László Domokos – Melinda Nyéki – Katalin Jakovác –
Erzsébet Németh – Csaba Hatvani

Risk Analysis and Risk Management in the Public Sector and in Public Auditing

Summary: The significance of organisational risk management has grown ostensibly during recent decades, and this is true regarding for-profit organisations and public entities alike. There are, however, unique traits that characterise risk analysis and risk management as applied in the public sector, both in terms of areas of application and execution. Being mandatory is the foremost feature of risk management as applied in the public sector, with efforts to minimise risk, and the promotion of compliant operation and financial management serving as the goal. A conclusion that can be drawn from the State Audit Office's audit and research experience is that even though internal controls are usually developed for risk management in organisations belonging to the central and local government subsystems of public finances, the conscious management of risks is not implemented. Organisations are yet in the learning phase of how to integrate risk management with organisational operations.

Keywords: organisational risk, risk analysis, risk management, organisational integrity, Supreme Audit Institution
JEL codes: D81, D83, G32, G38, H83

The risk-focused description and definition of organisations' operating environment and operations has gained increasing prominence over recent decades. Not only is this typical of the business sector, but also public entities. This "revolution of thinking" is attested by the abundance of international literature that deals with risk management, along with the increased prevalence of regulations on risk-related activities and of "good practices" supporting regulatory compliance. However, while the risk interpretation and risk attitude of a for-profit organisation is easy to delimit, and maximising profit and increasing enterprise value are the ultimate goals of risk management, these aspects are given a specific interpretation in the public sector.

The objective of this article is to provide insight into the particularities of risk analysis and risk management methods used by public entities in Hungary, as well as to present the features of a special area, i.e. selection-driven risk analysis that is applied during the State Audit Office's activity. To this end, we will first review the risk interpretation used in the public sector, the regulatory framework, and the areas of application. Then, the risk management of organisations will be presented based on the State Audit Office's experiences, using the results of its annual integrity surveys and its audits.

Levelezési e-cím: jakovac.katalin@asz.hu

THE CONCEPT OF RISK

Risk, risk analysis, risk assessment and risk management are all frequently used expressions in both the business and the public sector today; however, the overall picture is mixed as regards the interpretation of these concepts. The definition of risk varies by theory, such as in the technical, economic, psychological and sociological approaches (Vasvári, 2015). The risk concepts used in the public sector stand closest to what is known as the economic approach; they, however, regard risk in negative terms in most cases. Risk definitions related to risk management include the following.

- Risk is the chance of an event occurring that has a negative effect on the achievement of goals (COSO ERM).
- Risk is the positive and/or negative effect of uncertainty that influences the accomplishment of organisational goals (ISO Guide 73:2009, linked to the ISO 31000:2009 Risk Management standard).
- Risk is a factor that threatens the achievement of organisational goals [Government Decree 370/2011 Article 2(m)].
- In general, risk is some kind of event, activity or failure to perform an activity, which will likely occur in the future, and if it does, this will generally have a negative, but in some cases a positive effect on the achievement of the given organisation's goals (Internal Control Manual, Minister of Finance, 2010).
- Risk is the probability of all such elements and events occurring that may have an adverse effect on the operation of a budgetary institution (this is the definition typically found in risk management regulations).

The different definitions of the concept of risk include common elements that are generic in terms of content: they identify risk with an undesirable event (failure to perform an activity, error, deficiency, irregularity, damage, loss) that may potentially occur, and the impact(s) of which pose some kind of a threat, varying in degree, to achieving organisational goals, the operation and activities of the organisation, its catering to its duties or the implementation of a project. These examples also aptly illustrate that the interpretation of risk as a potential event (with a negative effect) is mixed with the notions of "impact" and "probability", which are required for determining its degree.

THE REGULATORY FRAMEWORK OF ORGANISATIONAL RISK MANAGEMENT

In public entities, the regulations of financial management and control systems were developed in the course of a multiple-step process. After the legislative basis was created, the regulatory concept was developed under the influence of the COSO model from 2009. New regulation appeared regarding the development of an internal control system for budgetary institutions, one that also included modern elements of responsible organisational governance and management (Ministry for National Economy, 2012).

The basis for this regulation is provided by the Act on Public Finances[1] ("Áht.") and Government Decree 370/2011[2] ("Bkr."), which define activities related to risk management as part of the internal control system. Áht. provides for the obligation of operating an internal control system, and Bkr. for the development of the internal control system, including risk assessment and management.[3] The Decree defines risk as a factor that threatens the achievement organisational goals, and a risk management system as the sum total of management tools and methods with elements including the identification, analysis, grouping and tracking of risks, and the mitigation of risk exposure as necessary. Legal regulations do not elaborate on risk management methods, so the responsibility for the development of an adequately

detailed process, its alignment with organisational goals and features, and its operation lies with the head of the organisation.

The expression "risk" itself appears on its own or as part of a conjunction is numerous legal documents (the word "risk" occurs in 426 legal documents, "risk analysis" in 278, and the word "risk management" in 228). The definition of the term, however, is not consistent; risk can be an event, as well as the possibility, probability or effect of an event.

The following regulatory examples are highlighted regarding organisational risks that arise in areas that are easily delimited within organisations.

Information security risks: In terms of protecting information stored and processed in central and local government bodies' electronic information systems, risk is the "degree of threat exposure". [4] Regulation is aimed at prevention and awareness raising, and the conscious management of any problems arising in the case of security incidents (e.g. ranking the organisation in what are known as security classes, developing an action plan required to achieve the stipulated security level and the introduction of safeguards commensurate with risks).

Risks related to integrity: the legal regulation[5] defines integrity risk as the possibility of a public administration body's integrity being harmed, and corruption risk as the possibility of granting or acquiring undue advantage. The Decree stipulates the annual survey of corruption and integrity risks, the development of an annual action plan for corruption prevention, and the preparation of an integrity report on the implementation of the plan.

Risk to health: "the combined effect of the probability and severity of health damage in an emergency".[6] In the labour safety domain, risk management means the systematic and regular analysis of risks to employees' health, along with measures specified and implemented to minimise health damage.

Some legal regulations specify requirements for the processes of managing risks outside the organisation. Such risks include those related to financial and investment activities; insurance risks; (public) health risks; risks to national security, security of supply, and food safety; force majeure risks (e.g. weather and other nature-related risks affecting agricultural production); risks taken into account in external audits (e.g. risk of tax fraud); risks involving the macro-economy (e.g. sustainability risk).

AREAS OF APPLICATION OF RISK ANALYSIS AND RISK MANAGEMENT IN THE PUBLIC SECTOR

There are countless events and circumstances that may hinder or threaten the achievement of any organisation's goals – regardless of whether it operates in the private or the public sector – as well as the optimal structure and performance of its activities. Most such evens can be predicted, their circumstances and impact can be estimated, and organisations can prepare for their occurrence or mitigation. Risk management is an organic part of responsible organisational governance; in terms of determining its goals, defining risk, and detecting risks, however, public sector institutions have unique traits that differ from those of organisations in the corporate domain.

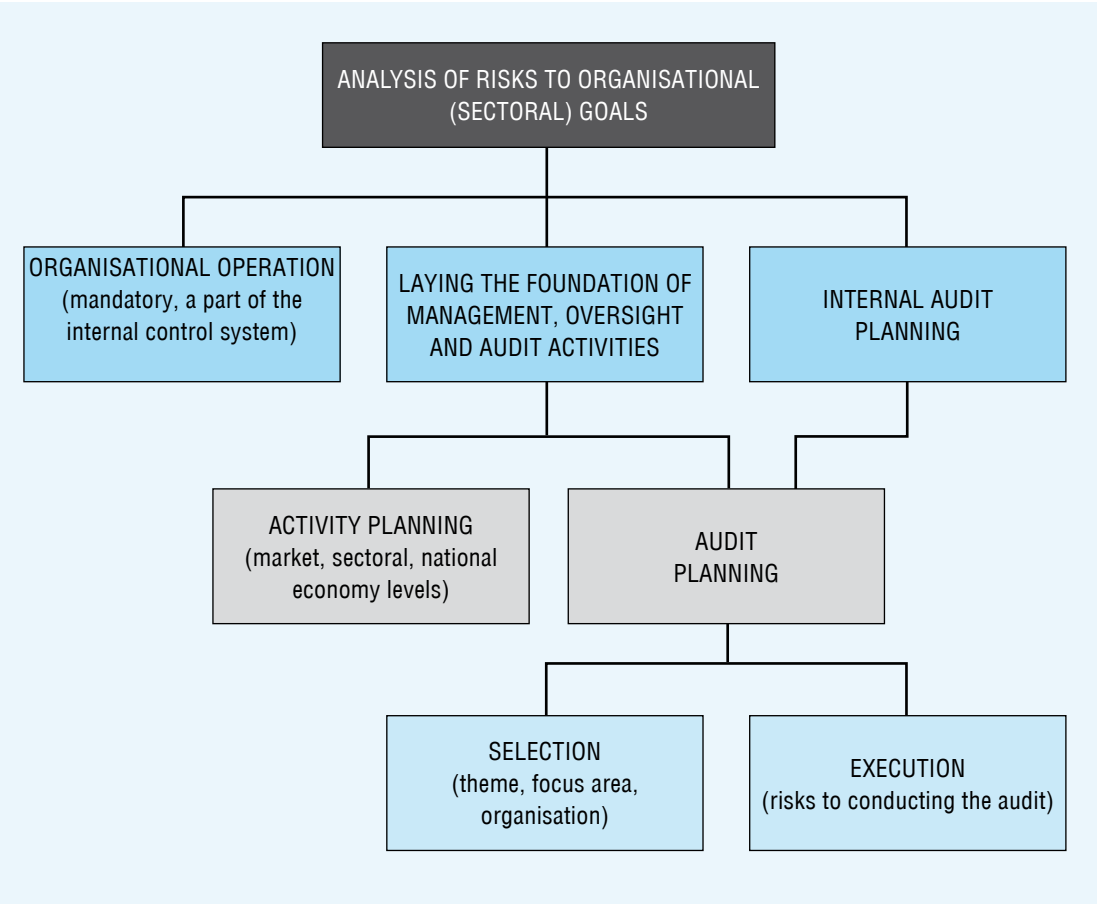
Chart 1 illustrates the grouping of areas and activities that use risk analysis and risk management.

Risk analysis performed by internal audit

Analysis by an independent internal audit aimed at selecting areas to be audited specifies the risks inherent to a budgetary institution's activity and internal control system. Internal

Chart 1

AREAS AND ACTIVITIES THAT USE RISK ANALYSIS



Source: Authors' own editing

audit uses a systematic and regulated procedure to assess the organisation's risk management processes, and its recommendations can actively contribute to their improvement and to informing responsible management. Internal auditors assess whether or not specific controls are effective in addressing the risks concerned, and conduct follow-up audits to determine whether the measures implemented have actually eliminated the risk detected, or reduced it below the risk tolerance limit. Therefore, in practice, in addition to external audits, it is internal audit that can cater to the continuous quality assurance of risk analysis and management practices in organisations.

Risk analysis conducted during management, oversight and audit activities

Oversight, (sectoral) management and audit duties are part of the core activities of numerous institutions, and performing these is likewise supported by risk analysis, which points attention to the riskiest areas, topics, processes, activities and organisations. Typical examples include the system of macroeconomic analyses carried out during budget planning, and the planning and monitoring of sectoral governance and oversight activities.

Within the planning of audits, the selection process and the analysis of audit subjects'

risks that supports sampling procedures can be distinguished logically from the enumeration of risks to the conduct of the audit. Risks are analysed by the audit organisation, but the risks themselves can arise in the audited organisations in the former, and in the auditing organisation in the latter case; the analyst and the party at risk are therefore separated from each other. Risk management is also given a specific interpretation in connection with audit activities, the reason being that measures aimed at reducing risks are implemented by the audited person (organisation), e.g. by preparing an action plan or regulating based on recommendations, findings or obligations imposed (in a resolution) by the audit organisation.

The fundamental question during the identification of risks, i.e. "Which are the possible events the effects of which can threaten goals?" remains unchanged. In this case, however, "goal" is not construed to mean an organisation's goals, rather, in broader terms, the basic social expectation of the compliant and efficient utilisation of public funds (this goal, by the way, also fundamentally defines the organisational goals that public entities have).

In the course of risk analysis, necessary, relevant and reliable information must be collected, possible threats identified and analysed (impact, probability), then evaluated. In that case, risk analysis is directed at mapping the areas and processes that bear the greatest risk, and at identifying and assessing risks present in organisations that can be audited. Where analysis involves a population (e.g. central subsystem institutions, partnerships, private individuals) with a great number of elements, the key goal of risk analysis is to sort the elements according to the specified risk criteria, i.e. to establish a kind of risk "ranking" in the interest of selecting the riskiest elements.

Risk analysis by Supreme Audit Institutions: the European Court of Auditors' methodology

Supreme Audit Institutions engage in risk analysis during the selection of audit priorities and areas, the analysis of audited entities' controls and measures, as well as the specification of audit questions and scope. At the same time, auditors also need to manage detection risks when conducting audits. These processes will now be presented on the basis of the European Court of Auditors' (ECA) methodology.

A dynamic review of policies and risks serves as the starting point for ECA's work programming system, in the course of which it takes risk analysis results into consideration, along with policy developments, stakeholders' priorities (including reports on EU budget final accounts), the outcome of the latest audits, the activity of other Supreme Audit Institutions, the accomplishments of the auditing profession, and any relevant media coverage. ECA specifies priorities as the result of this policy and risk review, including proposals on the distribution of tasks and a multi-year outlook plan that guarantees the achievement of strategic objectives. The document that contains ECA priorities provides a strategic foundation for the following year's annual work programme.

Possible audit topics may be selected along the lines of budget lines, the managing or beneficiary organisation, policy tools, programmes, projects, or a combination of these. It is important for the theme to be suitable for auditing, to have a sufficient impact, and to be selected in line with the strategy. The goal of the ECA-level standard analysis of potential audit topics is to allow the pinpointing of any possible deficiencies, overlaps, factor groups and synergies within the proposed audit assignments, thereby contributing to maximis-

ing the effect of the ECA's work in addition to the best possible utilisation of resources.

Audit risks can arise regarding financial reporting, compliance (ECA, 2012), and performance audits (ECA, 2006), or in all three areas at the same time. The ECA risk assessment is based on the COSO methodology. Audit risk comprises the following:

❶ inherent risk related to the nature of the audited party,

❷ control risk related to the audited party's controls, and

❸ detection risk, i.e. the risk of the auditor failing to detect discrepancies.

Auditors rely on different sources of information to engage in risk assessment procedures as early as during the audit planning stage. Risk assessment has to link information acquired from the audit area with the specification of audit questions and scope. Risk identification and assessment are not exact disciplines, and principally depend on the auditor's sound professional judgement. In forming their opinion, auditors have to rely on their know-how, the analysis conducted, and their experience. In the course of conducting an assessment, auditors have to be thorough, acting systematically and comprehensively so no significant risks go undetected.

Auditors ask the following questions: What error or discrepancy can result? What is the probability of that occurring? What consequence will this have? What kind of strategy does the audited party apply to reduce risk to the lowest possible level or to control it? Risk factors include the following: the nature and complexity of policy, the programme and operations; the diversity, consistency and clarity of the audited party's objectives and goals; the existence and use of performance measurement; the availability of resources; the complexity of the organisational structure and the clarity of responsibilities; the existence and quality of control systems; the complexity and quality of management information. During the preliminary study, the relative significance of these criteria must be analysed in the planning stage. Auditors usually concentrate on risks that may occur with a greater probability, and have a greater impact should they occur; and in doing so, they also take into consideration any steps the audited party may take in trying to reduce such risks.

The ECA believes that its performance audits:

❶ reflect risks in financial management, public interest, and the value-adding capacity of public sector audits,

❷ focus on questions related to performance, including such as may garner public interest, and are related to high-level EU objectives or policies that embrace multiple areas.

During performance audits, the risk assessment procedure is made up of four consecutive steps (ECA, 2013), each of which act as a kind of filter. Auditors can thus use information obtained about the audit area as the starting point to focus on the critical risks, which allows them to define the possible audit questions, as well as the potential scope of the audit.

❶ As the first step, the auditor will present the area to be audited in a diagram or logic model, and list the expected key controls. The programme logic model allows specifying and presenting the relationship between the socio-economic needs targeted by the intervention on the one hand, and the objectives, inputs, processes, outputs and outcomes (including results and impacts) on the other hand. The auditor may also present one or several elements of the model in greater detail, in a flowchart.

❷ The second step involves risk identification, including information about discrepancies, their main reasons, and the key potential consequences. A thorough review of the list of identified risks will be used to determine the significant and relevant ones among them.

❸ Analysing the probability and effect of these risks with an eye to assessing the level of risk is the third step. Then, the auditor will examine management responses and existing controls in respect of risks considered medium and high.

❹ The last step focuses on the key risks, and defines audit questions and the scope of the audit.

ECA published two landscape review reports in 2014: one regarding risks to the financial management of the EU budget, and one about shortcomings in accountability and the auditing of public funds. These reports built upon ECA's audit experience to discuss comprehensive policy areas and complex questions with the goal of informing decision-makers about current risks and challenges, so as to help them specify the areas where greater public insight should be granted, and more audits conducted.

THE ORGANISATIONAL RISK MANAGEMENT PROCESS

The following will present the key steps of organisational risk management using the SAO's experiences. The SAO has significant experience regarding the risk management processes that have been developed in public entities, since it gains an insight into both the development of internal regulation and risk management practices by virtue of the annual integrity surveys and its audits. The SAO evaluated the internal control system and more specifically the risk management system in a third of its audits in 2013, and in a fifth of its audits in 2014.

For organisations in the corporate domain, risk management is a modern organisational governance tool that seeks to optimise the result of business decisions. In the public sector, however, organisations with a hierarchical structure subject to bureaucratic control are seldom exposed to obvious "shocks", nor does the market signal their relative lags. Performance measurement is mostly benchmark-based, and currently there are few indicators to measure operational efficiency. For public sector institutions, risk management, including a conscious awareness and the active control of risks, is not only in the best interest of organisations, but also their statutory obligation. Its greatest value lies in its incorporation into a process and its regular and repeated execution, since it is impossible to gauge every risk even with the greatest level of preparedness when various specific decisions are made, but even if this were possible, the probability and potential effect of risks change continuously (Hornai, 2001, p. 43).

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".[7] So, the head of a public entity seeks to minimise risks, even if measures adopted to this end might have an excessive resource need. In many cases, there may – according to some theories – also be non-transparent goals underlying decisions made by senior officials, and knowing these can also help risk management motivations.[8] Loyalty, the joy in acting for the public or increasing power, income, prestige, security or comfort may, for instance, be such leader's goals (Blais and Dion, 1991). These factors may also play a role in how the risk perception and risk management attitude of a bureaucratic organisation's leader develops (Gajduschek, 2010).

The analysis and assessment of risks at public sector institutions plays a key role primarily in the selection of the appropriate control activities. Any control system can only respond properly to the risks for which it was created. So, as risks change, so should control

systems be tailored to the conditions undergoing changes. Achieving goals is not guaranteed even so; *Merétey-Vida* (2004) point out that only the level of what we refer to as reasonable assurance can be reached due to the risks that remain in the system (e.g. false perception, collusion or applying the cost to benefit principle). The probability of risk events occurring and/or their effect, however, can be reduced with control and monitoring activities in a control environment that is appropriately aligned to organisational characteristics.

The risk management process is also described by the standards and guidelines of international organisations and government institutions, including COSO ERM, the HM Treasury Orange Book, INTOSAI GOV 9130 Guidelines, the Risk Management standards by the Institute of Risk Management (2002) or the Australian and New Zealand Risk Management Standards (2004). Based on these, it is possible to define six steps in the risk management process, regardless of the domain in which an institution functions, from legislation through administration, environmental protection, healthcare, education and defence, to local governments. *Chart 2* presents a summary of these steps.

Specifying the risk management framework

The entire risk management process is conditional to organisational goals being known, and the relevant risks being established with reference to those goals. Reducing the number of risks or avoiding them is not necessarily the goal of risk management, instead, it is to minimise the possible effects of risks by achieving and maintaining the highest possible level of risk awareness (Hornai, 2001). The risk attitude of the organisation's leaders also influences the key goal of risk management. The public sector is specific in this respect as well. Namely, increasing social utility and serving the public good is the behaviour expected of the organisation, which it implements on a not-for-profit basis, under an obligation to perform duties. This is why the leader's primary goal is to perform the activities that are stipulated in legal regulations and other obligations. Risk events may pose a threat to the compliant, effective and cost-efficient performance of activities subject to some level of occurrence probability, and some degree of negative impact. This stage is properly established if the goal, object, stakeholders, characteristics, key inputs and outputs, outcomes, external and internal environmental criteria (including the risk of fraud and corruption) of the organisational processes are identified.

Risk identification

Risks must be mapped to actual processes and activities, as generalisations on risks will lead to analyses for their own sake. The identification of risks can be aided by answering questions like: What kind of process error can impede the achievement of goals? Which are the factors that need to be present and appropriately applied in order for the process to be completed properly? Does the process inherently include any criteria that may result in financial or other losses?

Specifying the root causes of risks (risk sources) can help in identifying risks.

Risk analysis

In every case, the general purpose of risk analysis is to identify the risks to achieving goals, and to assess them in the interest of specifying responses (measures). During risk analysis, the probability of occurrence and potential

Chart 2

THE STEPS OF THE RISK MANAGEMENT PROCESS

Risk management sub-process	Main focus	Content
DEFINITION	What is the framework? What can be subject to threat?	Determining goals, the economic and legislative environment, affected processes and activities, and recording the expected state.
IDENTIFICATION	What can happen? What have we not thought of so far?	Exploring and identifying possible risks, enumerating potential threats.
ANALYSIS	How likely is it? What and how great are the possible impacts?	Grouping and perception of risks, probabilities and expected impacts, estimating the magnitude of risk.
ASSESSMENT	What are the priorities? What is relevant?	This establishes relevance, priorities and acceptance level, and enumerates existing protective measures and required resources.
RESPONSES	What should we do?	Decision process about risk management measures and their implementation.
MONITORING	Are we doing it right?	Observing risk occurrence and impact, tracking and reviewing the measures taken, providing information to management. Revision of the risk management framework and, if necessary, the set of risk management criteria, having regard to any changes that occurred in the meantime.

Source: Author's own editing using Hornai (2001)

impact of various risks is estimated, and any factors that may influence the risks are listed. There are essentially two kinds of methodology used for this. Qualitative analysis, which determines risk severity levels, can be broadly used primarily in the case of risks that cannot be quantified, but it is less exact and also includes subjective elements. The resolution of the quantitative analysis of specific quantifiable risks is much finer and has a mathematical background. Individual risks can be modelled by modifying the selected variables, which leads to more accurate risk values that are closer to reality. Applying EVT (Extreme Value Theory), a relatively new branch of statistics, can take the spotlight in disaster management, healthcare or food safety, as it focuses on modelling events that occur with very low probability, but are extreme in terms of their risk impact (e.g. unusually heavy flooding or an extreme traffic situation). The analytical methods used may also involve the combined application of qualitative and quantitative elements, depending on the reliability, amount and quality of available information.

While in the business sector risks can, in most cases, be expressed in monetary terms based on the difference between a desired state and that actually achieved, they are harder to quantify in the public sector. The reason for this can be the nature of the activity (e.g. legislation, administration), the uncertainty in assessing outcomes produced in the long term (education, long-term investment projects and

development), or lack of information (e.g. a lack of past experiences or comparative data). Where suitable records or a case background is available for specific risks, the probability of occurrence and, in many cases, the effect of a risk can also be quantified using statistical methods (e.g. amount of public funds affected, duration of deviation from a fixed time limit, number of items erroneously posted to the books). Individual risks quite frequently have several potential effects, and some organisations seek to specify these in terms of multiple aspects such as an "impact on the operational process", "financial impact", or an "impact on the strategic goal".

In practice, the quantification of risks is generally understood as the ranking, using scales of 3 to scales of 5, of the estimated magnitude of impact on goals and that of the probability of occurrence. The degree of impact ranges from negligible to very significant, and the probability of occurrence from very low to almost certain. This qualitative method of analysis may rely on the opinion of experts or expert working groups, case studies and previous similar practices. It is expedient for the scale value applied to depend on the development of some kind of indicator assigned to the given risk or its variation between specified value limits (e.g. a classification of the number of yearly occurrences or the ratio of pecuniary damage to the annual budget). There is no single methodology that can fully screen out the subjective elements of analysis, but where analysis criteria and assessment are based on a consensus, disputes can be avoided.

Risk assessment

Risk matrices comprise the most widespread method of risk assessment, and serve to determine the significance of risks and their order of priority. The matrix is a two-variable "weighting" procedure, where one variable is the extent of impact, and the other is the probability of the risk occurring. Risk values are most often expressed in textual form (low, medium, high). Using a risk matrix reflects the practice-oriented approach of analysis, but it has the drawback of taking only two factors into consideration. Materiality level can be determined once the resulting risk values are known, and it serves as the baseline for identifying the relevant (material) risks of the various processes/activities, as well as for the ranking of processes by risk. An organisation's risk-taking level (risk appetite) is a cardinal matter for risk assessment, i.e. the level of risks the organisation is ready to accept before it deems necessary to take response measures. This is because the decision on measures is correlated to the degree of risk an organisation accepts.

Responses

Planning decisions on response measures can be facilitated by questions like: "What measures are there to ensure that such process errors or deficiencies will occur less frequently?" and "Are these actions suitable for reducing risks to an acceptable level?" Risk assessment also sees the determining of whether or not appropriate protection (control) is available, how efficiently it functions in the interest of preventing and reducing risks (assigning controls to risks), as well as the kind and amount of resources any possible measures will require. In the case of public sector institutions, the efficiency of control points that can be identified in the processes and that of their operation, i.e. the "coverage of risks" is one of the key issues. In numerous cases, there are multiple control activities in place to mitigate a given risk, therefore the combination and effectiveness of controls also needs to be evalu-

ated, along with whether or not unnecessary control activities can cause any decrease in efficiency.

Regarding the responses that can be given to risks, four fundamental types may be distinguished, namely: transfer, tolerate, treat, and terminate (INTOSAI GOV 9100). Organisations acknowledge risks below the acceptance level (tolerance limit), and this can also be supplemented by involving some kind of control activity (e.g. incidental audits). An organisation must, however, take response measures in the case of risks above the tolerance limit. Certain risk management measures may give rise to additional risks, and these also must be taken into account during assessment. These include, for example, outsourcing or engaging an external expert. Such measures depend on the partner's capacity to perform, while they typically appear as an integrity risk in organisations. A PPP arrangement can also be an example of this. Even though the point of a PPP is mutually advantageous and efficient risk sharing between the business partner and the public sector organisation, this is not achieved in many cases (Braunné, 2010).

The option of discontinuing activities is limited or impossible; this is because the very reason some activities are performed by the public sector is that nobody else is willing to assume their inherent high risks in order to achieve a goal that serves public interest (these can include e.g. national defence or disaster management).

The most frequently used methods are collected (in a standard-compliant grouping) in *Chart 3.*

Monitoring

Responses for managing risks are suitable if their implementation actually results in the reduction of risks, and the more efficient and budget friendly achievement of objectives. This is why the implementation of actions and their effects must be tracked continuously with particular attention, and reviewed as necessary. Risk management will only achieve its goal if it does not only appear in the organisation's operation as a required element of the internal control system that must be implemented as a rule, but as an organic part and an active tool of management.

Audit and research experiences

This chapter describes the State Audit Office's experiences concerning organisations in the central subsystem and local governments. In terms of the risk analysis and management practice of public sector institutions, it is in part the findings from SAO audits, and in part data from annual integrity surveys that provide opportunities for analysis [see Pulay (2014) on the role of integrity]. Integrity questionnaires are completed voluntarily, so these surveys render information about the "self-perception" of respondent organisations regarding their risk management activity. The SAO has also prepared a summary study about integrity survey results (Szatmári – Kakatics – Szabó, 2014a). The proportion of organisations that engage in systemic risk analysis – other than planning internal audit tasks – has not changed substantially based on the 2014 survey (2013: 38.2 per cent, *N*=1462; 2014: 37.7 per cent, *N*=1584).

Institutions of the central subsystem

Integrity surveys

The questionnaire was returned by 40.9 per cent of the 736 budgetary institutions (*N*=301) belonging to the central subsystem that were invited to respond. Based on the answers,

Chart 3

METHODS APPLIED FOR IMPLEMENTING RISK MANAGEMENT

Methods	Typical examples	
TRANSFER	Taking out insurance (primarily asset cover)	
TOLERATE	Acknowledging and accepting risk	
TREAT	PREVENT (reducing the probability of risks occurring)	• control activity (e.g. detailed internal regulation, the four-eyes principle, separation of duties and powers, access and decision-making rights, authorisation and approval procedures, consultation, certification) • modification of decision • asset protection, protection systems, security measures • IT support • organisational hierarchy • corporate decision-making • monitoring • quality assurance • integrity • the deterrence factor of accountability and sanctions
	SHARE (reducing impact, mitigation of damage upon occurrence)	• taking out insurance policies • outsourcing of task/activity (with the inclusion of risk management costs in the fee) • PPP arrangements • engagement of external experts (with the inclusion of risk management costs in the fee) • sanctions
TERMINATE	• suspension of any risky activity (that can be undertaken voluntarily) with an uncertain outcome • avoiding risky activities	

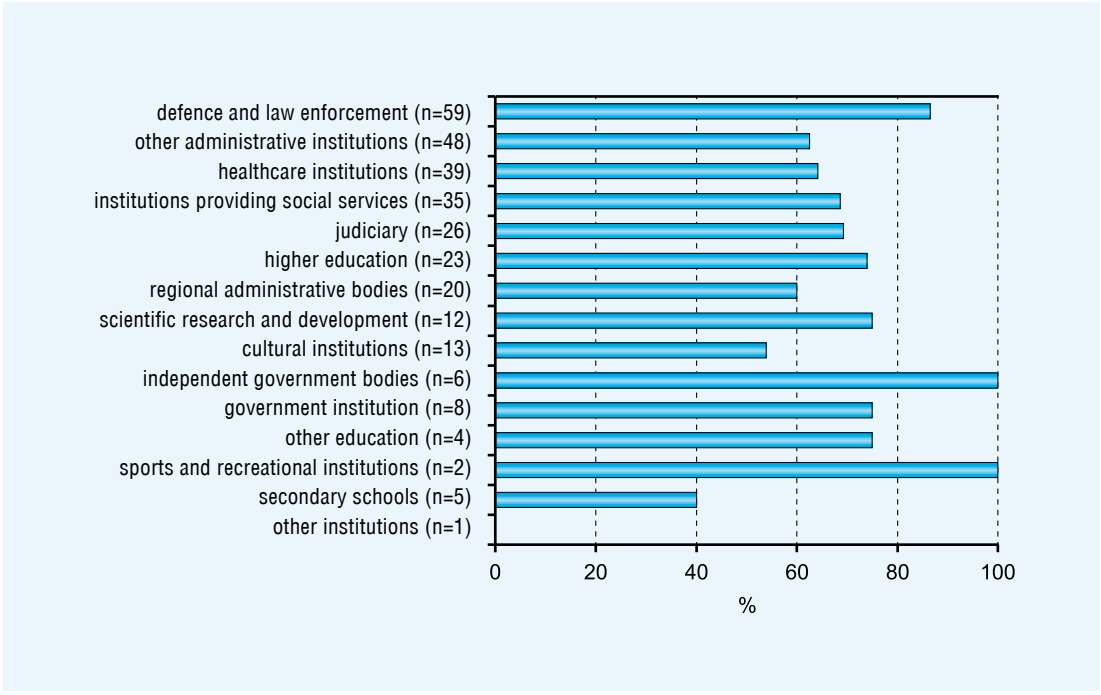
Source: Authors' own editing

only 70.4 per cent of budgetary institutions belonging to the central subsystem engage in systemic risk analysis despite the mandatory requirements. This proportion varies by institution group, as shown in *Chart 4.*

According to the survey's results, 80.7 per cent of the organisations that engage in risk analysis record risk factors identified during risk analysis in some sort of database. 95.8 per cent of the institutions stated that they evaluated risk analysis results; the application of risk management, however, is not consistent. Based on the responses, 66.5 per cent of the organisations manage risks in every case, and 31.1 per cent do so occasionally. 2.4 per cent of organisations – as they admitted themselves – never react to the problems detected. 94.7 per cent of respondent organisations perform regular risk analysis to substantiate audit plans. Less than a third (30.6 per cent) of respondent central organisations engage in corruption-related risk analysis. This control tool carries significance primarily in the case of budgetary institutions with a higher inher-

Chart 4

INSTITUTIONS BELONGING TO THE CENTRAL SUBSYSTEM THAT ENGAGE IN REGULAR RISK ANALYSIS (BY INSTITUTION GROUP AS THE RATIO OF RESPONDENTS, *N*=301)



Source: Authors' own editing

ent exposure to risk derived from administrative enforcement and the provision of public services, as its absence may reduce such organisations' integrity, and their capability to respond in order to counter corruption risks.

Audit experiences

The SAO audits internal controls using risk analysis as the basis, with efficiency and effectiveness in mind. In other words, not only does it assess the existence and quality of the regulatory environment, but also whether or not institutions use their lines of defence effectively. The 2013 final accounts audit found that in both the institutions and the organisations of institutional titles[9], risk management was the element of the internal control system where the greatest number of deficiencies was encountered.

During the final accounts audit, risk analysis was used to select, from the audit areas concerned, the organisations whose internal control systems were to be evaluated. The scope of the audit also included risk management, which constitutes an integral part of the internal control system. Individual findings were corroborated with audit evidence (regulations, certificates, minutes, declarations).

The main selection criteria included taking results from the preliminary survey of total budget expenditure and the internal control system's elements into consideration, along with increasing the coverage of institutions that can be included in the revision of final accounts. From the results of the final accounts audit, the following will highlight and detail the experiences acquired during the assessment of the internal control system in 63

budgetary institutions and 94 institutional title organisations. Of the 94 organisations, 30 were healthcare institutions.

Results

Based on audit experiences, the regulation of risk management essentially covered statutory requirements; however, internal regulations were not fully updated, and there were also some content-related deficiencies. In the majority of the audited entities (87.4 per cent), risk management regulations were rated compliant. The highest ratio of compliance with statutory requirements was seen at water management directorates (100 per cent) and law enforcement bodies (90.9 per cent), while most deficiencies were encountered at environment protection inspectorates, with 20 per cent of organisations rated non-compliant.

Only 93.7 per cent of organisations had effective procedural rules for risk management. The reason for the deficiencies was in part failure to update regulations, and 4 organisations did not even draft them despite statutory requirements that impose this as an obligation, nor do they engage in risk management activity. The major shortcoming of existing internal regulations was that they did not contain stipulations applicable to reviewing the risk environment (in 9.24 per cent of organisations with procedural rules in place), and to considering the feasibility of available responses to risks (5 per cent). *(See Chart 5)*

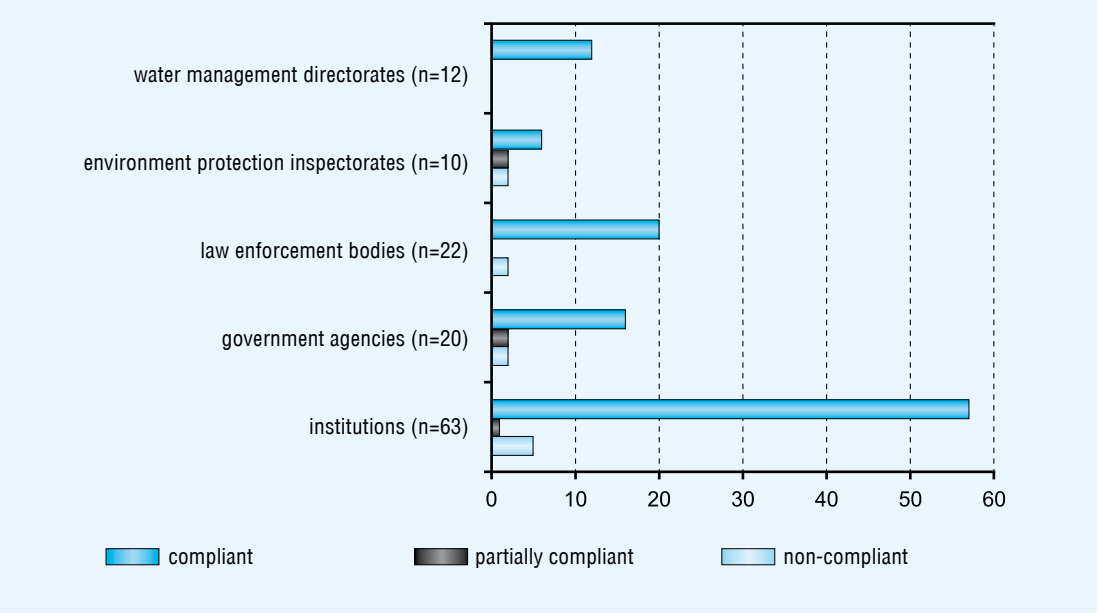
Risk management activity was rated compliant for 29.1 per cent, partially compliant for 40.2 per cent, and non-compliant for 30.7 per cent of the audited entities. The best ratio of compliance with requirements (41.7 per cent) was seen regarding the practices of the water management directorates, while those of law enforcement agencies proved to be the most deficient (45.5 per cent). Risks associated with activities were assessed (85 per cent) and analysed (81.1 per cent) in the vast majority of organisations; more than a third of the organisations (49), however, failed to properly manage risks. One of the reasons behind this was that more than a half of the organisations (56.2 per cent) did not specify an acceptable level of risk, nor did they consider the feasibility of answers (response measures) that can be given to risks (58.3 per cent). The logical pitfalls of implementing risk management in practice are well illustrated in the fact that five organisations considered possible response measures without specifying the level of acceptable risks. The final step of risk management, i.e. reviewing the entire process itself, shows a somewhat more favourable picture, but even so, just over two-thirds (67.7 per cent) of organisations completed this during the reporting year concerned. *(See Chart 6)*

The results of risk management rating were also examined relative to the audited organisations' budgets for 2013. From the data reported in the financial statements for 2013, adjusted total expenditure appropriations for the year concerned were taken as the basis for ranking the organisations into three classes. The assumption that risk management practices in organisations with a greater budget and a more articulated organisational hierarchy are more appropriate could not be confirmed. No correlation was found between organisation size and risk management ratings. Assigning the values of 1, 2 and 3 to the non-compliant, the partially compliant and compliant ratings respectively, organisations with a smaller total expenditure below HUF 5 billion can be characterised with an average of 2.02, medium-size ones with a budget of HUF 5–10 billion with 1.79, and larger ones with a budget over HUF 10 billion with 2.11. Based on these results, it was the medium-size organisations that least complied with requirements for risk management. *(See Chart 7)*

The work forms used during the audits also

Chart 5

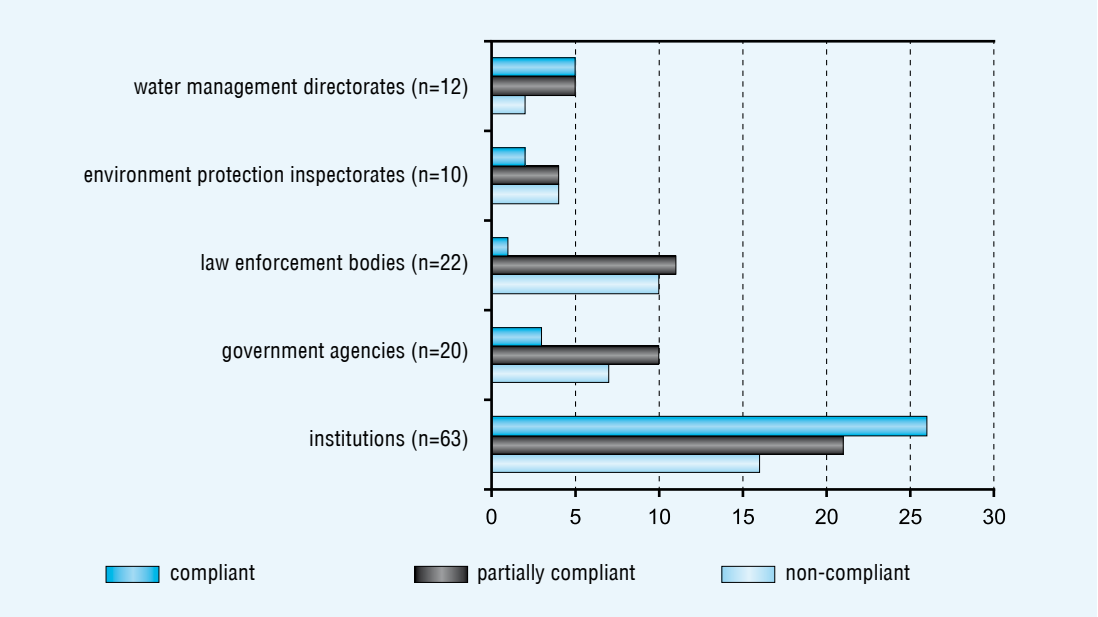
RATING OF RISK MANAGEMENT REGULATIONS
(*N*=127)



Source: Authors' own editing

Chart 6

RATING OF RISK MANAGEMENT
(*N*=127)



Source: Authors' own editing

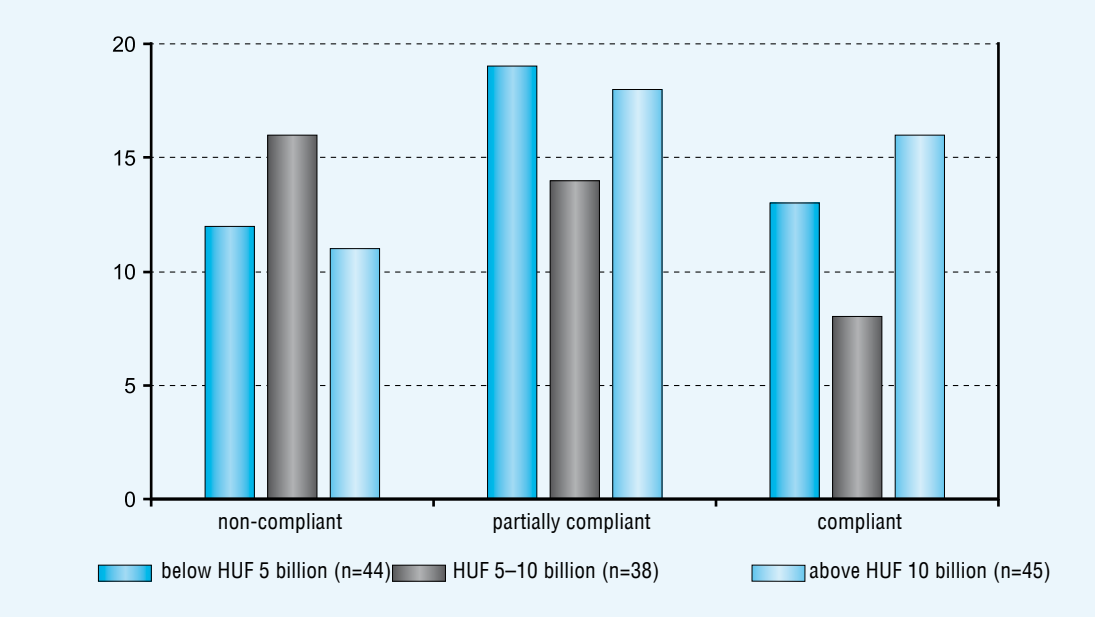
included questions on malpractices related to the operation of the organisations, on irregularities, and on integrity and corruption risks. Three-quarters of the audited entities have drafted general procedural rules for the receipt and investigation of reports about such risks. Close to a half of the government agencies, however, do not have such regulations, and this entails an increased integrity risk having regard to the inherently greater exposure resulting from their responsibilities for administrative enforcement. Almost a half of the organisations (45.7 per cent) assessed fraud and corruption risk as part of risk management, yet only 39.7 per cent of the audited entities developed action plans for corruption prevention based on a survey of integrity risks related to operations.

Based on the institutional documents that were requested during the audit, we also found that the system and process of organisational risk management – required under legal regulations – were not, in many cases, separated from internal auditing activity, which is supposed to be independent. Risks to an organisation's operational processes are often identified and assessed by an internal auditor instead of process owners or the responsible organisation units.

The 30 healthcare institutions that were selected for the audit did essentially develop procedural rules for risk management; a fifth of these organisations, however, failed to assess and analyse the risks associated with their activity, and consequently also failed to manage those risks. There was a regulatory deficiency in one institution, resulting from its failure to update existing regulations with respect to organisational changes. Failure to conduct a review of the risk management process (at least once a year) was a typical deficiency in almost a half of the institutions (43.3 per cent).

Chart 7

RISK MANAGEMENT RATINGS BY ORGANISATIONAL BUDGET
(*N*=127)



Source: Authors' own editing

Risk management in the local government subsystem

Experiences from the integrity survey with local governments

During the 2014 integrity survey, 706 local governments (almost a half of them local governments of villages/large villages) completed the questionnaire, in other words, more than a fifth of all local governments combined. Questions concerned the period between 2011 and 2013. As this research is described in detail by *Szatmári – Kakatics – Szabó* (2014b), only its main results are discussed here.

29 per cent of respondents stated that their organisations performed systemic risk analysis (other than planning internal audit tasks). This ratio corresponds to data for 2013. The ratio is higher with larger organisations; based on self-assessment, 51 per cent of the institutions employing more than 100 people conduct regular risk analysis. Even that is a relatively low proportion with regard to the fact that the statutory obligation also requires local governments to conduct risk analysis as part of the risk management system. Concerning corruption risks, a mere 7 per cent of all respondent organisations carry out the analysis, which corresponds to results from last year's survey.

90 per cent (2013: 85 per cent) of organisations that systematically conduct risk analysis evaluate its results, only one-third (2014: 32 per cent, 2013: 33 per cent), however, manage risks based on the results in every case. 60 per cent of the respondent entities record risk factors identified during risk analysis in a database.

Some three-quarters (72 per cent) of all respondent entities perform regular risk analysis as required by the legal regulations as part of the planning processes of their internal auditing. This value shows improvement relative to results from the previous year (67 per cent).

Overall, it may be argued that based on self-assessment, a much lower than expected percentage of respondents from the local government group engage in activities related to organisational risks that are defined as statutory obligations (risk identification, analysis and assessment, and the adoption of measures). 9 per cent of all respondents engage in risk management regularly, 17 per cent occasionally. These figures show that a greater proportion of larger-size organisations conduct risk management activities.

SAO audits

An analysis of results from audits conducted by the SAO in settlement local governments will provide a general overview of the risk management systems that have been developed in the local government subsystem of public finances.

This analysis was based on SAO audit reports concerning the development of internal control systems, as well as documents that were processed as part of the audits (N=62). During the audits, the SAO examined the regularity of developing internal control systems in settlement local governments. The audited period was 2012. Towns with county status as well as Budapest and its districts were not included among the audited local governments. The sample was selected taking risk criteria into consideration, so results cannot be projected to the entire population. In their examination of the characteristics of the sample, *Benedek – Szenténé – Béres* (2014) found that the number of towns and large villages was greater in the sample, while that of village local governments was smaller, and that the settlements in the sample were also unevenly located in geographical terms.

Questions in the programme part linked to risk management concerned the risk management policy, as well as the identification, analysis and assessment of risks, and the tracking of measures. Audit findings were based on

information from the certificates sent by the audited entities, and from other documents inspected on site. The compliance of developing risk management systems was assessed on the basis of the legal regulations effective in the audited period. Compliance was rated on the work forms containing the audit questions, based on the ratio of the score attained to the total attainable score. The risk management systems could be rated "compliant" (in the case of a result above 81 per cent), "partially compliant" (61–80 per cent), and "non-compliant" (below 60 per cent).

During analysis, the findings of the reports were processed by grouping them according to themes, then aggregating them.

Results

The development of risk management systems was non-compliant in 74 per cent, partially compliant in 15 per cent, and compliant in 11 per cent of the audited settlement local governments. 16 per cent of mayor's offices did not have a risk management policy, which is stipulated in legal regulations and is meant to specify the overall process for managing risks.

An analysis of the deficiencies shows that 37 per cent of the full sample failed to identify and record the external and internal risks inherent to the operation and financial management of mayor's offices. Around a half of the audited entities (53 per cent) did not assess the probability of identified risks occurring; moreover, 48 per cent failed to determine the effect that the risks identified would have on the budgetary institution in case they occurred. Some 73 per cent of mayor's offices did not determine the response measures that would be necessary in connection with the various risk factors depending on the organisation's risk tolerance limit. The method for tracking the implementation of the measures prescribed during risk management was not specified in 87 per cent of the cases.

Where risks were identified, one-quarter of the offices (25 per cent) did not properly assess the probability of risks occurring, and a fifth (18 per cent) their potential impact. Also in this case, more than a half of the audited entities (56 per cent) did not define the measures required to reduce risks below the risk tolerance limit.

Although more than a quarter of the audited local governments (27 per cent) did perform risk analysis and defined the required measures, in 70 percent of such local governments, the tracking of measures and thus the feedback process was not implemented.

Overall, 8 per cent of audited local governments fully discharged the statutory obligations for the development of a risk management system.

CONCLUSIONS

Based on statutory requirements, public entities are subject to the obligation of operating a risk management system as part of the internal control system. This entails the process of identifying risks through their analysis and assessment to instigating measures. Risk management itself, when construed as a response to risks to organisational goals, is the major mechanism of efficient control (INTOSAI GOV 9100). Risk management with the involvement of all stakeholders, when adequately elaborated for detail, also contributes to improving the overall internal control system, and this can be used to reduce the probability of occurrence and/or impact of risk events. This is also the thinking that underlies State Audit Office audits, when it evaluates how the internal control system's elements have been configured.

The SAO's audit and research experience shows that the regulatory background of risk management is indeed provided in organisa-

tions even if deficiencies occur. Internal regulations, however, are often drafted by formally adopting existing templates, without being tailored to the organisation concerned.

Even though they are obliged under statutory requirements to manage risk as part of the risk management system, only 46.8 per cent of the organisations that belong to the central subsystem and participate in the integrity survey do so regularly, while a mere 9 per cent of entities in the local government subsystem do so based on their own judgement. Audit results show that risk management activity is compliant in 29 per cent of audited entities in the central subsystem, and 11 per cent of those in the local government subsystem. Based on audit results, no correlation was found between organisation size and risk management ratings in the case of institutions in the central subsystem. All of this shows that a significant part of public entities do not manage risks consciously, i.e. risk management activity fails to serve its function in such entities.

Being mandatory is the foremost feature of risk management as applied by the public sector, with efforts to minimise risk, and the promotion of compliant operation and financial management serving as the goal. The audits have pointed out that the shortcomings of risk management typically resulted from failure to assess risks and consider possible response measures before executive decisions were made, failure to update regulations, and failure to conduct reviews.

Public entities are in the "learning" stage of the practical application of risk management that expedites and supports the achievement of organisational goals. Appropriate regulation is a necessary but insufficient requirement for effective risk management, as developing risk management "in principle" or formally adopting existing templates will not implement the process itself. For budgetary institutions, the fact is even more significant that substantial losses, which can also be expressed in terms of (public) funds, will occur due to failure to implement risk management measures. This is why the implementation of response measures for managing risks and their effects must be tracked continuously with particular attention, and reviewed as necessary. Based on audit experiences, the revision of risk management processes is also deficient, even though it would afford the opportunity for risk management to achieve its true goal, and not only appear in an organisation's operation as a required element of the internal control system that must be implemented as a rule, but as an organic part and an active tool of management.

It is important to highlight that risk management will only play its role, i.e. will not become a formality or something for its own sake if it is tailored to the particular organisational circumstances and processes; if potential specific steps that mitigate threats impeding or influencing operation, their negative impacts and the probability of their occurrence are considered, then monitored; and any risk occurrences are assessed, along with the effects of implemented measures and those of any that might not have been taken. By itself, risk management does not provide an adequate guarantee for the efficient operation of an organisation, but without it, institutional leadership can at best feel where and what degree of intervention is required for the sake of avoiding harmful consequences. Decisions taken to ensure that the effects assessed in connection with the identification of external and internal risks are kept at the specified level, along with the results of control measures taken to implement them can be considered to be the guarantees of achieving organisational goals efficiently. We need to emphasise that appropriately developed and operated risk management will also pro-

mote the continuous improvement of the overall internal control system itself, thereby organisations will more likely have the capacity to face risks in achieving organisational goals, and thus increase their "resilience" to threats.

Notes

[1] Act CXCV of 2011 on Public Finances

[2] Government Decree 370/2011 (XII. 31.) on the Internal Control System and on the Internal Audit of Central Budgetary Institutions

[3] The scope of Bkr.'s stipulations includes public entities (central budgetary institutions, public bodies (with exceptions), organisations in the local government subsystem, regional development councils and their working organisations, specific asset management organisations and other bodies). After 1 January 2014, the rules applicable to the internal control system of budgetary institutions must also be applied to other organisations belonging to the government sector.

[4] Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies

[5] Government Decree 50/2013 (II. 25.) on the Integrity Management System of Public Administration Bodies and the Order of Receiving Interest Advocates

[6] Act XCIII of 1993 on Labour Safety

[7] Reward may, for example, be understood as the increase of an organisation's prestige, greater social acceptance, more budgetary resources, greater powers, etc.

[8] In the bureaucracy theory of Public Choice, policy-makers and executive officials seek to maximise their personal utility. This theory is presented by *Niskanen* (1971). Among others, *Blais and Dion* (1991) examined Niskanen's fundamental assumptions, and voiced criticism primarily linked to the budget maximising goals of a bureaucratic institution's leader.

[9] An institutional title appears in the central budget's chapters and usually comprises several budgetary institutions that are identical in type or perform similar duties (SAO, 2009). This is why the concept of "institution" will henceforth be understood to mean institutions that form independent titles under the Act on the Budget. This study does not evaluate the internal control systems of chapter-managed appropriations that were audited during the final accounts audit.

Literature

Blais, A. – Dion, St. (1991): The Budget-maximizing bureaucrat: appraisals and evidence. *University of Pittsburgh Press*

Benedek, M. – Szenténé Tubak, K. – Béres, D. (2014): Belső kontrollok a települési önkormányzatoknál (Internal Controls in Local Governments). *Public Finance Quarterly*. 2014/3.

Braunné Fülöp, K. (2010): Szempontok a bizonytalanság és a kockázat értelmezéséhez a PPP-konstrukció példáján (Reflections on the interpretation of uncertainty and risk based on the example of PPP scheme). *Public Finance Quarterly*. 2010/1.

Gajduschek, Gy. (2000): A bürokrácia-fogalom értelmezése a társadalomtudományokban és ennek

jelentősége a közigazgatási szervezetek sajátságainak magyarázatában (Interpreting the Concept of Bureaucracy in Social Sciences, and Its Significance in Explaining the Particularities of Public Administration Entities), PhD thesis, Faculty of Law and Political Sciences, Eötvös Loránd University, Doctoral School of Political Science, Budapest

HM Treasury (2004): The Orange Book – Management of Risk – Principles and Concepts, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Hornai, G. (2001): Kockázat és kockázatkezelés. (Risk and Risk Management.) (MVM Hungarian Electricity Company Disclosures. 2001/04)

Merétey-Vida, Zs. (2004): Belső kontrollrendszer különböző felfogások tükrében (Internal Control Systems in Different Approaches). (Budapest Business School, Faculty of Finance and Accounting, edited version of the paper presented at the conference held on 4–5 November 2004)

Niskanen, W. (1971): *Bureaucracy and Representative Government*. Chicago: Aldine-Atherton

Pulay, Gy. (2014): A korrupció megelőzése a szervezeti integritás megerősítése által (Preventing Corruption by Strengthening Organisational Integrity). *Public Finance Quarterly*, 2014/2.

Szatmári, J. – Kakatics, L. – Szabó, Z. Gy. (2014a): Összefoglaló tanulmány a 2014. évi Integritás felmérés eredményeiről (Summary Study on the Results of the 2014 Integrity Survey). State Audit Office of Hungary, November 2014http://www.asz.hu/tanulmanyok/2014/osszefoglalo-tanulmany-a–2014-evi-integritas-felmeres-eredmenyeirol–1/integritas-tanulmany-benyujtasra.pdf

Szatmári, J. – Kakatics, L. – Szabó, Z. Gy. (2014b): Elemzés a 2014. évi integritás felmérés „helyi önkormányzatok" csoportban mért eredményeiről (Analysis of the Year 2014 Integrity Survey's Results Measured in the "Local Governments" Group). State Audit Office of Hungary, December 2014http://integritas.asz.hu/uploads/files/helyi_%C3%B6nk_elemz%C3%A9s_v%C3%A9gleges.pdf

Vasvári, T. (2015): Kockázat, kockázatészlelés, kockázatkezelés (Risk, Risk Perception, Risk Management). *Public Finance Quarterly*. 2015/1.

State Audit Office of Hungary (2009): Segédlet I. A költségvetési címek pénzügyi (szabályszerűségi) ellenőrzés előkészítéséhez (Field Manual I for Preparing Financial (Regularity) Audits of Budget Titles)

The State Audit Office of Hungary's reports, as well as documents and certificates that corroborate audit findings

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

European Court of Auditors (2012): Financial and Compliance Audit Manual, http://www.eca.europa.eu/Lists/ECADocuments/FCAM_2012/FCAM_2012_EN.pdf

European Court of Auditors (2006): Performance Audit Manual, http://www.eca.europa.eu/Lists/ECADocuments/PERF_AUDIT_MANUAL/PERF_AUDIT_MANUAL_EN.PDF

European Court of Auditors (2013): Risk Assessment in Performance Audits, http://www.eca.europa.eu/Lists/ECADocuments/GUIDELINE_RISK_102013/GUIDELINE_RISK_102013_EN.pdf

Institute of Risk Management (2002): Risk Management Standard, https://www.theirm.org/knowledge-and-resources/risk-management-standards/irms-risk-management-standard/

INTOSAI (2004): INTOSAI GOV 9100 – Guidelines for Internal Control Standards for the Public Sector (2004), http://www.asz.hu/modszertan/iranyelvek-a-belso-kontroll-standardokhoz-a-kozszferaban-intosai-gov–9100/issai–9100.pdf

INTOSAI: INTOSAI GOV 9130 – Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management, http://www.issai.org/media/13341/intosai_gov_9130_e.pdf

ISO Guide 73:2009, linked to the ISO 31000:2009 Risk Management standard

Javaslatok a korrupciós kockázatok kezelésére – Kockázatkezelési és ellenőrzési módszertan (Recommendations for Managing Corruption Risks – A Risk Management and Audit Methodology) (EU Priority Project no. SROP–1.2.4–09–2009–0002 titled Mapping of Corruption Risks – Dissemination of Integrity Driven Public Administration Culture, State Audit Office of Hungary Project Office, 2012)

Ministry for National Economy (2012): A magyarországi államháztartási belső kontrollrendszer bemutatása (The Internal Control System of Hungarian Public Finances), http://ngmszakmaiteruletek.kormany.hu/a-hazai-allamhaztartasi-belso-kontrollrendszer-bemutatasa–2012

Ministry of Finance (2010), Belső Kontroll Kézikönyv (Internal Control Manual) (guide)

Standards Australia (2004): Australian and New Zealand Risk Management Standard AS/NZS 4360:2004.