applied, irrespective of organisation type, both in the public and the private sectors,[8] as recommended both by the Information Systems Audit and Control Association (ISACA) and by the process assessment model of IT governance (COBIT).

Nevertheless, besides audit specialists, managers and their consultants should also acquire the proposed method (Ivanyos et al., 2015). The cooperation agreement between the State Audit Office and the Budapest Business School may provide an adequate framework for implementing new training programmes aimed at the enhancement and measurement of corporate governance and risk management capabilities. In addition to the training programmes, it would also be expedient to disseminate survey results and experiences to the public sector on a continuous basis.

At the same time, based on the results achieved so far, further research topics should also be explored. Among them, for the purposes of this study we wish to highlight, in view of their existing and long-term significance, two areas for improvement. Firstly, criteria and practices for public sector risk management should be developed and rendered accountable in accordance with the criteria of sustainable development. The second area concerns the functions to be performed in the context of public sector risk management in relation to the development of the regional economy. In our opinion, research on both topics would contribute to the development of public sector institutions and to enhancing our ability to efficiently meet the external and internal expectations intensified by new challenges.

Notes

[1] This is partly owing to the translation of the document entitled "Guidelines for Internal Control Standards for the Public Sector" (*INTOSAI,* 2004) adopted at the 2004 Budapest world congress of INTOSAI, where the Hungarian version of the diagram depicting the control system replaced the term "risk assessment" with the far broader term of "risk management".

[2] Hungarian standard effective from 1 January 2015: MSZ ISO 31000:2015 Risk assessment and management. Basic principles and guidelines.

[3] With respect to the concurrent consideration of time and space considerations, regional economics, for example, distinguishes between "static" and "dynamic" agglomeration benefits, the former essentially allowing for cost reduction while the latter facilitating innovation and differentiation (Lengyel and Rechnitzer, 2004).

[4] The methodology of Governance Capability Assessment (also referred to as "Governance SPICE" by a narrow segment of the academic community) has been developed under the direction of the Budapest Business School and the professional coordination of János Ivanyos, with support from the European Commission under the (IA-Manager and MONTIFIC) Leonardo da Vinci LLP-projects implemented between 2005 and 2010, and presented at professional consultations (with, among others, the President of the European Court of Auditors) and at international and local IIA and ISACA conferences. The methodology developed on the basis of the ISO/IEC 15504 process assessment standard (*ISO/IEC,* 2003) presented at the workshop of the 2010 pan-European EuroCACS Conference of the Information Systems Audit and Control Association (ISACA) in Budapest has been fully incorporated into the Audit Guidelines of the COBIT 5 IT governance framework (COBIT Process Assessment Model) published in 2012.

[5] The model of corporate governance and the risk management and compliance governance scenarios for the selection and application of governance practices supporting the achievement of organisational goals have been developed under the direction of the Budapest Business School and the professional coordination of János Ivanyos, with support from the European Commission under the BPM-GOSPEL (Business Process Modelling for Governance SPICE & Internal Financial Control) Leonardo da Vinci LLP-project (2010–2013). The performance indicators for risk management governance are presented in this article based on the results of this project.

[6] Performance indicators of lower governance and capability levels should be understood as the performance indicators (performance drivers) of the next (higher) level.

[7] The achieved capability levels of the designed (and in this case, risk management supporting) governance processes contribute to effective risk management governance as performance drivers.

[8] The case study (*Trusted Business Partners Kft.,* 2013) on the applicability of the methods presented in this study was prepared under the programme entitled "Corporate governance in public asset management" launched by the management of the Hungarian National Asset Management Inc. (MNV Zrt.) in 2013 for the purpose of improving the governance and risk management practices of companies owned by the state of Hungary.

Literature

Domokos, L. – Nyéki, M. – Jakovác, K. – Németh, E. – Hatvani, Cs. (2015): Risk Analysis and Risk Management in the Public Sector and in Public Auditing. *Public Finance Quarterly,* 2015/1

Farkas, Sz. – Szabó, J. (2005): *A vállalati kockázatkezelés kézikönyve (Corporate Risk Management Handbook)*. Dialóg Campus Kiadó. Budapest–Pécs

Ivanyos, J. – Roóz, J. (2010): A new approach in the assessment of the internal control systems applied in the public sector. *Public Finance Quarterly,* 2010/2

Ivanyos, J. – Sándor-Kriszt, É. – Messnarz, R. (2015): ECQA Governance Capability Assessor Skills for Managing Strategic Directions, Systems, Software and Services Process Improvement. Springer International Publishing, pp. 260−275

Ivanyos, J. – Sándor-Kriszt, É. (2015): ECQA Governance SPICE assessor skills for evaluating integrated risk management scenarios. *Journal of Software: Evolution and Process,* Vol. 27, pp. 545–554, doi: 10.1002/smr.1729.

Ivanyos, J. (2015): A kockázatkezelés újraértelmezése a vállalatirányítás hatékonyabbá tételére (Reconsidering Risk Management for Improving the Efficiency of Enterprise Governance). *CONTROLLER INFO,* 2015/3

Lengyel, I. – Rechnitzer, J. (2004): *Regionális gazdaságtan (Regional Economics)*. Dialóg Campus Kiadó. Budapest–Pécs

Vasvári, T. (2015): Risk, Risk Perception, Risk Management – a Review of the Literature. *Public Finance Quarterly,* 2015/1

Budapesti Business School (BGF) (2015): Organisational and Operational Regulations of the Budapest Business School. Online: http://www.bgf.hu/documents/SZABALYOZO_DOKUMENTUMOK/05szervezeti_es_mukodesi_rend/SZMR_2015_06_26.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004): Enterprise Risk Management − Integrated Framework. Online: http:// www.coso.org/-ERM.htm

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012): Enterprise Risk Management − Understanding and Communicating Risk Appetite. Online: http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013): Internal Control − Integrated Framework. Online: http://www.coso.org/IC.htm INTOSAI (2004): INTOSAI GOV 9100 – Guidelines for Internal Control Standards for the Public Sector. Online: http://www.asz.hu/modszertan/iranyelvek-a-belso-kontroll-standardokhoz-a-kozszferaban-intosai-gov-9100/issai-9100.pdf

ISACA (2012): COBIT Process Assessment Model (PAM): Using COBIT 5. Online: http://www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx

ISO 31000:2009 Risk Management − Principles and Guidelines

ISO/IEC 15504-2:2003 Information Technology − Process Assessment − Part 2: Performing an Assessment

Ministry for National Economy (2012): Magyarországi államháztartási belső kontroll standardok (Internal Control Standards of Hungarian Public Finances). Online: http://allamhaztartas.kormany.hu/download/d/1b/01000/bkstand12közzé.pdf

State Audit Office of Hungary (2015): Az állami

felsőoktatási intézmények gazdálkodása és működése – Ellenőrzési tapasztalatok (Financial Management and Operation of Public Higher Education Institutions – Audit Experiences). Online: http://www.asz.hu/tanulmanyok/2015/az-allami-felsooktatasi-intezmenyek-gazdalkodasa-es-mukodese-ellenorzesi-tapasztalatok/az-allami-felsooktatasi-intezmenyek-gazdalkodasa-es-mukodese-ellenorzesi-tapasztalatok.pdf

Trusted Business Partners Kft. (2013): Kockázatkezelési Esettanulmány – Integrált megfelelés-irányítási forgatókönyvek alkalmazása a vállalati kockázatkezelésben (Risk Management Case Study – Applying Integrated Assurance Management Scenarios in Enterprise Risk Management). Online: http://mnv.hu//data/cms938892/hatarozat_1._sz._melleklete_Kockazatkezelesi_Esettanulmany_v2.pdf