RAISING THE AWARENESS OF THE SAIS ON THE ERM Approach in Auditing and Developing Risk-based Annual Audit Plans

Survey Assessment Report

EUROSAI Project Group
May 2023
Quality and Transparency Statement

This is to certify that the assessment report titled as “RAISING THE AWARENESS OF THE SAIS ON THE ENTERPRISE RISK MANAGEMENT (ERM)-ERM Approach in Auditing And Developing Risk-Based Annual Audit Plans” has been developed by following the Quality and Transparency process stated in the “QUALITY AND TRANSPARENCY PROTOCOL FOR EUROSAI PRODUCTS AND DOCUMENTS” as detailed below:

i) Representation of the membership of the PG/TF/WG or group elaborating the product

Turkish Court of Accounts (TCA) is the leader of the PG launched under EUROSAI ESP SG1. SAIs of Hungary and Romania joined the PG as observers. Feedbacks from 28 EUROSAI members were received for the Survey conducted and 2 member SAIs provided peer-review support.

ii) External stakeholder representation/contribution, if any

NA

iii) ToR/Work plan: existence and approval of a ToR/Work Plan to develop the product

ToR of the PG was approved by the EUROSAI Coordination Team in February 2022.

iv) Openness and transparency

At GB technical meeting and GB meeting held in October and November 2021 respectively, the context of the PG was introduced to all participants and the call for interested SAIs was made. Also negotiations with various SAIs continued following the ToR’s approval and they were invited to the PG via e-mail correspondence.

Progress regarding the output of the PG were presented on different occasions organized through the late 2021 and whole 2022, such as the EUROSAI Post-Congress Get-Together held in May 2022 (Brochure “A Quick Update on Project Groups Set by the TCA for ESP 2017-2024/2021-2022 PERIOD was prepared and delivered), EUROSAI GB meetings (both technical and presidential level) as well as EUROSAI SG1 meeting.

Survey was sent to EUROSAI members for inclusiveness and also peer-review were reflected in the document.
v) Work method

November 2021
Project group approval and interested EUROSAI members confirm participation

February 2022
Draft survey prepared and sending it to the observers for feedbacks

March-May 2022
Application of the survey to EUROSAI member SAIs and gathering the first results

November 2022
Sending the draft report to the observers of PG for a review and finalisation of output

March 2023
Approval and dissemination of the assessment report

vi) Exposure:

The output document will be sent by e-mail to all EUROSAI members, and made available to EUROSAI community and external stakeholders on the EUROSAI website (database of products) as well as BIEP.

Metin YENER
President of the Turkish Court of Accounts
1. INTRODUCTION .................................................................................................................................................................. 1
   1.1. EUROSAI Project............................................................................................................................................................... 1
   1.2. Survey...................................................................................................................................................................................................................... 1

2. RISK MANAGEMENT FUNDAMENTALS ......................................................................................................................2
   2.1. Resources Referenced in the Survey................................................................................................................................................. 2
      2.1.1. Principles of ISO 2018 .........................................................................................................................................................................2
      2.1.2. Components and Principles of COSO 2017........................................................................................................................................3
   2.2. Relationship Between the Survey and Key Risk Management Components.....................................................4

3. RESULTS OF THE SURVEY............................................................................................................................................... 6
   3.1. SAIs’ Awareness of Risk Management.............................................................................................................................................. 6
   3.2. Risk Management Practices of the Auditees .............................................................................................................................15
   3.3. SAIs’ Practices Regarding the Auditees’ Risk Management......................................................................................................................20
   3.4. Consideration of Risk Management Practices of the Auditees in Annual Audit Planning ........................21

4. CLOSING REMARKS ..........................................................................................................................................................23
   4.1. Risk Management Awareness of Sais and their Practices Regarding the Auditees’ Risk Management ....23
   4.2. Further Works for Development of A Method for Risk-Based Annual Audit Plans.............................................. 24

ANNEX 1: SURVEY .................................................................................................................................................................. 25
1. INTRODUCTION

In this rapidly changing era, it has become very difficult to predict the future with the effects of developing technology, globalization, and unexpected negative developments such as the COVID-19 epidemic. Since organizations have to make decisions under continuous uncertainty, described as an absolute cloud of fog created by these expected or unexpected developments, risk management (RM) has increasingly attracted their attention in recent years.

The issue of how this trend, which has been rising in recent years, will be reflected in the field of auditing is very important for the SAIs to remain relevant. As we all know, audits are implemented by taking risks into account. However, risks should not be limited just to the execution of audits; risks, especially enterprise level ones, should also be taken into account while making annual audit plans or choosing audit topics among the alternatives. There are various approaches on how to do this, and some SAIs might have specific approaches and practices in this regard. Considering these matters, the Project Group (PG) “Raising the Awareness of the SAIs on the Enterprise Risk Management (ERM) of the auditees and using the ERM approach in developing risk-based annual audit plans” was developed in November 2021.

1.1. EUROSAI Project

The SAI of Türkiye launched this project as the leader in November 2021 with the participation of the SAIs of Hungary and Romania as observers. The project supports the implementation of Strategic Goal 1 in the EUROSAI Strategic Plan 2017-2024, and specifically Objective 1.2 “To support the development of innovative approaches and methods in audit and governance of SAIs making use of new technologies.”

The objective of the PG is to:

- Determine the level of awareness of the SAIs on RM,
- Understand the general concept of the organizations’ risk practices under the relevant SAIs’ mandate (e.g., whether the long-term planning is stimulated by regulations or there is an applicable RM framework within the public sector environment),
- Reveal the most basic practices of SAIs about their auditees’ RM systems, such as whether they carry out assessment/evaluation of auditees’ risk practices, and
- Lay the groundwork for the development of methodology for risk-based annual audit plans.

1.2. Survey

To achieve the PG’s goals, a questionnaire consisting of the following four parts was prepared:

- SAI’s Awareness of RM,
- RM Practices of the Auditees,
- SAI’s Practices Regarding the Auditees’ RM,
- Consideration of RM Practices of the Auditees in Annual Audit Planning.

This survey shown in Annex 1 was applied to SAIs in the EUROSAI region between 24.03.2022 and 16.05.2022.

28 SAIs have responded to the survey. We would like to thank them for their cooperation.

This report describes the results of the survey, which has been prepared based on the internationally accepted RM frameworks which are explained under the next title.
RAISING THE AWARENESS OF THE SAIS ON THE ENTERPRISE RISK MANAGEMENT (ERM)

2. RISK MANAGEMENT FUNDAMENTALS

2.1. Resources Referenced in the Survey

There are different internationally accepted principles and standards for what RM is and how it should be applied. Among all resources related to the subject, “ISO 31000 (2018) Risk Management-Guidelines” (ISO 2018) and “COSO Enterprise Risk Management-Integrating with Strategy and Performance (2017)” (COSO 2017) are referenced as primary resources to be able to form a framework to assess the survey results.

In this PG, ISO 2018’s principles were favored in structuring the survey with a deductive perspective. Thus, an integrated, well-structured, and comprehensive RM has been featured in line with ISO’s principles and framework to conclude that the SAIs’ and other organizations’ awareness of RM is adequate.

On the other hand, COSO 2017’s RM components and principles were considered in setting forth the necessary actions/processes for establishing an ideal RM. For example, ‘delegation of authority to design and implement RM practices’ under the ‘Governance and Culture’ component of the RM is one of the requirements of an ideal RM system according to COSO 2017. Requirements similar to this example were included in the survey to draw conclusions about the RM practices of SAIs and auditees.

2.1.1. Principles of ISO 2018

According to ISO 2018, RM is the ‘coordinated activities to direct and control an organization with regard to risk’. ISO’s eight RM principles suggest organizations establish a RM system, which is:

- integrated,
- structured and comprehensive,
- customized,
- inclusive,
- dynamic,
- based on the best available information,
- considering human and cultural factors, and
- targeting continual improvement.

ISO 2018’s principles highlight the importance of the integration of RM with all organizational activities and a structured and comprehensive approach to RM to contribute to consistent and comparable results. Organizations should customize their systems, because every entity has a different business context as per its objectives. Since the risk environment and risks themselves change, it is better to build a dynamic and inclusive system to observe the changes and involve stakeholders’ views in the process. While establishing and improving the system, human and cultural factors, historical information, and experiences should be taken into account, as well as the entities’ visions and future expectations.¹

2.1.2. Components and Principles of COSO 2017

"COSO Enterprise Risk Management-Integrating with Strategy and Performance (2017)" (COSO 2017) defines five main components of RM encompassing 20 principles to structure an efficient RM system. Here is a table showing COSO (2017)'s components and principles:

Table 1

<table>
<thead>
<tr>
<th>Governance &amp; Culture</th>
<th>Strategy &amp; Objective-Setting</th>
<th>Performance</th>
<th>Review &amp; Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Attracts, Develop, and Retains Capable Individuals</td>
<td></td>
<td>14. Develops Portfolio View</td>
<td></td>
</tr>
</tbody>
</table>

In an exemplary RM system according to COSO 2017 components, the process flows from developing a risk policy/approach in the desired organizational culture, to identifying strategies that take risks into account, to formulating business objectives that align with and support strategies. However, the RM process does not stop here; iterative risk identification, assessment, and treatment follows strategy and objective setting. Finally, with the help of well-structured communication and reporting, the entire system is continually reviewed for any significant changes in the business environment or risk assumptions. The chart below depicts the RM steps:

---


3- RM steps are formulated according to COSO 2017 Risk Management components and principles and ISO 2018's RM process.
An effective RM requires an appropriate business culture along with well-identified assignments of authority, roles, responsibilities, and capable human resources. The availability of desired culture makes it easier to integrate RM with organizations. In recent years, organizations have been advised by internationally accepted frameworks (here ISO 2018 and COSO 2017) to integrate RM with the whole entity rather than treat it as a separate function. In this respect, ISO and COSO share a common view on integrating the RM system with the culture, activities, and functions of organizations so that staff at different levels are focused on managing and optimizing risks. This is the only way entities can adapt an enterprise-wide RM system.

Establishing a dynamic and integrated system as demonstrated above helps entities deploy a proactive approach to risks, allowing organizations to shift their views to the outcome/reward of the risks taken in this changing world.

### 2.2. Relationship Between the Survey and Key Risk Management Components

This report describes how well SAIs and the auditees are aware of the basics of the RM system and derives SAIs’ approach to RM in audit planning. It should also be noted that the survey’s aim was not to assess whether RM exists and functions properly in targeted organizations, but to understand the level of awareness about RM. Therefore, not all requirements of an ideal RM system were included in the survey. In this respect, sufficient factors were considered to draw a conclusion about the target audience’s basic RM approach. A table showing the relationship between key RM components according to COSO 2017 and including elements in the survey is given below:

#### Table 2

<table>
<thead>
<tr>
<th>Key components of RM</th>
<th>Basic actions to meet components' requirements</th>
<th>Related questions in the survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and culture</td>
<td>Defining roles and responsibilities clearly</td>
<td>Q4</td>
</tr>
<tr>
<td></td>
<td>Delegation of authority to design and implement RM practices</td>
<td>Q-4, Q10</td>
</tr>
<tr>
<td>Strategy and objective setting</td>
<td>Developing a RM framework</td>
<td>Q3, Q19, Q20</td>
</tr>
<tr>
<td></td>
<td>Designing RM systematically and with an enterprise wide view</td>
<td>Q9, Q22, Q14</td>
</tr>
<tr>
<td></td>
<td>Determining a risk strategy including the risk appetite and risk tolerance</td>
<td>Q5,</td>
</tr>
<tr>
<td></td>
<td>Deciding long-term strategies</td>
<td>Q6, Q15, Q16, Q17</td>
</tr>
<tr>
<td></td>
<td>Formulating operational objectives</td>
<td>Q7, Q18</td>
</tr>
<tr>
<td>Performance</td>
<td>Identifying risks in strategic and operational levels</td>
<td>Q8, Q11, Q21,</td>
</tr>
<tr>
<td></td>
<td>Developing a risk portfolio</td>
<td>Q12</td>
</tr>
</tbody>
</table>
RAISING THE AWARENESS OF THE SAIS ON THE ENTERPRISE RISK MANAGEMENT (ERM)

<table>
<thead>
<tr>
<th>Key components of RM</th>
<th>Basic actions to meet components' requirements</th>
<th>Related questions in the survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review and revision</td>
<td>Assessing substantial change</td>
<td>Q13-d</td>
</tr>
<tr>
<td></td>
<td>Reviewing risks and entity performance in pursuit of strategies and business objectives</td>
<td>Q13-e</td>
</tr>
<tr>
<td>Information, communication and reporting</td>
<td>Leveraging IT</td>
<td>Q13-a</td>
</tr>
<tr>
<td></td>
<td>Using communication channels to support RM</td>
<td>Q13-b, Q13-c</td>
</tr>
</tbody>
</table>

This table indicates how the survey revealed SAIs’ and auditees’ awareness of RM, which was one of the aims of the survey. Moreover, understanding SAIs’ practices regarding the auditees’ RM approaches and considering their RM practices in annual audit planning are other aims of the PG. To meet these aims, questions between 24 and 31 were directed to the participants.
3. RESULTS OF THE SURVEY

3.1. SAIs' Awareness of Risk Management

The first aim of this PG is to understand the level of RM awareness among SAIs. Awareness can basically be defined as knowledge, understanding, or perception about something. In this survey, “awareness” refers to the quality of being aware of what RM's basic concepts are and how they are applied to organizations.

On the basis of ISO 2018 and COSO 2017, explained under the title 2.1, the basic terms of RM were included in the first two questions. The responses indicate that most SAIs are aware of the definition of basic terms and their application.

Chart 1

These are some terms related to RM. Please check the ones that your SAI is familiar with.
As summarized in Chart 1, all SAIs are aware of terms, such as governance, operational risks, RM, risk identification, control activities, and internal control. In addition, most terms other than risk appetite and risk tolerance are recognized by more than 90 percent of SAIs. The least known expressions are risk appetite and risk tolerance. Bearing in mind that many SAIs reported knowledge of risk appetite and risk tolerance (78.6% and 89.3% of the respondents, respectively), since these two terms require more detailed technical knowledge compared to the rest, fewer SAIs reported knowledge of them.

The chart below shows the same result as the previous question that, in addition to knowing basic terms, many SAIs also know when and how to apply the fundamentals of RM to their organizations.

**Chart 2**

These are some terms related to RM. Which of the following terms is your SAI aware how and when to apply to the organization?
RM Framework

As all entities, whether for-profit, non-profit, or governmental, face rapidly changing risks, adapting a framework including the principles and key steps of RM can be the cornerstone of an organization’s culture. Since the main aim of RM is to help organizations achieve their objectives through considering risks in the strategy-setting process and daily operations, the existence of a RM framework or policy will assist organizations in achieving their objectives more effectively. A RM framework also allows entities to identify, assess, and control their risks systematically, which will probably result in a good example of RM integration into significant activities for efficient implementation.

For all these reasons, we asked SAIs whether they have an applicable RM framework/policy. According to the responses, 23 SAIs (out of 28) report that they have an applicable RM framework. Some SAIs (21 out of 23) also provide supplementary explanations of the scope and coverage. According to the responses, we conclude that SAIs tend to develop their own frameworks instead of a direct adaptation of international standards. Only one SAI mentions such a direct adaptation. Since we do not have a chance to reach all contents of the documents, we cannot comment on the use of the internationally accepted RM framework in their internal policy papers. However, we can say that the frameworks generally include risk identification, assessment, and control procedures, just as expected.

Chart 3

Is there an applicable RM framework/policy in your SAI? If yes, could you please name it and address the scope and coverage?

No 17.9% (5)
Yes 82.1% (23)

When we take a closer look at the responses, we see that the SAIs, who state that they apply a framework that is not separately issued, include their risk-related strategies in other internal documents such as strategic plans, annual plans, operational plans, audit manuals, and audit standards. Five SAIs with no separate framework also report compliance with other legal instruments issued by their governments.

RM frameworks generally include some aspects related to roles and responsibilities to be defined in the system. It is highly important for organizations to make a clear definition of roles, responsibilities, risk ownership, and reporting relationships when designing RM. According to ISO 2018, assigning authority, responsibility, and accountability at appropriate levels within organizations is part of “leadership and commitment” component of RM. Similarly, COSO 2018’s Principle 2 suggests that an organization should clearly assign the authority to design and implement RM practices and, management should define the roles and responsibilities along with accountability for the overall entity and its business units. In this respect, management should clearly define the roles, responsibilities, and accountabilities of individuals, teams, departments, etc.
Taking this role of management into consideration, we asked SAIs whether the management defines roles and responsibilities in their entity. 15 SAIs (out of 28) report that the management clearly defined the related roles and responsibilities; 11 of them state these definitions are partially made. Only 2 SAIs express that there is no definition of roles, responsibilities, risk ownership, or reporting relationships regarding RM.

**Chart 4**

**Does the management of your SAI make a clear definition of roles, responsibilities, risk ownership and reporting relationships regarding RM?**

- Not defined 7.1% (2)
- Partially defined 39.3% (11)
- Clearly defined 53.6% (15)

One SAI responded to this question with “partially defined” and added that roles and responsibilities are exclusively defined with regard to the prevention of and fight against corruption. With this example, we understand that even if not all RM-related roles are defined for the overall entity, it is still possible to assign individuals or teams to a particular role based on the risks organizations face.

**Risk Strategy**

The RM process begins with developing a risk strategy, including the RM’s scope, criteria, and analyses of the business context (i.e., factors that influence organizations) before setting strategies and objectives. RM’s scope may vary from entity to entity. Some organizations may choose to integrate RM with all activities, while others may restrict RM to selected levels, such as strategic or operational.

Determining criteria means planning the RM approach by defining appropriate risk assessment tools such as risk appetite and risk tolerance. Risk appetite can be defined as the amount and type of risk that the organization can or cannot take to achieve its goals and objectives. Risk tolerance is the acceptable level of variation in performance.

In this context, as an initial step, we wanted to find out SAIs’ risk approaches by asking whether they have a risk strategy that includes the basis of RM, such as risk appetite and risk tolerance. Our survey shows that the majority (17 out of 28) determine a risk strategy, but a significant number report that they do not have any risk strategies.
RAISING THE AWARENESS OF THE SAIS ON THE ENTERPRISE RISK MANAGEMENT (ERM)

Chart 5

Does your management determine your SAI’s risk strategy including basis of RM such as risk appetite and risk tolerance?

No 39,3% (11)
Yes 60,7% (17)

Strategy and Objective Setting

After determining their risk strategy (including RM scope, risk criteria, and analyses of business context), entities should determine their long-term strategies and business objectives. Even though the main purpose of RM is to contribute to the achievement of organizational goals, it should be noted that new RM approaches highlight the importance of taking risks into consideration while establishing strategies and formulating objectives at various levels.

The survey shows that 27 respondents out of 28 determined their strategic aims.

Chart 6

Are long-term strategies of your SAI determined (i.e. strategic aims/goals/objectives)?

No 3,6% (1)
Yes 96,4% (27)

Out of 27 SAIs that set their strategic aims, 17 state that the strategic aims are determined with a risk-based approach, and 10 SAIs do not take risks into consideration in this process.
Chart 7

If YES to previous question; are your SAI's strategic aims determined risk-based? (i.e. is a risk analysis made for alternative strategies before setting them or are the risks of existing strategies assessed?)

![Chart 7]

No 37% (10)
Yes 63% (17)

After formulating their strategies, organizations should establish their business (operational) objectives at different levels to align with and support those strategies. According to the responses of 28 respondents, the majority (26 SAIs) have developed their business objectives.

Chart 8

Are the business (operational) objectives of your SAI determined (at business/operational level or as operational/annual plans)?

![Chart 8]

No 7.1% (2)
Yes 92.9% (26)

Risk Identification

Risk identification and treatment are highly technical and iterative processes so new knowledge and analysis can lead to a revision of risks and controls. A variety of approaches are available for risk identification, assessment of the severity of risks, risk prioritization, and controls. As mentioned earlier, the aim of this survey is not to evaluate the effectiveness of RM but rather to provide some insights into SAIs' awareness of RM. Therefore, we only aimed at figuring out SAIs' basic approach to risk identification.

In this context, we asked SAIs whether they identify risks. The survey shows that 25 SAIs identify the risks they face. Only a few (3) do not carry out such identification.
RAISING THE AWARENESS OF THE SAIS ON THE ENTERPRISE RISK MANAGEMENT (ERM)

Chart 9

Are risks determined in your SAI?

Yes 89,3% (25)

No 10,7% (3)

Even though the integration of RM with the functions and significant activities of an entity, from setting strategies to day-to-day operations, is ideal, this might take place only at some high levels, such as developing the vision of an entity or strategy setting. Moreover, organizations might not prefer (or might not be able) to deal with risks by developing a comprehensive system. In addition, many organizations might already have an internal control system; for this reason, risk practices might be restricted by internal control practices. All these issues reflect different possible approaches to risk identification and treatment. In this context, SAI’s approach to determining and treating the risks is sought in the survey. The summary of the responses is shown below.

Chart 10

What is your SAI’s approach to determine and treat the risks?

Risk management and internal control system are integrated in that both entity level risks and operational risks are determined and treated. And also, risks are considered in making decisions including developing strategies and allocation of resources; 60%

Risks are determined and treated, but neither in terms of risk management nor internal control practices; 4%

Risks are only approached within internal control practices; 12%

Risk management is separately designed from internal control system, and, the system is with established enterprise-level functions that aggregate and manage risks with an enterprise wide view; 12%

Other (please explain); 12%
15 SAIs (out of 25 that identify risks) state that risks are considered in the strategy setting process, in making decisions, and in allocating resources. The survey shows that these SAIs also identify entity-level (enterprise) risks and operational ones. This option is ideal in that RM is integrated with the strategies, decision-making process, and operations.

Three SAIs report that RM is established separately from internal control systems and with an enterprise-wide view. It can be said that these SAIs also consider risks at both strategic and operational levels.

Three SAIs declare that they approach risks only within the framework of internal control. Since “making strategic decisions impacting the entity’s objective is not part of internal control” but might be a process of RM approaches⁴, this option implies that in these SAIs, risks affecting achievement of pre-set objectives are identified and treated.

Only one SAI reports that risks are identified and treated without a structured system. In addition, two SAIs identify and treat risks for some specific functions, such as financial operations.

**Risk Types**

In the survey, we asked SAIs what types of risks they identify. According to the responses, 25 respondents (out of 25) identify their information technology-related risks. 24 of them identify:

- Risks related to SAI’s reputation, independence, and credibility,
- Risks related to audits,
- Risks related to operations (payrolls, procurement, daily expenditures, revenue, and other operations).

20 SAIs out of 25 identify compliance risks and 15 identify reporting risks (SAIs’ own reporting). According to the supplementary information provided by SAIs, one SAI also considers professional development/training risks and, one SAI states that “a risk analysis is made considering all risks to the production of the Court of Audit's reports and to its functioning including risks related to the context and the expectations of and towards stakeholders.”

**Chart 11**

What types of risk are determined?

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks related to SAI’s reputation, independence, and credibility</td>
<td>96,00%</td>
</tr>
<tr>
<td>Risks related to audits</td>
<td>96,00%</td>
</tr>
<tr>
<td>Risks related to information technology</td>
<td>100,00%</td>
</tr>
<tr>
<td>Risks related to operations (payrolls, procurement, daily expenditures, revenue, other operations)</td>
<td>96,00%</td>
</tr>
<tr>
<td>Compliance risks</td>
<td>80,00%</td>
</tr>
<tr>
<td>Reporting risks (SAI’s own reporting)</td>
<td>68,00%</td>
</tr>
<tr>
<td>Other (Please further specify)</td>
<td>12,00%</td>
</tr>
</tbody>
</table>

⁴ - COSO Internal Control-Integrated Framework, May 2013 page: 15
Risk Register

After identifying the risks, it is important to record and classify them to be able to design a good system. In this context, having a risk registry provides significant advantages. A risk registry (inventory) is a simple list of risks that organizations face and identify. Having a risk registry enables organizations to group similar risks under standard categories such as reputational risks, financial risks, and IT risks. In this way, entities may determine risks impact at different levels (business objectives, enterprise objectives, or strategies).

The survey shows that 22 SAIs out of 25 who identify the risks, have risk registries. And, out of the 22, who have the registry, 21 state that they monitor the risk register systematically.

Chart 12

Is there a risk register in your SAI?

| YES | 22 |
| NO  | 3  |

Review/Revision, Information, Communication and Reporting of RM System

Even though there are numerous approaches to managing risk in organizations, regardless of their size and structure, people in managerial roles have responsibilities for designing RM and delegating roles, responsibilities, and accountabilities across the organization. The role of management is to not only design and implement RM, but also ensure that it functions efficiently and is updated against substantial change in the internal and external environment affecting risks. To be able to achieve its role, management needs to access accurate and timely information. Fortunately, advances in technology make it possible to transform data into information without creating obstacles. Herewith, leveraging IT to support RM with timely reporting is essential for the management to achieve its targets.

Another critical element of an effective RM is communication. The existence of communication channels and the quality of interaction throughout the entity affect the effectiveness of RM in several ways. For example, well-structured internal communication between management and staff allows management to clearly convey the entity’s vision, strategy, objectives, and responsibilities to employees. On the other hand, staff should have the opportunity to communicate with management about potential risks and threats. For all these reasons, communication is a key component of RM.

Organizations operate in an internal and external environment that can change over time. Substantial changes might require revisions of strategies and organizational objectives as well as risks and the RM system. Therefore, management should carry out ongoing monitoring and periodic reviews of the RM system.

For these reasons, we posed Question 13 to find out SAIs’ perceptions of RM’s adequacy for information systems, communications channels, and review and revision measures. The table below summarizes the results.
Table 3

<table>
<thead>
<tr>
<th>Statement</th>
<th>Highly agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Highly disagree</th>
<th>Number of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our SAI’s IT systems guarantee the management access to timely, qualitative reports on the fulfillment of stated objectives.</td>
<td>7%25</td>
<td>16%57</td>
<td>5%17</td>
<td>0%0</td>
<td>28</td>
</tr>
<tr>
<td>The quality of interaction among the management, staff and departments allows employees to do their jobs effectively.</td>
<td>12%42,9</td>
<td>16%57</td>
<td>0%0</td>
<td>0%0</td>
<td>28</td>
</tr>
<tr>
<td>There are defined channels which allow rapid, obstacle-free communication with the management about potential risks and threats.</td>
<td>11%39,3</td>
<td>14%50</td>
<td>3%10,7</td>
<td>0%0</td>
<td>28</td>
</tr>
<tr>
<td>Our SAI considers internal and external changes that can affect achievement of our strategy and business objectives such as impact of audit, timely audit reports, high quality audits, other operational objectives etc.</td>
<td>14%50</td>
<td>14%50</td>
<td>0%0</td>
<td>0%0</td>
<td>28</td>
</tr>
<tr>
<td>Our SAI regularly reviews the organization’s performance to understand if the strategies and business objectives are met (or can be still achieved) and whether identified risks are realistic to achieve targets</td>
<td>14%50</td>
<td>14%50</td>
<td>0%0</td>
<td>0%0</td>
<td>28</td>
</tr>
</tbody>
</table>

The survey shows that 7 SAIs out of 28 are highly satisfied with their IT systems that allow management to access timely reports on the fulfillment of stated objectives. 16 SAIs state that the capabilities of the IT systems related to the reports mentioned are adequate. Five SAIs disagree with that the IT system produces timely, qualitative reports on the fulfillment of stated objectives.

When it comes to communication, all respondents state that the quality of interaction among the management, staff, and departments allows employees to do their jobs effectively at some level (high or fair). And all SAIs except three report that there are communication channels for obstacle-free communication with the management about potential risks and threats.

All SAIs state that they monitor changes affecting the objectives and review their performance to understand whether the strategies and business objectives are met (or can still be achieved) and whether identified risks are realistic for achieving targets.

3.2. Risk Management Practices of the Auditees

Strategy and Objective Setting in Auditees

In some countries, governments stimulate strategic planning through legal arrangements. This helps governmental agencies make their long-term plans with a standardized perspective, which generally results in implementations that are more efficient. Survey results show that all countries with respondents stipulate long-term planning through legislation. According to supplementary information, the legislation is applied to;

- Central government agencies in 27 countries,
- Local government agencies in 21 countries,
- Public companies in 17 countries, and
- Semi-state bodies, not-for profit organizations, and independent institutions in some countries.
Chart 13

The survey shows that even if governments stipulate long-term planning through legislation, it cannot be taken to mean that all entities determine their strategies. However, based on survey responses it can safely be interpreted that significant numbers of auditees identify their strategies.

Chart 14

Do audited entities determine their long-term strategies (even if it is not stipulated by legislation)?

Looking into the identified operational objectives, we can see that the majority of auditees set them as well as strategies.
According to the responses given to Question 3, we see that more than 80 percent of SAIs have a RM framework. In this survey, we wanted to understand whether there is an applicable RM framework within the public sector environment. According to the responses, there is a framework for the use of entities in the public sector in 23 countries (out of 28).

Some countries also provide supplementary information about the scope of these frameworks. When analyzing additional information, SAIs' statements indicate that governments issue legal documents/guidance generally on internal control covering RM components.
Countries might tend to see RM as a part of internal control. However, it should be noted that although internal control and RM are highly related, they have different focuses; neither supersedes the other. Internal control mostly focuses on providing reasonable assurance that targets will be achieved by highlighting controls in operations and compliance with relevant laws and regulations. Furthermore, setting strategies and objectives considering business context and risks is not a part of internal control but RM's. On the other hand, RM's focus is on managing risk through:

- Recognizing culture,
- Developing capabilities,
- Applying practices (supporting decision-making at all levels),
- Adding value to organizations, and
- Integration of the system with the entity’s strategy setting, functions, and activities (considering risks in strategy/objective setting and day-to-day operations)

The survey shows that more than 80% of the countries responding to the questionnaire have an applicable risk framework. Possibly as a result of this advantage, 21 SAIs (out of 28) report that significant numbers of auditees identify their risks (Moreover, 2 SAIs inform that all the entities identified their risks). Only 4 SAIs state the opposite of this statement.

**Chart 18**

**Do the audited entities identify their risks?**

<table>
<thead>
<tr>
<th>Description</th>
<th>Percentage</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>No knowledge within our SAI</td>
<td>3.6% (1)</td>
<td></td>
</tr>
<tr>
<td>They all do</td>
<td>7.1% (2)</td>
<td></td>
</tr>
<tr>
<td>Significant numbers do not</td>
<td>14.3% (4)</td>
<td></td>
</tr>
<tr>
<td>Significant numbers do</td>
<td>75% (21)</td>
<td></td>
</tr>
</tbody>
</table>

Risk types are important for this PG in that one of the focuses of RM is considering risks at the strategic level. In this context, the survey shows that the auditees determine their strategic risks in 16 countries out of 21 (two SAIs skipped this question).

---

7- COSO Enterprise Risk Management: Integrating with Strategy and Performance (2017) page 10-12
Even though a significant number of organizations identify their strategic risks, it is not certain whether they design a proper RM system, according to the SAIs' responses to the following question. The chart below shows whether auditees execute RM practices across the organization in a systematic and consistent manner.

**Chart 20**

**Do audited entities execute RM practices across the enterprise in a systematic and consistent manner?**
3.3. SAIs’ Practices Regarding the Auditees’ Risk Management

SAIs carry out different types of audits depending on their mandate. According to ISSAI 100, there are three main types of public-sector audits; financial audit (FA), performance audit (PA), and compliance audit (CA). ISSAI 100 also recognizes audits or other engagements on any subject of relevance to the responsibilities of management and those charged with governance and the appropriate use of public resources, such as adherence to internal control standards, real-time audits.

According to the audit principles set by ISSAIs, risk assessment is an important element of any type of audit. For example, a risk assessment shall be conducted in the planning phase of the financial audit. Therefore, every SAI considers their auditees’ risks at some level.

Herein, we posed the question, “Does your SAI carry out assessment/evaluation of auditees’ risk practices?” Only two SAIs report that they do not carry out such assessments.

Then, we examine through what types of audits and other engagements SAIs assess the risk practices of the auditees.

Chart 21

Through what types of audits does your SAI carry out the assessment/evaluation of risk practices of the audited entities?

According to results, 22 SAIs (out of 26) conduct risk assessment in traditional audits (FA, CA, PA). Five SAIs report that they also carry out stand-alone evaluation. One SAI provides additional information about their specific methodology (integrity assessment). One SAI also mentions that they carry out regularity audits consisting of financial, compliance audit, and evaluation of internal control systems of entities, which also covers the assessment of RM.

As seen in Chart 21 above, SAIs approach risk assessment traditionally. The next chart explains in what focus areas the risk assessment is carried out. According to responses, many respondents (14 out of 26) assess auditees’ risk practices in all three focus areas of understanding the entity, executing the audit and separate evaluation of internal controls/RM. Three SAIs make risk assessment only while understanding the entity, one SAI only while executing the audit, and three SAIs while evaluating the risk practices separately.

This part of the questionnaire aims at revealing whether SAIs take risks into account while preparing annual audit plans. For that purpose, we pose SAIs three questions:

- Prior to the start of audits, are the risks of the auditees assessed within the framework of SAI’s annual audit planning efforts? (Not in the framework of individual audit planning)
- What criteria are used to assess the risks of the auditees?
- Are the risks identified by the auditees for their organization considered in the annual audit plan of your SAI?

The survey shows 26 SAIs (out of 28) consider the auditees’ risks while preparing annual audit plans. The most common criteria used by SAIs (out of 26) are:

- Assessment based on prior audits (23 SAIs)
- Strategic importance (e.g., government priorities) (21 SAIs)
- Follow-up results (20 SAIs)
- Fraud prevention (e.g., reported cases in recent years) (19 SAIs)
As seen above, there are many risk criteria, including the auditees’ enterprise risks, used by SAIs when planning audits. From this aspect, it is very important that institutions share their enterprise risks with the SAIs and that these risks are taken into account in the annual plans. In this context, 17 SAIs report that they already consider the risks identified by the auditees for their organization.

**Chart 23**

Are the risks identified by the auditees for their organization considered in the annual audit plan of your SAI?

- Yes 60,7% (17)
- No 39,3% (11)
4. CLOSING REMARKS

4.1. Risk Management Awareness of SAIs and their Practices Regarding the Auditees’ Risk Management

The RM proposed by the sources referenced in this PG is a system that is integrated with the significant activities of institutions, has an enterprise perspective beyond individual operations, and is structured comprehensively. Moreover, there are essential steps to be taken for an ideal RM.

Although the recommendations of internationally recognized standards are taken as a basis in this PG, the authors of this report are aware the fact that RM frameworks should be adapted according to the specific needs of the countries, as in every standard. Therefore, this survey was designed by taking into account the very basics of RM.

In the survey, we tried to understand how the SAIs generally approach RM, besides details about processes. In this context, we see that 18 SAIs (out of 28) report that RM should be structured to set risk-based strategies and achieve them along with the business objectives through a risk-based decision-making process as suggested by RM frameworks (ISO and COSO in this PG). 10 SAIs are more in favor of ensuring the safety of assets, checking the consistency and reliability of accounting data, enhancing operational efficiency, and encouraging its implementation, which is closer to an internal control perspective.

The process and basic steps of RM implemented in SAIs and organizations under their jurisdiction are described throughout the report. Here is a summary of the key takeaways from the survey regarding the systems:

✔ Many SAIs (23 out of 28) have applicable RM frameworks defining RM processes. Moreover, 23 countries have a framework for the entities operating in the public sector.

✔ The survey shows that only about half of the responded SAIs (53.6%) clearly define their risk management related roles and responsibilities which are key elements of an efficient RM system.

✔ 60 percent of SAIs in the survey report that they have integrated RM and internal control systems where both entity level risks and operational risks are determined and treated. These SAIs also consider risks while making decisions including developing strategies and allocating resources as suggested by internationally recognized standards such as ISO and COSO.

✔ When looking at the auditees’ risk practices, the survey shows that ‘majority of auditees’ in eight countries (out of 28); ‘some auditees’ in 12 countries execute RM practices across the organization in a systematic and consistent manner.

✔ 26 SAIs (out of 28) carry out assessments of auditees’ risk practices through their audits (FA, CA, PA) and other engagements, such as stand-alone evaluations. 12 SAIs also form an opinion based on their assessment.

Consequently, the survey results show that the SAIs’ awareness of RM is quite satisfactory, as are their practices regarding the auditees’ RM.
4.2. Further Works for Development of a Method for Risk-based Annual Audit Plans

Since one of the objectives of the PG is to lay the groundwork for the development of methodology for risk-based annual audit plans, the survey also focuses on the consideration of risks in annual audit plans. In this regard, it is clearly seen that most SAIs (26 out of 28) use different risk criteria when preparing audit plans. When we look at the top ten risk criteria preferred by the respondents, we see that “enterprise risks” rank tenth from the top. Moreover, 17 SAIs (out of 28) report that risks identified by the auditees for their organization are considered in the annual audit plans. Therefore, further planning for the development of a systematic method for risk-based annual audit plans would be beneficial for SAIs, who do not consider risks in their planning or have a limited list of risk criteria. In this way, entities or sectors with higher risks might be given priority for any type of audit engagement, or audit topics with higher risks can be selected for relative audit periods.
ANNEX 1: SURVEY

SAIS' AWARENESS OF RISK MANAGEMENT

Questions under this title aim at understanding SAIs’ awareness and basic knowledge of risk management. Please consider your organization’s expertise, knowledge and experiences when answering the questions.

1. These are some terms related to risk management. Please check the ones that your SAI is familiar with.

<table>
<thead>
<tr>
<th>Governance</th>
<th>Risk appetite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission of an entity</td>
<td>Risk tolerance</td>
</tr>
<tr>
<td>Vision of an entity</td>
<td>Risk identification</td>
</tr>
<tr>
<td>Strategic (entity level) objectives</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>Business (operational) objectives</td>
<td>Risk prioritization</td>
</tr>
<tr>
<td>Risk</td>
<td>Risk responses</td>
</tr>
<tr>
<td>Strategic risk (entity level risk)</td>
<td>Control activities</td>
</tr>
<tr>
<td>Operational risk</td>
<td>Internal control</td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
</tr>
</tbody>
</table>

2. These are some terms related to risk management. Which of the following terms is your SAI aware how and when to apply to the organisation?

<table>
<thead>
<tr>
<th>Governance</th>
<th>Risk appetite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission of an entity</td>
<td>Risk tolerance</td>
</tr>
<tr>
<td>Vision of an entity</td>
<td>Risk identification</td>
</tr>
<tr>
<td>Strategic (entity level) objectives</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>Business (operational) objectives</td>
<td>Risk prioritization</td>
</tr>
<tr>
<td>Risk</td>
<td>Risk responses</td>
</tr>
<tr>
<td>Strategic risk (entity level risk)</td>
<td>Control activities</td>
</tr>
<tr>
<td>Operational risk</td>
<td>Internal control</td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
</tr>
</tbody>
</table>
3. Is there an applicable risk management framework/policy in your SAI? If yes, could you please name it and address the scope and coverage?

☐ Yes ☐ No

If yes; explanation (Title, scope and coverage briefly; if also possible, link to the related document)…………………………………………………

4. Does the management of your SAI make a clear definition of roles, responsibilities, risk ownership and reporting relationships regarding risk management?

☐ Clearly defined ☐ Partially defined ☐ Not defined

Remarks:........................................................................................................................................................................

5. Does your management determine your SAI's risk strategy including basis of risk management such as risk appetite and risk tolerance?

☐ Yes ☐ No

6. Are long-term strategies of your SAI determined (i.e. strategic aims/goals/objectives)?

☐ Yes ☐ No

If yes; are your SAI's strategic aims determined risk-based? (i.e. is a risk analysis made for alternative strategies before setting them or are the risks of existing strategies assessed?)

☐ Yes ☐ No

7. Are business (operational) objectives of your SAI determined (in business/operational level or as operational/annual plans)?

☐ Yes ☐ No

8. Are risks determined in your SAI? (If NO, please go to Q13)

☐ Yes ☐ No
9. What is your SAI's approach to determine and treat the risks?

☐ Risks are determined and treated, but neither in terms of risk management nor internal control practices.

☐ Risks are only approached within internal control practices.

☐ Risk management is separately designed from internal control system, and, the system is with established enterprise-level functions that aggregate and manage risks with an enterprise wide view.

☐ Risk management and internal control system are integrated in that both entity level risks and operational risks are determined and treated. And also, risks are considered in making decisions including developing strategies and allocation of resources.

☐ Other (please explain)……………………………………………………………………

10. Who is responsible for risk identification and treatment in your SAI? (Multiple answers possible)

☐ A delegated person (i.e. risk manager, chief of risk management, risk leader)

☐ A delegated board/committee

☐ A delegated department

☐ Senior management

☐ Employees/business units

☐ Other (Please explain briefly) ....................................................................................

11. What types of risk are determined? (Multiple answers possible)

☐ Risks related to SAI's reputation, independence and credibility

☐ Risks related to audits

☐ Risks related to information technology

☐ Risks related to operations (payrolls, procurement, daily expenditures, revenue, other operations)

☐ Compliance risks

☐ Reporting risks (SAIs' own reporting)

☐ Other (Please further specify).................................................................................

12. Is there a risk register in your SAI?

☐ Yes ☐ No

If yes; does your SAI monitor the risks register systematically?

☐ Yes ☐ No
13. Please select the most convenient option for your SAI (Please check only one option for each statement)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our SAI’s IT systems guarantee the management access to timely, qualitative reports on the fulfilment of stated objectives.</td>
<td>□ Highly Agree □ Agree □ Disagree □ Highly Disagree</td>
</tr>
<tr>
<td>The quality of interaction among the management, staff and departments allows employees to do their jobs effectively.</td>
<td>□ Highly Agree □ Agree □ Disagree □ Highly Disagree</td>
</tr>
<tr>
<td>There are defined channels which allow rapid, obstacle-free communication with the management about potential risks and threats.</td>
<td>□ Highly Agree □ Agree □ Disagree □ Highly Disagree</td>
</tr>
<tr>
<td>Our SAI considers internal and external changes that can affect achievement of our strategy and business objectives such as impact of audit, timely audit reports, high quality audits, other operational objectives etc.</td>
<td>□ Highly Agree □ Agree □ Disagree □ Highly Disagree</td>
</tr>
<tr>
<td>Our SAI regularly reviews the organization’s performance to understand if the strategies and business objectives are met (or can be still achieved) and whether identified risks are realistic to achieve targets.</td>
<td>□ Highly Agree □ Agree □ Disagree □ Highly Disagree</td>
</tr>
</tbody>
</table>

14. Which of the following statements is considered more appropriate by your SAI? (Please check only one option)

- □ Risk management should be structured to set risk-based strategies and achieve them along with the business objectives through risk-based decision-making process
- □ Risk management should be structured to achieve objectives, to ensure the safety of assets, to check the consistency and reliability of accounting data and, to enhance operational efficiency

RISK PRACTICES OF THE AUDITED ENTITIES

Questions under this title aim at understanding the risk practices of the audited entities. Please remember that even if no risk management is structured in the entities, it is still possible to answer these questions, because any activities related to risks are the focus of this survey.

15. Is long-term planning (generally is referred to “strategic planning”) stipulated in your country by laws or other regulations within public sector?

- □ Yes
- □ No
16. If the answer to Q 15 is YES, for which organizations is this legislation applied to? (Multiple answers possible)

☐ Central government
☐ Local government
☐ Public companies (state owned companies)
☐ Other (please explain)……………………………………………………….

17. Do audited entities determine their long-term strategies (even if it is not stipulated by legislation)?

☐ They all do
☐ Significant numbers do
☐ Significant numbers do not
☐ None of them does

Explanation..............................................................................

18. Do audited entities determine their business/operational objectives?

☐ They all do
☐ Significant numbers do
☐ Significant numbers do not
☐ None of them does

Explanation..............................................................................

19. Is there an applicable risk management framework within the public sector environment?

☐ Yes (explain briefly)☐ No

If yes; explanation (Title and scope; if possible link to the related document).............................................

20. If the answer to Q 19 is YES, for which organizations is this framework applied to? (Multiple answers possible)

☐ Central government
☐ Local government
☐ Public companies (state owned companies)
☐ Other (please explain)……………………………………………………….
21. Do the audited entities identify their risks?

☐ They all do  
☐ Significant numbers do  
☐ Significant numbers do not  
☐ None of them does

If yes; what types of risks are identified? (Multiple answers possible)

☐ Strategic (entity-level) risks

☐ Business (operational) risks

☐ Financial risks

☐ Compliance risks

☐ No  
☐ No knowledge within our SAI

22. Do audited entities execute risk management practices across the enterprise in a systematic and consistent manner?

☐ Yes, majority of auditees do  
☐ Yes, some auditees do  
☐ No but, few auditees do  
☐ No, majority of auditees do not  
☐ No knowledge about it within our SAI

23. In which area should the audited entities improve their abilities regarding risk management? (Multiple answers possible)

☐ Risk management awareness  
☐ Experience on risk management  
☐ Technical skills  
☐ Communication skills  
☐ Risk management knowledge  
☐ Other (please explain)…………………………………………………………

---

8- Risks that either affect or are created by business strategy decisions and strategic aims  
9- Risks that an organization’s ability to execute its strategic plan and operational objectives  
10- Risks include areas such as financial reporting, valuation, market, liquidity, and credit risks.  
11- Risks relate to legal and regulatory compliance.
SAIs’ PRACTICES REGARDING THE AUDITED ENTITIES’ RISK MANAGEMENT

Questions under this title aim at understanding if SAIs consider the audited entities’ risk practices (within the scope of internal control, risk management etc.) in the framework of an audit, evaluation or assessment. Please take any activities related to risks of the entities into account when answering the questions.

24. Does your SAI carry out assessment/evaluation of audited entities' risk practices? (If NO, go to Q28)

☐ Yes ☐ No

Explanation (if needed) ........................................................................................................................................

25. Through what types of audits does your SAI carry out the assessment/evaluation of risk practices of the audited entities? (Multiple answers possible)

☐ Financial audit
☐ Compliance audit
☐ Performance audit
☐ Standalone evaluation
☐ Other (please further describe) ..........................................................................................................................

26. In what focus areas does your SAI carry out assessment/evaluation of the audited entities' risk practices? (Multiple answers possible)

☐ Within the framework of understanding the entity in audits (E.g. Determining/identifying procedures for assessing risks of material misstatements)
☐ Within the framework of conducting phase of audits
☐ Within the framework of separate evaluation of internal controls/risk management
☐ Other (please further describe) ..........................................................................................................................

27. Are the results of the assessment/evaluation of the risk practices included in the audit reports?

☐ Yes ☐ No

If yes; Is an opinion formed based on the assessment/evaluation of the risk practices?

☐ Yes ☐ No
CONSIDERATION OF RISK MANAGEMENT PRACTICES OF THE AUDITED ENTITIES IN ANNUAL AUDIT PLANNING

Questions under this title aim at revealing if SAIs take risks into account when preparing annual audit plans.

28. Prior to the start of audits, are the risks of the audited entities assessed within the framework of SAI’s annual audit planning efforts? (Not in the framework of individual audit planning)

☐ Yes  ☐ No

29. If the answer to Q 28 is YES, what criteria are used to assess the risks of the audited entities?

☐ Non-utilisation of funds (unspent balances, parking of funds)
☐ Fraud prevention (e.g. reported cases in last years)
☐ Realization of revenues
☐ Existence of risk management
☐ Risk management effectiveness
☐ Enterprise risks
☐ Population of the territory the entity functions in
☐ Automation of government functions
☐ IT risks
☐ IT controls
☐ Availability of internal audit
☐ Assessment based on prior audits
☐ Strategic importance (e.g. government priorities)
☐ Gap in Audit
☐ Visibility in media
☐ Follow-up results
☐ None of the above
☐ Other (please explain)....................................................................................................................
30. Are the risks identified by the auditees for their organization considered in the annual audit plan of your SAI?

☐ Yes   ☐ No

31. Would it be beneficial to set a relationship between the auditees’ entity-level (enterprise-level) risks defined by the entities and SAIs’ annual audit plans? (I.e. entities with higher enterprise-level risks might be given some sort of priority for any type of audit. Or, audit topics related to some sectors with higher enterprise-level risks might be selected)

☐ Yes, it would be beneficial
☐ No, not necessarily
☐ Other (please explain)

Explanation:............................................................