



Experientia mutua omnibus prodest – Mutual Experience Benefits All

Research paper on risk management in the light of the results of the global survey of 2012

November 2013

INTOSAI SUBCOMMITTEE ON INTERNAL CONTROL STANDARDS

Introduction

The events that the global economy has witnessed over the last decade, economic headwinds, breaking news on turmoil in several countries, fraud and corruption on the part of public servants, and austerity measures undertaken due to budget restrictions – these all demonstrate that more attention should be paid not only to the ultimate effects and outcomes, but also, or even primarily, to the methods that the public administration uses to proceed with uncertainty in the rapidly changing times. From this perspective, the concept of *risk management*, more and more widespread around the globe, seems to provide an improved approach that supports managers and employees in creating the present and the future in line with common expectations. Commonly recognized *advantages* of structured risk management processes include, but are not limited to:

- ✚ increased likelihood of achieving objectives,
- ✚ improved identification of threats and opportunities,
- ✚ improved compliance with relevant legal and regulatory requirements and international norms,
- ✚ improved governance, transparency, confidence and trust,
- ✚ establishment of a reliable basis for decision making and planning,
- ✚ improved controls,
- ✚ improved operational effectiveness and efficiency,
- ✚ effective and efficient service delivery,
- ✚ enhanced health and safety performance, as well as environmental protection,
- ✚ minimized losses incurred by the institution,
- ✚ improved awareness and transparent evaluation and mitigation of risks facing a process,
- ✚ promotion of effective and efficient use of resources.

Going back to the *historical background*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the aftermath of a series of high-profile business scandals and failures, released *ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK* in 2004. In the executive summary COSO, explained that *the underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.*

Operations of the public sector, similarly to those of private organizations, all involve the risks of jeopardizing the achievement of objectives. Due to the general expectation that public servants should be accountable and serve the public interest with fairness and manage public resources properly, the INTOSAI community widely recognizes the concept of enterprise risk management, which has resulted in the development by the Subcommittee on Internal Control Standards of the *GUIDELINES FOR INTERNAL CONTROL STANDARDS FOR THE*

PUBLIC SECTOR – FURTHER INFORMATION ON ENTITY RISK MANAGEMENT (INTOSAI Gov 9130) in 2007. It is necessary to emphasize that INTOSAI GOV 9130 was not intended to replace the *GUIDELINES FOR INTERNAL CONTROL STANDARDS FOR THE PUBLIC SECTOR* (INTOSAI GOV 9100), but it was rather aimed to provide complementary and up-to-date information on risk management.

In 2012, the INTOSAI Subcommittee on Internal Control Standards conducted a global survey among the INTOSAI community. *The aim of the survey* is to provide a general overview on risk management in the public sector. The results of the survey will be used as a background and consideration for updating INTOSAI GOV 9100 and INTOSAI GOV 9130 which will be implemented after 2013. The questionnaire for the survey was developed by the SAI of Austria – the Coordinator for Task 3 of the Action Plan of the Subcommittee on Internal Control Standards, in cooperation with the SAI of Poland – the Subcommittee Chair. To gain necessary information, the questionnaire was sent to all INTOSAI members and it contained questions on:

- ✚ importance of risk management in the public sector (central government),
- ✚ standardization of risk management,
- ✚ implementation of risk management,
- ✚ guidelines on risk management/internal control,
- ✚ promoting risk management and elaborating new INTOSAI guidelines by the Subcommittee on Internal Control Standards,
- ✚ auditing risk management by SAIs.

Answers were received from 62 INTOSAI member SAIs from all over the world, representing the whole INTOSAI community associated in seven regional working groups (45.2% from EUROSAI)¹.

The basics of risk management in the light of the INTOSAI approach

1. The primary concept of risk approach in the public sector is expressed in the *Guidelines for Internal Control Standards for the Public Sector (INTOSAI GOV 9100)* released in 2004. The guidelines refer to the worldwide recognized integrated framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) of 1992. Even though the publication is dedicated to the internal control framework, there is no doubt that dealing with risk is in the center of the recommended approach:

¹ An extrapolation of the results to INTOSAI as a whole is not possible since about two-thirds of the INTOSAI members did not participate in the survey. However, this survey depicts the main trends in risk management. The specific results of the survey are presented on the following pages of this paper by total number and percentage of the returned questionnaires.

- a) as stated in the definition, internal control is a process designed to address risks and to provide reasonable assurance in pursuit of the entity's mission and objectives;
- b) risk is a possibility of an event that may occur and adversely affect the achievement of the objectives;
- c) risk assessment is one of the components of adequately designed and effectively implemented internal control. Risk assessment is described as the process of identifying and analyzing relevant risks to the achievement of the entity's objectives and determining the appropriate response. The whole process consists of successively followed stages: (1) risk identification, (2) risk evaluation, (3) risk significance assessment, (4) response development;
- d) to create adequate, cost-effective and efficient internal control, risk management must be aligned with objective setting processes, and putting into practice specific control activities. Objective setting is a precondition to risk assessment – objectives must be defined before the management can identify risks. On the other hand, internal controls are a response to risk for they are designed to make uncertainty manageable;
- e) the expectations towards risk go far beyond merely financial aspects and objectives; this should be a comprehensive approach and include risk due to external and internal factors considering the organization, entity or department levels;
- f) risk assessment should support objectives being met in a broad perspective, including the area of performing operations, fulfilling accountability, complying with applicable laws and regulations and, last but not least, safeguarding resources against loss, misuse and damage²;
- g) the concept of reasonable assurance inherently embraces risk as the core point of reference for developing, implementing and maintaining internal control systems; reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with certainty;
- h) INTOSAI GOV 9100 indicates that, since governmental, economic, industrial, regulatory and operating conditions are in constant shifts, risk assessment should be an on-going, iterative process performed regularly as a periodical activity rather than a single-ended operation;
- i) because employees are those who make internal control – ergo risk assessment – work, they must know their roles and responsibilities in the field of risk assessment, especially frontline individuals who conduct daily assignments, managers in charge of designing, implementing and supervising internal control systems, and internal auditors responsible for independent and objective assurance and consulting activities;
- j) SAIs and external auditors also play a significant role with regard to risk assessment. They can determine the significance and sensitivity of the risk for which controls are being assessed, on their own evaluate the exposure to misuse of public resources, or a failure to obtain the objectives set. Ultimately,

² Information technology, which has advanced these days, and made organisations increasingly depended on automated systems, appears as another crucial issue when it comes to risk assessment. Although the common application of information technologies in the public sector has not been perceived from the perspective of internal control objectives so far, it is necessary to emphasize that the INTOSAI community is aware of risks in this field and has decided to extend the scope of control activities to include information technology.

depending on the scope of their empowerment, they can assess the adequacy of the control design, testify whether controls put in place are effective, and discuss necessary corrective actions with the auditees.

COSO Enterprise Risk Management

1) The Committee of Sponsoring Organizations of the Treadway Commission released *Enterprise Risk Management – Integrated Framework* (COSO ERM) in 2004³. It was aimed to support entities in the assessment and enhancement of their internal control systems. The intention was not to replace the internal control framework developed in 1992 as *Internal Control – Integrated Framework* (COSO I), but to expand the array of opportunities that entities face in the field of internal control, focusing on the perspective of risk management. An approach demonstrated in COSO ERM is accepted and customized to the specifics of the public sector by INTOSAI in *INTOSAI GOV 9130 Guideline for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management*, developed by the Subcommittee on Internal Control Standards in 2007. As described in INTOSAI GOV 9130, in the public sector the notions of value creation and value preservation do not have as much direct relevance as in the private sector. In this situation, the substitution “service” creation and preservation has been done to make COSO ERM fully applicable to public sector entities. Additionally the term “entity” is used in INTOSAI GOV 9130 instead of “enterprise” which has a private sector association.

The most meaningful issues of COSO ERM are the following:

- a) COSO ERM goes beyond the concept of internal control of 1992 and takes into account the following aspects:
 - ✚ management considers the entity’s risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks,
 - ✚ enterprise/entity risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance,
 - ✚ entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses,
 - ✚ every enterprise/entity faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks,
 - ✚ by considering a full range of potential events, management is positioned to identify and proactively realize opportunities,

³ http://www.coso.org/documents/coso_erm_executivesummary.pdf

- ✚ obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation;
- b) the above issues are reflected in the definition of enterprise risk management which reads that it is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives;
- c) events can have negative impact, positive impact, or both. Events with a negative impact represent risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation;
- d) an innovative approach is demonstrated with regard to objective setting. COSO ERM, in comparison to COSO I, sets forth four groups of objectives, namely strategic, operations, reporting and compliance. High-level goals, aligned with mission or vision, are a new dimension for internal control systems. The mission or vision of an organization appears for management as a starting point in establishing a cascading system of the objectives beginning from strategic objectives and strategy;
- e) instead of the five components of internal control identified in the Internal Control Framework of 1992, COSO ERM consists of eight interrelated components. These components are:
 - ✚ internal environment – the tone of an organization and basis for how risk is viewed and addressed by an entity's people,
 - ✚ objective setting – objectives must exist before management can identify potential events affecting their achievement,
 - ✚ event identification – internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities,
 - ✚ risk assessment – risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent basis and a residual basis,
 - ✚ risk response – management selects risk responses developing a set of actions to align risks with the entity's risk tolerance and risk appetite,
 - ✚ control activities – policies and procedures are established and implemented to help ensure the risk responses are effectively carried out,
 - ✚ information and communication – relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities,
 - ✚ monitoring – the entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through on-going management activities, separate evaluations, or both.

ISO 31000

In November 2009, the International Organization for Standardization (ISO) issued *ISO 31000:2009 Risk management – Principles and guidelines* (ISO 31000)⁴. The standard aims to provide organizations with guidance and a common platform for managing different types of risk in organizations that vary in size, type, complexity, structure, activities and location. One of the objectives of ISO 31000 is to achieve a level of consistency in risk management without the rigid uniformity. ISO also released *ISO Guide 73:2009 Risk management – Vocabulary* to provide a closer explanation with respect to terms and definitions. The advantages of ISO publications are the holistic and practical approach obtained through presenting three interrelated perspectives regarding risk management, namely: critical principles, entire framework and how effective process should be put into practice. The guidelines in the field of risk management developed by the INTOSAI Subcommittee on Internal Control Standards have no reference to the ISO standards, however the survey indicates that standards are applied in the public sector in some countries, so it would be favorable to introduce the INTOSAI community to several main backgrounds.

The most interesting assumptions of ISO 31000 are the following:

- a) the term risk implies an effect of uncertainty on objectives. It must be remembered that an effect may be positive or negative. Objectives can have different aspects and can be applied at different levels of the organization and specific activities. Risk is often expressed in terms of a combination of consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. In turn, risk management is defined as coordinated activities to direct and control an organization with regard to risk;
- b) according to ISO 31000, there are eleven principles which significantly contribute to running risk management in a professional, ordered and systematic manner. These are:
 - ✚ creating and protecting values: in the pursuit of achieving the objectives of the an organization,
 - ✚ being an integral part of the organizational process: so it should be built in the internal structures, processes and procedures, and not separated from them,
 - ✚ being a part of decision making: it helps managers make better decisions to minimize risk and optimize every opportunity,
 - ✚ addressing uncertainty explicitly: inherent on daily basis in every kind of business,
 - ✚ being systematic, structured and timely: it should be planned and controlled like any other kind of activity,
 - ✚ basing on the best available information: it should consider information from a wide spectrum of sources, observation, experience, forecast and experts,
 - ✚ tailoring: to the organization's stakeholders, context and risk profile,

⁴ <http://www.ferma.eu/risk-management/standards/iso-standard/>, <http://www.inconsult.com.au/Articles/ISO%2031000%20Overview.pdf>, http://www.theiaa.org/chapters/pubdocs/99/IIA_Presentation_4_10_12_Final.pdf.

- ✚ taking into account human and cultural factors: it should consider people's skills, capabilities, perceptions, intentions, expectations and cultural elements,
 - ✚ being transparent and inclusive: it includes internal and external stakeholders in the process of development of the context and risk criteria,
 - ✚ being dynamic, iterative and responsive to change: in order to be effective and adequate, it should respond to changes in the internal and external environment,
 - ✚ facilitating continual improvement and enhancement of the organization: by encouraging the organization to be flexible and improve the level of the maturity of risk management processes.
- c) to assist organizations in their endeavor in the field of risk management, ISO 31000 describes the attributes of enhanced risk management, namely:
- ✚ continual improvement,
 - ✚ full accountability for risks,
 - ✚ application of risk management in all decision making,
 - ✚ continual communications,
 - ✚ full integration in the organization's governance structure;
- d) implementation of risk management requires ongoing commitment and must be mandated from the senior and top management. The framework consists of four essential elements. In the first place, designing the framework to manage risk by, among others, defining context, developing policy, assigning resources, designating responsibility, determining information channels and reporting systems. Implementing risk management and rolling out monitoring and reviewing framework are the next steps, with activities such as indicating risk owners, training staff, risk workshops and building risk management as part of operational processes. Whereas risk management is not a one-off project, continual improvement is embedded as an essential driver to bring the theory near to the practice, and to reflect true expectations of the stakeholders;
- e) risk management is a process. For that reason specific and consecutive steps are determined in ISO 31000. The first is establishing the context, i.e. taking into consideration, at the beginning of the process, external and internal factors which influence the organization, such as social, political, economic conditions, as well as the strategy of the organization, its resources and capabilities. While the risk assessment stage is the engine of risk management and consists of (1) risk identification, (2) risk analysis and (3) risk evaluation, risk treatment is a phase when an organization gives a response to risk in a chosen manner. Monitoring and reviewing align with the above steps, and are critical to keeping the risk management process relevant to the needs and expectations of an organization. Because ISO 31000 promotes the consultative team approach, communication and consultation between a risk manager, a risk owner and stakeholders should occur at any time.

Summary – the main observations from the survey

A statistical extrapolation of the survey results would be irrelevant due to the limited number of countries which attended the survey⁵. Still, the survey results allow for summarizing findings and practices, and for formulating several essential conclusions, namely:

- 1.1. The internal environment, the tone at the top, commitment of employees at various levels of an entity, and external stakeholders seem to be critical to establish, maintain, develop and optimize risk management processes. In the light of the survey, the existence of the awareness of the connections between good governance and risk management is rather unequivocal, and consequently the importance of risk management is generally accepted in the public sector. Although the global financial crisis de facto is not the starting point for the increased engagement in this field, it probably, to some extent, causes the acceleration of the process of seeking for new tools for improving the state of public affairs.
- 1.2. The engine of the concept is the term “risk” itself, commonly agreed and applied globally in the public sector. It could be natural and understandable, in some sense, that the term “risk” in many languages, cultures and societies has mainly negative connotations, because for many it is very close to the term “hazard”. This “pessimistic” approach, as a result, disregards the fact that many recognized settlers of risk management standards promote a wider approach when it comes to “risk” that encourages to look at the other side of a coin – potential opportunities. The attitude confined towards risk may jeopardize the relevance and the effectiveness of the risk management process, by making it reactive instead of proactive, and may hamper continual improvement and performance optimization. Anyway the clear explanation of the term “risk” appears as a topic for further discussion amongst the INTOSAI community.
- 1.3. Standardization is the essence of further development and a platform for exchanging different perspectives and experience. For the majority of countries, guidelines such as INTOSAI GOVs and standards such as COSO ERM and ISO 31000 are recognized and commonly accepted, there are, however, a visible number of countries where national risk management and internal control guidelines are not based on these guidelines and standards. Importantly, COSO ERM is the point of reference for guidelines established in the public sector on one hand, while external assessment carried out by SAIs is predominantly based on INTOSAI GOVs on the other.
- 1.4. Risk management should be a systematic, documented, repeatable, and continually developed process to demonstrate a high level of excellence and professionalism. Generally, as it follows from the survey, the importance of risk management is usually reflected formally, in various manners though, and the requirements are derived mainly from guidance and sometimes even from legal obligations. The survey

⁵ See footnote 1.

indicates that the attitude towards the definition of risk management varies from country to country. Moreover risk management is not always regarded as a systematic, structured and formalized system, and the lack or insufficient advancement of critical elements, such as internal environment, objective setting, event identification, risk response, information and communication, or monitoring procedures, were displayed by many countries. Risk management is developed as a structured process mainly in most advanced public entities rather than in the public sector as a whole, which may testify to limitations of public entities' resources, such as knowledge, skills, experience or practical guidance on the implementation of risk management processes.

- 1.5. The capability of public entities to conduct risk assessment with respect to the likelihood and impact of the most influential kinds of risk requires some improvement and additional support. Such kinds of risk as missed opportunities, sustainability risks and political risks are still a serious challenge in many countries, and there is some room for improvement in the field of corruption risk. However human factor proves to be critical for ensuring the effectiveness of the risk management processes – this is people who makes risk management operate – the survey shows that in practice training is usually provided to a limited number of employees only – usually a few experts from an organization are trained rather than the majority of employees.
- 1.6. Although SAIs develop guidelines and procedures for external evaluation of risk management, there is a problem with assessing the maturity level of risk management.
- 1.7. In the light of SAIs' expectations, the current INTOSAI guidelines on risk management seem to be a little bit theoretical. A strong need for a more practical approach has appeared. When elaborating new guidelines on risk management, the Subcommittee on Internal Control Standards intends to apply a hands-on approach, accompanied with operative tools development. The question of combining, to a justified extent, of COSO ERM with ISO 31000 seems to call for an in-depth discussion among the Subcommittee members while reviewing INTOSAI 9130 towards a more practical approach. To that end, transfer of knowledge in different forms from more advanced countries will be welcomed. An applicable maturity model for risk management aligned with internal assessment and external audit tools appears as a common need.
- 1.8. It is noticeable that in the public sector in general, formal processes of risk management have not been established. It may mean that INTOSAI GOVs are not commonly used and that SAIs should promote them more actively.

Findings and practices in the light of the results of the 2012 survey

1. Importance of risk management in the public sector (central government)

- 1.1. The large majority (nearly 80 percent) of the countries declare the importance of risk, and the necessity for risk management is generally acknowledged in the public sector (central government). What is more, risk management is widely considered as an essential part of good public governance. Consequently, a link between risk management and good governance has been reflected in public policies (e.g. in relevant strategic documents) by all accounts.
- 1.2. The results of the survey indicate that the awareness and concrete efforts towards risk management sharply increased since the beginning of the Global Financial Crisis in 2008. This perspective has led to an approach where financial risks and corruption are a predominant consideration. However, it is noticeable that strategic and operational risks have been regarded as important to manage. Interestingly, although public sector entities operate in a strongly politically tailored environment, barely half of the respondents acknowledge taking political risks into account while establishing risk management processes.
- 1.3. Even though the recognized international standards and guidelines on risk management released by INTOSAI and other parties confirm that risk can be perceived as both a negative and a positive event, only few countries claim that they make allowance for missed opportunities as a risk factor in their analysis.

2. Standardization of risk management

- 2.1. In most of the countries surveyed, there are some legal requirements or other obligations, such as regulations, policies or best practices, for the implementation of risk management in the public sector (central government). The application of guidelines is the most popular approach. Less than one-third of the respondents confirm the existence of legal requirements on risk management.
- 2.2. A clear definition of risk management is provided in less than one-third of the countries surveyed, and in more than 50 percent of responses a description of important elements of risk management is included in legal provisions, regulations and guidelines. In some cases risk management is defined with the use of examples.
- 2.3. A formalized system of risk management (e.g. standards, formalized procedures, reporting requirements, etc.) for the public sector (central government) does not exist in a significant number of countries and in

one-third of those surveyed only partial formalization has been put in place. As a result, merely one-fifth of those surveyed confirm the existence of a systematic attitude towards risk management.

- 2.4. Approximately two-thirds of those surveyed confirm, in a determined manner, that all spectrum of the management components (internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, monitoring) were covered by the standards and procedures.
- 2.5. Some disparities are visible and worth emphasizing, for example:
- a) about 10 percent of the countries miss the opportunity for developing standards and procedures on internal environment that, in accordance with INTOSAI GOVs framework, form the background for the implementation of risk management processes,
 - b) risk assessment is declared to be established by all countries (fully or partially), whereas objective setting and event identification are at a remarkably lower level (about one-fifth of the respondents indicate that there are no standards or procedures developed in these areas at all),
 - c) control activities are developed widely when such components of risk management as risk response and monitoring are less advanced. It is noticeable that about 28 percent of the responding countries partially or totally lack the risk response approach,
 - d) the information and communication component is the least developed and seems to be underestimated when rolling out risk management approach in public organizations. More than ten percent of the responding countries lack standards and procedures in this area, while 15 percent of the respondents declare that standards and procedures have been partially developed.

3. Implementation of risk management

- 3.1. Risk management, understood as a structured process for identifying and monitoring of emerging risks, has already been developed within the central government, self-governments and public enterprises mainly in more advanced entities of the public sector (36 percent, 26 percent and 38 percent respectively). At the national government, local government and public enterprise level correspondingly as many as 17 percent, 31 percent and 11 percent of the countries surveyed demonstrate that formal processes of risk management have not been established.
- 3.2. In the light of the survey results the profound or partial decentralization prevails when it comes to the organization (e.g. coordination, guidelines, summary of results, consolidated reporting) of risk management processes from the system perspective.
- 3.3. Risk management and internal control systems in the central government are usually considered and organized, to some extent, as integrated networks (widely in 23 percent and partly in 46 percent of the responding countries).

- 3.4. The current level of the ability of the public administration to identify and assess the likelihood and impact of the most influential kinds of risk is mostly declared as at the medium stage in the whole spectrum. Identification and assessment of risk tailored to missed opportunities, sustainability risk and political risk seems to be the most problematic: almost 80 percent, 55 percent and 50 percent of those surveyed declare a low ability or the lack of ability in these areas respectively. On the other hand, there is a comparatively high percentage of countries with an ability as regards financial and operational risk. Still, in this area medium skills also prevail among public entities. Attention should be paid to the fact that about 38 percent of the respondents admit low or no competence in identifying and assessing corruption risk in the public sector.
- 3.5. Weaknesses in risk identification and risk evaluation are identified by SAIs as the most common problem in respect of risk management in their countries (above a half of the responses).
- 3.6. Excellent training facilities are declared only by one respondent, and good training facilities by two responding countries. On the other end of the scale, the obvious lack of training was displayed by almost one-third of the countries surveyed. The prevailing tendency is training available only for few experts from an organization.

4. Guidelines on risk management and/or internal control

- 4.1. Formal national risk management and internal control guidelines for the public sector (central government) exist in about 40 percent of the countries that responded to the survey, and in 30 percent guidelines have been developed for internal control only. Almost 25 percent of the countries, according to the responding SAIs, have neither risk management nor internal control guidelines elaborated.
- 4.2. National guidelines for the public sector (central government) are mostly set up as obligatory regulations and refer to widely recognized international standards, such as INTOSAI guidelines, the COSO ERM framework or ISO 31000. Frequently, a code of ethics or a code of conduct is included as part of national regulations.
- 4.3. Surprisingly, the COSO ERM framework is more widespread in the public sector than INTOSAI GOVs. Still, some 30 percent of the responding countries do not have any reference to international standards.
- 4.4. The level of integration of guidelines on risk management with those on internal control is more or less balanced (in 23 percent of the responding countries it is assessed as widely integrated, in 25 percent as partly integrated, and in 23 percent as widely separated). There are also cases where the concepts of risk management and internal control are completely integrated (14 percent) and totally separated (16 percent).

5. Risk management from the perspective of SAIs

- 5.1. While more than a half of SAIs have developed guidelines and procedures for assessing risk or evaluating risk management in the public sector, there is room for improvement. The most advanced is the area of financial audit, where about 70 percent of offices have put in place a formal approach for preparing guidelines and procedures. The least advanced is the area of performance auditing, with almost 45 percent of negative answers. A similar situation is observed when we analyze the layout of the audits conducted by SAIs with regard to risk management in the public sector. External risk assessments made within financial audits are a common practice among 64 percent of the respondents. As for compliance audits, this percentage stands at 55, and as for performance audits – at 46.
- 5.2. Predominantly risk management assessment is part of an overall audit of an organization, which is demonstrated by 85 percent of the SAIs surveyed.
- 5.3. Although COSO ERM is most frequently the point of reference for guidelines established in the public sector, external assessment carried out by SAIs is predominantly based on INTOSAI GOVs (64 percent of the answers received) and then on the COSO ERM framework (36 percent). In 15 percent of the countries surveyed, risk assessments are conducted with no reference to recognized standards.
- 5.4. Findings from SAIs' reports indicate that weaknesses in risk evaluation and risk identification are the main problem in the public sector. The lack of implementation of risk management at all is also a considerable weakness. From the perspective of SAIs, most of their countries have not established mature⁶ and satisfying risk management processes.
- 5.5. In the case of 43 percent of the respondents it was difficult to assess if the level of risk management is mature or immature, satisfactory or unsatisfactory. While in 28 percent it was somewhat immature or mostly unsatisfactory. Ultimately, with regard to 6 percent of the responding countries, the levels are considered very immature or very unsatisfactory.

6. Promoting risk management and elaborating new INTOSAI guidelines – SAIs' expectations

- 6.1. The SAIs surveyed indicate the following issues to be the most important and beneficial in respect of future activities of the INTOSAI Subcommittee on Internal Control Standards:
- implementation guidelines,
 - best practices,
 - examples of other countries' experience,

⁶ The following stages used in COSO's 2010 report on the ERM framework, available from www.coso.org, could provide an orientation:

- systematic, robust and repeatable process with regular reporting of aggregate top risk exposures,
- documented and monitored process with periodical reporting of aggregate top risk exposures,
- mostly informal and unstructured, with ad hoc reporting of aggregate top risk exposures,
- mostly track risks by individual silos of risk, with minimal reporting of aggregate top risk exposures,
- there is no structured process for identifying and reporting top risk exposures.

- a maturity model,
- modern and updated guidelines for risk management,
- assessment tools,
- audit tools,
- minimum standards for the implementation of risk management.

6.2. The following issues, according to SAIs, should be focused on when developing new or restructuring the existing INTOSAI guidelines on risk management:

- implementation guidelines,
- maturity models,
- best practices,
- assessment tools,
- auditing procedure of risk management systems,
- practical application,
- a small country perspective,
- gradual implementation (step by step),
- different methods and/or assessment tools for public entities of different size,
- role of management in risk management and internal audit,
- structure of risk management in an organization and its relationship with internal audit,
- risk management mechanisms,
- capacity building of SAIs on risk management framework,
- SAIs' review of risk management.

6.3. Although many SAIs express the opinion that guidelines should only be based on the COSO Integrated Enterprise Risk Management framework, a significant number of countries (55 percent) claim that other standards should be also considered, especially ISO 31000 Risk management – Principles and guidelines and ISO Guide 73 Risk management – Vocabulary.

6.4. The development and further elaboration of a maturity model for risk management (e.g. similar to the COBIT maturity model⁷ with specific criteria for the public sector) is considered as a very sensible approach by almost 75 percent of those surveyed. Although support for developing a standardized certification process for internal control and/or risk management is demonstrated by some 63 percent of SAIs, the rest is of the opinion that continuous monitoring of the internal control system is more important than a certificate, questioning the necessity for certification and its usefulness.

⁷ The COBIT maturity model describes six different levels of maturity for IT processes: 0 Non-existent; 1 Initial/Ad Hoc; 2 Repeatable but intuitive; 3 Defined Process; 4 Managed and Measurable; 5 Optimised. See www.isaca.org for further information.

The results of the survey in figures

REPRESENTATION OF INTOSAI REGIONAL WORKING GROUPS IN THE SURVEY

	EUROSAI	ASOSAI	ARABOSAI	OLACEFS	AFROSAI	CAROSAI	PASAI
Total of returned questionnaires ⁸	28	20	8	6	10	1	1
% of Regional Group members	56.0	43.5	36.4	25.0	19.6	4.8	3.8
% of returned questionnaires	45.2	32.3	12.9	9.7	16.1	1.6	1.6

QUESTIONS

SECTION 1: IMPORTANCE OF RISK MANAGEMENT IN THE PUBLIC SECTOR (CENTRAL GOVERNMENT) IN YOUR COUNTRY

1. Is the importance of risk and necessity for risk management commonly acknowledged in the public sector (central government)?

	commonly acknowledged	widely acknowledged	partly acknowledged	only selectively acknowledged (e.g. financial risks)	not acknowledged at all
Total of returned answers (61) ⁹	14	20	14	10	3
% of returned answers	23.0	32.8	23.0	16.4	4.9

Comments: *Although risk management may be acknowledged, proactive steps are not taken for risk management at the governmental level.*

2. Have awareness and concrete efforts towards risk management increased or decreased in the public sector (central government) since the beginning of the Global Financial Crisis in 2008?

	very much increased	increased	neither increased nor decreased	decreased	very much decreased
Total of returned answers (60)	3	36	21	0	0
% of returned answers	5.0	60.0	35.0	0.0	0.0

Comments: *A number of public sector entities have undertaken serious efforts to improve risk management since 2008.*

⁸ Twelve INTOSAI member SAIs belong to two regional working groups, so the total percentage of the returned questionnaires exceeds 100.

⁹ In the survey, 62 SAIs participated, still every time the results were related to the number of the answers provided for a given question. In some cases answers were not provided, because at the responding SAIs the required information is not collected or unavailable. The number of the SAIs that responded to a given question is provided in brackets.

3. What kinds of risks are primarily taken into account with established risk management in public administration (central government)?

Kind of risk ¹⁰	Total of returned questionnaires		% of returned questionnaires	
	yes	No	yes	no
Financial risks (57)	51	6	89.5	10.5
Political risks (53)	27	26	50.9	49.1
Strategic risks (55)	41	14	74.5	25.5
Operational risks (56)	46	10	82.1	17.9
Property/casualty/hazard risks (52)	31	21	59.6	40.4
Health/safety risks (51)	30	21	58.8	41.2
Sustainability risks (51)	28	23	54.9	45.1
Corruption (55)	44	11	80.0	20.0
Missed opportunities (52)	12	40	23.1	76.9

Comments: *The following risks have also been indicated as taken into account with established risk management in the public sector: environmental risk, information technology risk, economical risk, technological risk, legal risk, managerial risk, reputation risk, partners risk, disaster risk, ethics risk, security risk, personnel risk, etc.*

4. Is risk management considered to be an essential part of good public governance?

	Yes	No
Total of returned answers (61)	52	9
% of returned answers	85.2	14.8

5. Is a link between risk management and good governance reflected in the public policies (e.g. in relevant strategic documents) at the central government level?

	regularly	mostly	in some policies or recent documents	only very rarely	not at all
Total of returned answers (61)	3	14	31	9	4
% of returned answers	4.9	23.0	50.8	14.8	6.6

Comments: *Risk management is still a fairly new concept in central government.*

¹⁰ In INTOSAI GOV 9130 *Further Information on Entity Risk Management*, Figure 1, some typical risks of government entities are listed.

SECTION 2: STANDARDIZATION OF RISK MANAGEMENT IN YOUR COUNTRY

6. Is there a legal requirement or another kind of obligation (e.g. regulation, guideline, etc.) for the implementation of risk management in the public sector (central government)? (*more than one answer possible*)

	legal obligation	regulation	other kind of obligation	guideline	no obligation
Total of returned answers (60)	17	18	5	22	14
% of returned answers	28.3	30.0	8.3	36.7	23.3

7. Do these documents provide a clear definition or description of risk management? (*more than one answer possible*)

	formal definition	description of important elements	description by examples	no definition or description
Total of returned answers ¹¹ (46)	14	27	8	6
% of returned answers	30.4	58.7	17.4	13.0

8. Is there a formalized system of risk management (e.g. standards, formalized procedures, reporting requirements, etc.) for the public sector (central government)?

	yes	no	partially
Total of returned answers (59)	14	26	19
% of returned answers	23.7	44.1	32.2

9. What components of risk management are covered by these formal standards, procedures, etc.?

Components of Risk Management	Total of returned answers ¹²			% of returned answers		
	Yes	no	partially	yes	no	partially
Internal Environment (32)	22	3	7	68.8	9.4	21.9
Objective Setting (33)	25	6	2	75.8	18.2	6.1
Event Identification (32)	19	7	6	59.4	21.9	18.8
Risk Assessment (33)	28	0	5	84.8	0.0	15.2
Risk Response (32)	23	5	4	71.9	15.6	12.5
Control Activities (32)	26	4	2	81.3	12.5	6.3
Information and Communication (33)	24	4	5	72.7	12.1	15.2
Monitoring (32)	23	3	6	71.9	9.4	18.8

¹¹ As for question No 6, 46 SAIs answered that there is some sort of obligation (e.g. a regulation, a guideline, etc.) for implementation of risk management in the public sector. So when analyzing the results for question No 7, only those answers have been considered that confirm that such an obligation exists.

¹² As for question No 8, 33 SAIs replied that there exists or partially exists a formalized system of risk management (e.g. standards, formalized procedures, reporting requirements, etc.) for the public sector. When analyzing the results for question No 9, only those answers have been considered that confirm that such a system exists.

SECTION 3: IMPLEMENTATION OF RISK MANAGEMENT IN YOUR COUNTRY

10. Has risk management as a structured process for identifying and monitoring emerging risks already become a standard or a wide spread practical exercise in the Public Sector?

a) within central government (federal/state government)

	standard	wide spread practical exercise	in most advanced entities	only few examples	not established
Total of returned answers (59)	6	7	21	15	10
% of returned answers	10.2	11.9	35.6	25.4	16.9

b) within self-government (local government) administration¹³

	standard	wide spread practical exercise	in most advanced entities	only few examples	not established
Total of returned answers (55)	3	6	14	15	17
% of returned answers	5.5	10.9	25.5	27.3	30.9

c) within public enterprises¹⁴

	standard	wide spread practical exercise	in most advanced entities	only few examples	not established
Total of returned answers (56)	8	9	21	12	6
% of returned answers	14.3	16.1	37.5	21.4	10.7

11. Is risk management in central government organized as a more centralized (e.g. coordination, guidelines, summary of results, consolidated reporting by the ministry of Finance) or decentralized process?

	completely centralized	widely centralized	partly centralized/ partly decentralized	widely decentralized	completely decentralized
Total of returned answers (51)	5	5	15	21	5
% of returned answers	9.8	9.8	29.4	41.2	9.8

¹³ Some of the responding SAIs do not have a legal mandate to audit self-government entities, so the answer has not been given.

¹⁴ Some of the responding SAIs do not have a legal mandate to audit public enterprises, so the answer has not been given.

12. Are risk management and internal control system in central government considered and organized more separate (different systems, guidelines, processes and owners) or more integrated?

	completely integrated	widely integrated	partly integrated	widely separated	completely separated
Total of returned answers (52)	5	12	24	7	4
% of returned answers	9.6	23.1	46.2	13.5	7.7

13. What is the current level of ability of the public administration/sector to identify and to assess the likelihood and impact of the following kinds of risks?

Kind of risk	Total of returned answers				% of returned answers			
	high	medium	low	no or low ability	high	medium	low	no or low ability
Financial risk (54)	18	27	7	2	33.3	50.0	13.0	3.7
Political risk (54)	7	20	16	11	13.0	37.0	29.6	20.4
Strategic risk (54)	8	31	9	6	14.8	57.4	16.7	11.1
Operational risks (54)	15	26	10	4	27.3	47.3	18.2	7.3
Property/casualty/hazard risk (51)	8	21	14	8	15.7	41.2	27.5	15.7
Health/safety risk (52)	10	22	13	7	19.2	42.3	25.0	13.5
Sustainability risk (54)	1	23	18	12	1.9	42.6	33.3	22.2
Corruption (53)	9	24	16	4	17.0	45.3	30.2	7.5
Missed opportunities (54)	1	10	21	22	1.9	18.5	38.9	40.7

14. Are the provided risk management training facilities for civil servants satisfactory?

	excellent training facilities	good training facilities	sufficient training facilities	training only for few experts	obvious lack of training
Total of returned answers (57)	1	2	11	24	19
% of returned answers	1.8	3.5	19.3	42.1	33.3

Comments: *Training is not a problem as long as there is no clear policy for promoting risk management.*

SECTION 4: GUIDELINES ON RISK MANAGEMENT AND/OR INTERNAL CONTROL

15. Do formal national risk management or/and internal control guidelines for the Public Sector (central government) exist in your country?

	risk management and internal control guidelines exist	guidelines only for risk management	guidelines only for internal control	neither risk management nor internal control guidelines
Total of returned answers (59)	24	3	18	14
% of returned answers	40.7	5.1	30.5	23.7

If there are no guidelines skip questions 17 to 20¹⁵ and go to question 21.

16. If there are national guidelines for the Public Sector (central government), are they used?

	obligatory	voluntarily
Total of returned answers (43)	29	14
% of returned answers	67.4	32.6

17. Do these guidelines refer to international standards (e.g. INTOSAI Guidelines, COSO ERM framework, ISO 31000, other)?

	yes	no
Total of returned answers (43)	31	12
% of returned answers	72.1	27.9

18. Do these guidelines integrate risk management and internal control or are risk management and internal control guidelines separated?

	completely integrated	widely integrated	partly integrated	widely separated	completely separated
Total of returned answers (44)	6	10	11	10	7
% of returned answers	13.6	22.7	25.0	22.7	15.9

¹⁵ As for question No 15, 45 SAIs replied that formal national risk management or/and internal control guidelines for the public sector exist in their countries. So when analysing the results for questions 16-19 only those replies have been considered that confirm the existence of any guidelines.

19. Do these guidelines refer to international standards? (*more than one answer possible*)

	INTOSAI Guidelines	COSO ERM framework	ISO 31000	other	no reference
Total of returned answers (43)	14	18	3	8	13
% of returned answers	32.6	41.9	7.0	18.6	30.2

Comments: *The following standards have also been indicated: AS/NZS 4360:2004, FERMA Standards, COCO, IIA Standards.*

20. Do national guidelines or other national regulations include a Code of Ethics or a Code of Conduct?:

	yes	No
Total of returned answers (56)	39	17
% of returned answers	69.6	30.4

SECTION 5: PROMOTING RISK MANAGEMENT AND ELABORATING NEW INTOSAI GUIDELINES BY THE SUBCOMMITTEE

21. What are the most interesting and important aspects or needs of INTOSAI member countries in respect of future activities of the Subcommittee (e.g. implementation guidelines, best practices, assessment tools, maturity models, etc.)?

The responding SAIs indicate the following issues to be the most important and beneficial in respect of future activities of the ICS Subcommittee:

- implementation guidelines,
- best practices,
- examples of other countries experience,
- maturity model,
- modern and updated guidelines for risk management
- assessment tools,
- audit tools,
- minimum standards for the implementation of risk management.

Other comments:

- *Emphasis on building risk culture and highlighting the significant outcomes of risk management.*
- *Implementation guidelines containing practical notes on recommended assessment criteria and tools, most often used maturity models and examples of best practices in the public sector and SAIs experience.*
- *Management of the political risk – how it should be performed.*
- *What are the most typical risks and specific risk areas in the public sector?*

- *What are the specific features of risk management in the public sector?*
- *Dissemination of already existing assessment tools and maturity models would be useful*
- *Development of a risk management framework, including risk management policies and strategies.*
- *We consider the risk management systems of long term sustainability issues to be of utmost importance. Therefore, it would be useful to evaluate the need to adjust and develop the guidelines and best practices in this field. It would be also useful to give guidance how to combine risk management at an entity level (e.g. individual government agency) with a broader whole of government level risk management.*
- *Another important issue is the capacity of the risk management systems to cover the systemic risk caused by exogenous, stochastic and unpredictable events, even in the cases where these are considered as highly improbable. Also here, it would be useful to evaluate the need to develop best practices.*
- *Very significant risk management issue for the public sector are the ICT-project management and risk management in ICT-projects. Guidance is needed on (a) how to combine ICT-standards and best practices in ICT-project management to overall entity risk management, and (b) in particular on how to combine ICT-risk management and ICT-project risk management with systems for managing performance and operational risks in the public sector.*
- *With attention for the cost/benefit aspects.*
- *Customized models.*
- *Forms used in evaluating risks and their methodology.*
- *Studies that may help risk management officials in developing risks management systems.*
- *Highlighting various experience and expertise in risk management.*
- *Elaborate guidelines to promote risk management in countries where it does not exist.*

22. When developing new or restructuring existing INTOSAI guidelines on risk management what should be the focus and the most important issues of these new guidelines?

The responding SAIs indicate that the following issues should be focused on when developing new or restructuring the existing INTOSAI guidelines on risk management:

- implementation guidelines,
- maturity models,
- best practices,
- assessment tools,
- auditing procedure of risk management systems,
- practical application,
- a small country perspective,
- gradual implementation (step by step),

- different methods and/or assessment tools for public entities of different size,
- role of management in risk management and internal audit,
- structure of risk management in an organization and its relationship with internal audit,
- risk management mechanisms,
- capacity building of SAI on risk management framework,
- SAIs review of risk management.

Other comments:

- *The new guidelines should be clear on the scope of risk management, tools on risk assessment, communication and reporting, as well as best practices of risk management.*
- *How to implement the concept of risk management?*
- *Explain and demonstrate by examples.*
- *How to create atmosphere in the project of risk management?*
- *How to set mitigation measures?*
- *How to engage the right project team?*
- *Additional guidelines on the key elements that entities should consider for creating a foundation to effectively manage risk.*
- *The focus should be on risk evaluation and risk response. Practical examples or best practices would be very useful.*
- *More examples from practice in different countries and, if possible, some recommendation on which assessment tools and maturity models are best to be applied in the public sector.*
- *To promote good practices of risk management systems in the public sector.*
- *The guidelines should be practical and should follow international best practice and be public sector specific.*
- *System of risk management.*
- *How to integrate risks of different areas into one common or general risk management?*
- *Elaborate on the prerequisite in terms of training.*
- *Improve operational effectiveness and efficiency of audit tools on risk management.*
- *Criteria about when/where risk management should or should not be used is a key issue.*
- *Assurance of the risk management process.*
- *Assessing the quality of risk management documentation.*
- *How to develop a risk management framework including implementation guidelines?*
- *How to develop and implement risk assessment tools and agree action on the risk identified?*
- *The identification of best practices with respect to risk management.*
- *Very recent risks related to the global financial crisis and corporate governance.*
- *Detail guidelines on assessment of the likelihood and impact of different kinds of risk.*
- *Development of a “core model” for risk management in the public sector should be a priority.*

- *Development of INTOSAI guidelines on risk management should be based on international standards.*
- *The main focus should be to include the systemic risk concept in the framework of the public risk management guidelines. Due to the increasing global integration, governments and public entities depend on global processes. These are often outside their sphere of influence and difficult to predict, but their occurrence might have severe impact on governments' operations.*
- *Another main focus should be the combination of ICT risk management to the overall internal control and risk management system, and the construction of a whole-of-government risk management system in which various entities and policy level risk management systems have a clear and defined role.*
- *Risk management should be integrated with the management control cycle.*
- *The verification of the real effectiveness of guidelines by indicating good practice examples.*
- *Risk management has to be understood as a top-management duty.*
- *Focus on how to transform the abstract concepts within the guidelines to concrete audit practice for the benefit of operational auditors.*
- *Focus on assessing the risk management process by SAI auditors (the link between the existing risk management process in the audited entity and the audit risk – inherent risk, control risk and detection risk).*
- *Backing of risk management in legislation and internal audit charter.*
- *Reporting format on risk management by internal audit and external audit.*
- *IT-governance.*
- *Risk of material misstatements in public accounts, political risk and objective setting.*
- *Usage of risks management evaluation results.*
- *Methods used in studying, fighting and declining every kind of those risks.*
- *The tool or evaluation must be conducted in the same standard.*
- *Each process should have the practical report format.*
- *Risk management practical methods with focus on concrete issues of risk management in connection with internal audit.*
- *The components of risk management and the coordination of various risk assessments by different sections of the central government.*
- *Establishment of effective and efficient methodologies of assessing risk management in public sector entities.*
- *Guidelines that will be relevant to risk management challenges faced by public sector entities, taking into account the vast technological advancements that have taken place in recent years. In other words, the need for guidelines that will move with the current time.*

23. Should risk management guidelines for the Public Sector be harmonized with private sector guidelines?

	completely harmonized with private sector	partly adopted to public sector specifics	adopted to public sector specifics	strongly adopted to public sector specifics	separate and specific guidelines for public sector
Total of returned answers (61)	2	19	19	7	14
% of returned answers	3.3	31.1	31.1	11.5	23.0

Comments: *Risks vary so specifics of the public sector should be absolutely taken into consideration.*

24. Should these guidelines only be based on COSO's integrated Enterprise Risk Management framework or should also other standards (especially ISO 31000 Risk management – Principles and guidelines, ISO Guide 73 Risk management - Vocabulary) be integrated? (*more than one answer possible*)

	only COSO ERM	ISO 31000/ Guide 73	other standards
Total of returned answers (58)	20	32	11
% of returned answers	34.5	55.2	19.0

Comments:

- *Those standards are too complex for the current level of risk management*
- *All available best practices should be referenced*
- *All available standards should be taken into consideration and adapted to the public sector*
- *The following standards have been indicated: FERMA standard, IEC/ISO 31010:2009, etc.*

25. Is the development and further elaboration of a maturity model for risk management (e.g. similar to the COBIT maturity model¹⁶; with specific criteria for the Public Sector) considered a sensible approach?

	very sensible	sensible	neither sensible nor insensible	insensible	very insensible
Total of returned answers (58)	9	40	6	2	1
% of returned answers	15.5	69.0	10.3	3.4	1.7

26. Should internal control and/or risk management be incorporated into a standardized certification process (e.g. ISO certification)?

	yes (as part of quality management)	yes (as a separate certification standard)	No
Total of returned answers (59)	27	10	22
% of returned answers	45.8	16.9	37.3

Comments:

- *Certification cannot be an "end in itself".*
- *The continuous monitoring of internal control systems is more important than a certificate.*

¹⁶ See footnote 7.

- Certification is not necessary. Very doubtful about its usefulness.

SECTION 6: RISK MANAGEMENT AUDIT BY YOUR SAI

27. Has your SAI established guidelines and procedures for assessing risk or evaluating risk management in the public sector? (e.g. in auditing standards, auditing manuals, etc.)?

Type of audit	Total of returned answers		% of returned answers	
	yes	no	Yes	No
for financial audit (53)	37	16	69.8	30.2
for compliance audit (48)	27	21	56.3	43.8
for performance audit (47)	26	21	55.3	44.7

28. Has your SAI conducted audits of risk management in the public sector?

Type of audit	Total of returned answers		% of returned answers	
	yes	no	Yes	No
for financial audit (53)	34	19	64.2	35.8
for compliance audit (50)	28	23	54.9	45.1
for performance audit (51)	27	23	54.0	46.0

29. Was the assessment of risk management the explicit subject of the audit or was it part of an overall audit of an organization, entity or broader subject?

	RM explicit audit subject	RM part of an overall audit	Both
Total of returned answers (47)	1	40	6
% of returned answers	2.1	85.1	12.8

30. Was the assessment based on a specific standard on risk management? (*more than one answer possible*)

	INTOSAI Guidelines	COSO ERM framework	ISO 31000	other	no reference to a standard
Total of returned answers (47)	30	17	2	10	7
% of returned answers	63.8	36.2	4.3	21.3	14.9

Comments: *The following standards have also been indicated: FERMA Standard, ISA, etc.*

31. What were the main findings and weaknesses in respect of risk management? (*more than one answer possible*)

	missing implementation of risk management	no standardization of risk management	weaknesses in risk identification	weaknesses in risk evaluation	weaknesses in risk reaction
Total of returned answers (47)	25	22	24	26	20
% of returned answers	53.2	46.8	51.1	55.3	42.6

Comments: *Other findings could also be indicated, such as weaknesses in documentation on the risk management process and weaknesses in risks monitoring.*

32. What was the level of maturity¹⁷/degree of satisfaction with audited risk management and/or internal control system(s) in the Public Sector (central government)?

	very mature/ very satisfied	somewhat mature/ mostly satisfied	between mature and immature/ neither satisfied nor dissatisfied	somewhat immature/ mostly dissatisfied	very immature/ very dissatisfied
Total of returned answers (47)	2	9	20	13	3
% of returned answers	4.3	19.1	42.6	27.7	6.4

Comments: *Public sector entities generally have established risk management frameworks but weaknesses exist in the frameworks application for individual program activities.*

LIST OF COUNTRIES WHICH RESPONDED TO THE QUESTIONNAIRE ON RISK MANAGEMENT IN THE PUBLIC SECTOR

EUROSAI

1. Austria
2. Belgium
3. Bosnia and Herzegovina
4. Bulgaria
5. Cyprus (declares also membership in ASOSAI)
6. Czech Republic
7. Denmark
8. Estonia
9. Finland
10. France
11. Georgia (declares also membership in ASOSAI)
12. Germany

¹⁷ See footnote 6.

13. Hungary
14. Iceland
15. Italy
16. Latvia
17. Lithuania
18. Netherlands
19. Malta
20. Norway
21. Poland
22. Portugal (declares also membership in OLACEFS)
23. Russian Federation (declares also membership in ASOSAI)
24. Romania
25. Slovakia
26. Sweden
27. Turkey (declares also membership in ASOSAI)
28. Ukraine

ASOSAI

29. Australia
30. Bangladesh
31. Bhutan
32. China
33. Korea
34. Malaysia
35. Maldives
36. Pakistan
37. Philippines
38. Thailand

ARABOSAI

39. Jordan
40. Kuwait (declares also membership in ASOSAI)
41. Oman (declares also membership in ASOSAI)
42. Qatar (declares also membership in ASOSAI)
43. Saudi Arabia (declares also membership in ASOSAI)
44. United Arab Emirates (declares also membership in ASOSAI)
45. Yemen (declares also membership in ASOSAI)

AFROSAI

46. Burundi
47. Côte d'Ivoire
48. Egypt (declares also membership in ARABOSAI)
49. Lesotho
50. Republic of South Africa
51. Rwanda
52. Tanzania



Experientia mutua omnibus prodest – Mutual Experience Benefits All

- 53. Uganda
- 54. Zimbabwe
- 55. Zambia

OLACEFS

- 56. Brazil
- 57. Colombia
- 58. Costa Rica
- 59. Honduras
- 60. Salvador

PASAI

- 61. Kiribati

CAROSAI

- 62. Bahamas