14th Scientific Research Competition of the ARABOSAI

Topic 4: The Role of Supreme Audit Institutions in Developing Risk Management Systems in Government Entities

Prepared by: Faisal Mani
Prosecutor at the Tunisian Court of Accounts

June 2024

"In reality, disorder cannot be managed; one can only attempt to prevent it, mitigate its effects, or restore order."
Simon Eiken & Olivier Villin (Crisis Management – Corporate Response, EFE 2006)

Table of Contents

V. Challenges and Difficulties

1. Challenges Faced by Supreme Audit Institutions
2. Difficulties Encountered by Audited Government Entities

- Conclusion
- Recommendations
- References

The Role of Supreme Audit Institutions in Developing Risk Management Systems in Government Entities

Introduction

Throughout history, societies worldwide have been exposed to various risks, crises, and disasters, whether natural (environmental catastrophes), political (wars, conflicts, revolutions), economic (financial crises, inflation, debt surges, investment decline), social (strikes, protests, rising unemployment), or technological (cyberattacks, data breaches, system failures).

Studies indicate that over 90% of natural disasters are linked to climate change, including floods, droughts, earthquakes, and pandemics. These unpredictable events often disrupt public institutions and threaten the continuity of government services.

Risk governance requires public institutions to be well-prepared rather than resorting to last-minute emergency responses. While governments bear primary responsibility for risk management, Supreme Audit Institutions (SAIs) also have a critical role to play.

As independent oversight bodies, SAIs are tasked with auditing public funds, ensuring financial integrity, and evaluating governance efficiency. They, too, face risks in fulfilling their mandates and must implement robust internal risk management strategies, as outlined in INTOSAI-P12 Principle 9, which calls for SAIs to regularly assess organizational risks and establish effective internal controls.

Moreover, SAIs must set an example for public institutions in risk management. It would be inconsistent for an SAI to hold government entities accountable for failing to implement risk management policies without having done so itself.

As public entities face increasingly complex risks that may threaten their existence, establishing strong risk management systems becomes a critical priority. Effective risk management helps anticipate threats, mitigate their impact, and ensure the continuity of public services.

Risk is broadly defined as a potential future harm that may result in human, economic, or environmental losses. Risk management is the systematic process of identifying, evaluating, and addressing risks to minimize their impact. International frameworks such as ISO 31000 - 2018 and COSO ERM provide structured methodologies for risk assessment.

Risk management is the first step in crisis and disaster response. Crisis management, guided by frameworks such as ISO 22361, involves implementing predefined strategies to handle emergencies and minimize disruptions. In this context, strategic foresight is crucial, and public institutions must analyze data, detect warning signs, and act proactively.

A key component of crisis management is the development of Crisis Management Plans (CMPs), which outline roles, communication protocols, and resource allocation strategies to ensure swift and coordinated decision-making during emergencies.

Research Problem

Given the increasing importance of risk management in the public sector and the mandate of SAIs, this study seeks to answer the following questions:

- What role can SAIs play in developing and improving risk management systems in government entities?
- What tools and mechanisms can SAIs use to enhance risk management in the institutions they audit?
- How do SAIs contribute to evaluating existing risk management systems?
- What impact do SAI reports and recommendations have on governmental risk management practices?

Research Objectives

To address the problem posed by research and answer the questions raised therein, the main elements and objectives of this research will be based on the following:

1. The role of SAIs in educating and raising awareness of the importance of implementing risk management systems in government institutions.
2. The contribution of SAIs to Assess risk management frameworks in audited entities.
3. Analyze the impact of SAIs reports and recommendations on public risk management practices.
4. Identify challenges SAIs face in supporting governmental risk management systems.

Research Methodology

The methodology of this research focuses on defining the scope of study, identifying related issues, and applying an inductive approach. Various up-to-date sources, international standards, and best practices related to risk management have been analyzed.

Additionally, this study examines case studies from SAIs that have implemented risk management frameworks. One key reference is IDI's CRISP initiative (Crisis and Risk Management for SAIs), launched in 2020 by the INTOSAI Development Initiative (IDI), which aims to strengthen SAIs' capacities in risk management and crisis response.

This research also includes:

- A review of theoretical concepts, including definitions of risk, crisis, and disaster management.
- A comparative analysis of risk management models, such as ISO 31000 and COSO ERM.
- A study of audit reports and recommendations issued by SAIs regarding public risk management.
- An assessment of challenges that SAIs face in promoting risk management systems in government entities.

The research is structured into five main sections:

1. Fundamentals of Risk Management – Providing readers with essential concepts before delving into more specific analyses.
2. The Role of SAIs in Risk Awareness and Education – Exploring how SAIs promote risk awareness in the public sector.
3. SAIs' Contribution to Evaluating Risk Management Systems – Analyzing how SAIs assess the effectiveness of risk management frameworks.
4. The Impact of SAI Reports on Risk Management Practices – Studying how audit recommendations influence risk-related policies.
5. Challenges Faced by SAIs – Identifying difficulties encountered by SAIs in supporting governmental risk management.

I. General Framework: Principles and Foundations of Risk Management

Risk management is a systematic and proactive approach aimed at identifying, assessing, and addressing potential threats that could negatively impact an organization. It follows a structured methodology, incorporating internationally recognized frameworks such as ISO 31000 - 2018 and COSO Enterprise Risk Management (ERM).

The key components of risk management include:

1. Identifying Risks

Risk identification is the first step in the process and involves systematically recognizing internal and external threats that could disrupt operations.

- Risks may be strategic, operational, financial, technological, or environmental.
- Public sector risks include budgetary constraints, fraud, cybersecurity threats, and political instability.

2. Risk Assessment

Once identified, risks must be evaluated in terms of likelihood and impact:

- Likelihood: The probability of the risk occurring.
- Impact: The severity of the consequences if the risk materializes.
- Risk Matrix: A tool that categorizes risks based on their likelihood and impact to prioritize response strategies.

The following table presents a model of a probability and consequences classification system that includes five (5) levels, inspired by ISO 31000's guidance:

Relative Risk Assessment	Likelihood Level	Percentage Range	Category	Description	Consequence Level
Almost Certain	High Probability	91 – 100%	5	Significantly disrupts operations and threatens survival	Catastrophic
Likely	Likely to Occur	61 – 90%	4	Proven public embarrassment with extensive media coverage	High
Moderate	Possible Occurrence	41 – 60%	3	Proven public embarrassment	Medium
Unlikely	May Not Occur	11 – 40%	2	Proven consequences that can be quickly corrected	Low
Rare	Highly Unlikely	0 – 10%	1	Minor consequences that can be contained and quickly addressed	Very Low

3. Risk Treatment

Risk treatment strategies can be classified as:

- Risk Avoidance: Eliminating activities that lead to risk.
- Risk Mitigation: Implementing controls to reduce the likelihood or impact of risks.
- Risk Transfer: Shifting the risk to third parties (e.g., insurance).
- Risk Acceptance: Acknowledging and preparing for risks that cannot be eliminated.

4. Performance of the Risk Management Process

A successful risk management system requires:

- Clear governance structures defining roles and responsibilities.
- Integration with decision-making at all levels of the organization.
- Continuous monitoring to detect emerging risks.

5. Defining Risk Responses

Organizations must establish clear response protocols to address identified risks, including:

- Crisis management plans to handle emergency situations.
- Early warning systems to detect risk indicators.
- Incident response mechanisms to mitigate potential damages.

6. Training and Awareness

A risk management culture can only be effective if employees are trained and aware of their roles in mitigating risks.

- Regular training sessions and simulations enhance preparedness.

- Workshops and guidelines ensure compliance with best practices.

II. Education and Awareness on the Importance of Risk Management Systems

Due to their mandates, authority, and expertise, SAIs are uniquely positioned to influence government entities and public sector organizations. They play a crucial role in raising awareness about governance principles, sound public management, and performance efficiency, including the importance of risk management systems.

This section explores SAIs' role in fostering a risk-aware culture and promoting best practices in risk management within government institutions.

1. Establishing a Risk Awareness Culture

SAIs routinely and continuously identify emerging and evolving risks within the entities they oversee. This process serves as a crucial starting point for encouraging these entities to adopt a structured risk management system based on strategic planning and business continuity frameworks.

By identifying, analyzing, and assessing potential risks that pose real threats within a given institution’s operational environment, SAIs are better positioned to persuade decision-makers of the necessity of implementing a risk management system.

INTOSAI’s principles and standards emphasize that SAIs, as active partners in public sector auditing, should use their knowledge and insights to support public sector reforms and act as a reliable source of independent and objective foresight, helping drive positive change.

Additionally, INTOSAI standards recommend that SAIs engage in meaningful and effective dialogue with stakeholders, highlighting how their work contributes to improving the public sector. While maintaining their independence, SAIs should provide guidance on best practices, maximizing the impact of their audit findings and professional opinions. To achieve this effectively, SAIs must ensure effective communication with audited entities and other relevant stakeholders, keeping them informed of emerging issues and developments.

Beyond their traditional audit roles, such as financial audits, performance audits, compliance audits, and policy evaluations, SAIs play a vital role in preventing corruption, promoting transparency, enforcing governance principles, and ensuring sound public financial management.

In this sense, SAIs can guide, support, and assist government entities in developing and implementing risk management frameworks, helping them enhance their governance and resilience.

The audit and oversight activities conducted by (SAIs) have a -makers toward optimal resource utilization, ensuring compliance with efficiency, effectiveness, and economy principles while reinforcing desirable values and enhancing decision-making.

Regarding risk management awareness, SAIs focus on convincing public sector leaders to integrate risk management into their strategic plans and decision-making processes to achieve organizational goals optimally.

SAIs promote proactive risk management rather than a reactive approach by:

- Encouraging well-planned and well-managed risk-taking.
- Enhancing performance and strategic planning.
- Ensuring a focus on service delivery and continuous improvement.
- Identifying threats and opportunities at all levels.
- Providing reasonable assurance that risks affecting objectives are effectively managed.

Additionally, SAIs emphasize the importance of developing and improving risk policies, strategies, and frameworkswhile supervising and reviewing risk management. They promote a risk-conscious culture, ensuring compliance with risk management policies, procedures, and annual risk certifications.

Public institutions' strategies and operational plans are built on various assumptions, making it crucial to design them with risk considerations in mind. This enhances preparedness, resilience, and performance, reducing negative events and missed opportunities while improving goal achievement and overall efficiency.

2. Promoting Best Practices in Risk Management

As part of their efforts to support and assist government entities in adopting and establishing an effective risk management system, SAIs can provide guidance, advice, and recommendations on best practices. These include: Developing a risk management policy or strategy, establishing a dedicated risk management unit, allocating the necessary financial and human resources, implementing a business continuity management system, conducting monitoring, evaluation, and continuous improvement activities.

a) Developing a Risk Management Policy or Strategy

In response to the challenges faced by countries and governments worldwide economically, socially, politically, and environmentally due to global crises such as climate change, pandemics, and rapid technological advancements, it has become essential to establish mechanisms for anticipating risks and crises. Governments must adopt scientifically developed intervention plans through a risk management system that ensures the continuity of state institutions.

Given the system’s importance in crisis prevention and response efficiency, it is crucial for government entities to adopt this approach to enhance disaster management before, during, and after crises. This system enables:

- Accurate assessment of potential risks that could disrupt government operations.
- Development of intervention plans for managing different types of threats.
- Ensuring business continuity by minimizing downtime.
- Establishing early warning committees for proactive crisis prevention.

Given these factors, it may be necessary to mandate the adoption of a risk management system across public institutions to anticipate and mitigate risks effectively.

b) Creating a Dedicated Risk Management Unit

Arisk and crisis management unit should be established within each government entity, operating under the direct supervision of the head of the institution. Its structure, responsibilities, and procedures should be defined according to the institution's legal framework.

This unit is responsible for monitoring and anticipating crises, implementing the business continuity plan, and evaluating its outcomes. It plays a key role in ensuring preparedness through comprehensive planning, training, response protocols, and communication strategies, strengthening institutional resilience.

The risk management team consists of multidisciplinary experts who ensure effective crisis response, minimizing disruptions and damages.

c) Providing the Necessary Resources for Risk Management

To successfully implement a risk management system, government entities must allocate adequate financial, human, and infrastructural resources.

- **Financial Resources**:
  Government entities must dedicate budgetary allocations for risk management activities and ensure the availability of essential logistical and operational tools for their risk management teams.
- **Human Resources**:
  Institutions should provide qualified personnel capable of managing risks effectively, creating a supportive work environment, and offering continuous training and capacity-building programs to enhance their expertise.

d) Establishing a Business Continuity Management System

A Business Continuity Management System (BCMS) refers to the set of measures and procedures adopted by a government entity to manage crises, minimize their negative impacts, and ensure the continuity of essential services during extreme situations while working toward restoring normal operations based on a pre-established plan.

The approach to developing a Business Continuity Plan (BCP) follows these key steps:

- **Planning**

This phase involves a deep understanding of the government entity, its operational environment, and its legal and regulatory obligations. It includes:

- Leadership engagement and commitment to the continuity policy.

- Defining objectives and allocating necessary resources.

- **Implementation**

Implementation includes activating communication plans, assessing business continuity needs, and conducting:

- Business Impact Analysis (BIA) to evaluate potential operational disruptions.

- Risk Assessment and Management strategies.

- Execution of business continuity and risk mitigation plans.

The OECD Council Recommendation (2014) on risk management highlights the importance of proactive investment in risk prevention and mitigation. Additionally, international standards such as (ISO 22301, ISO 27005, and ISO 27031) provide frameworks for business continuity planning, ensuring organizations enhance crisis response and remote work capabilities.

- **Monitoring, Evaluation, and Improvement**

This primarily involves monitoring and tracking the skill development of individuals responsible for implementing the business continuity plan, overseeing and managing related documentation, conducting regular drills and test exercises, and making necessary revisions and updates. Additionally, it includes measuring, monitoring, and evaluating the internal audit system and continuous improvement processesto ensure efficiency, effectiveness, and sustainability.

III. Contribution to the Evaluation of Risk Management Systems

SAIs work to identify key risks, disasters, and crises, assessing their likelihood and frequency—an essential first step in crisis audit management.

In this context, SAIs ensure that audited entities conduct risk assessments within their operational environments. They verify the existence of an updated risk map, developed based on a thorough risk analysis, and confirm that entities have established a dedicated risk register to document and monitor potential risks.

1. Ensuring the Existence of a Risk Management Policy

There is no doubt that audit reports and recommendations from (SAIs) regarding the evaluation of national and local policies for disaster and crisis management play a crucial role in helping decision-makers take the necessary measures to improve, develop, and correct weaknesses in existing frameworks.

During these audits, SAIs review the legislative frameworks, accountability mechanisms, national requirements, and internal controls in place. For example, they assess national disaster response plans and verify whether:

- Government entities have signed bilateral or multilateral agreements on risk reduction and crisis response.

- Authorities have insured against residual risks to minimize financial losses.

- A dedicated budget or financial allocations exist for implementing risk or disaster management plans.

- A clear framework defining roles, responsibilities, and coordination among stakeholders is in place.

- Non-governmental organizations (NGOs) or international organizations participate in designing and implementing disaster management plans.

2. Ensuring the Existence of a Dedicated Risk Management Structure

In addition to policy evaluation, (SAIs) will audit the assignment of roles and responsibilities within the entity's risk management framework. This includes verifying:

- The identification of risk management structures within the organization.
- Clear designation of powers and responsibilities at each level.
- The availability of qualified and sufficient personnel.
- The establishment of a leadership hierarchy and an efficient information flow between relevant structures.
- Risk analysis and issues related to coordination among different agencies at national, regional, and local levels.
- The existence of a coordination mechanism in case of disasters and whether stakeholders are aware of their responsibilities (Who? What? When? How?).

SAIs may also assess coordination effectiveness based on recent disasters or crisis simulations, using the findings as feedback for correcting errors and addressing weaknesses.

Audit results will guide SAIs in recommending the elimination of redundancies, ensuring optimal resource utilization in terms of efficiency, effectiveness, and cost, and enhancing risk awareness. Additionally, SAIs will highlight possible solutions adopted by other entities and explore alternative communication methods, such as media, satellites, IoT technologies, and emerging communication tools.

3. Risk Assessment and Problem Analysis

As part of their oversight duties, SAIs verify the existence of a modern and systematic information system that provides reliable data for disaster and crisis risk management.

For example, SAIs assess whether government entities use Geographic Information Systems (GIS) to mitigate disaster risks and whether these systems can:

- Evaluate the scale and likelihood of potential losses or damages.
- Provide a comprehensive understanding of risk causes and impacts.

SAIs also ensure that risks related to operational processes, financial flows, and service delivery are identified and tested to determine whether essential services can be maintained during crises.

Additionally, SAIs analyze risks concerning data, documents, and evidence since disasters can severely disrupt institutional performance and jeopardize critical records, leading to risks such as conflicts of interest or overlapping responsibilities.

Moreover, SAIs verify whether funding mechanisms for disaster response are clearly defined and properly managed. This includes:

- Monitoring the receipt, allocation, and expenditure of disaster-related funds from government budgets, local donations, and international aid.
- Ensuring periodic reporting on disaster relief fund distribution.
- Evaluating risk measures related to asset loss due to disasters.

A. Risk Analysis: Issues Related to Early Warning Mechanisms

SAIs verify whether governments and public entities have established early warning systems to anticipate crises and disasters. These systems must be based on risk assessments specific to relevant public institutions to ensure timely response and preparedness.

B. Risk Analysis – Pre-Disaster Activities

SAIs ensure that government entities:

- Promote public awareness and community participation in disaster risk reduction.
- Conduct training programs and public education campaigns on disaster prevention.
- Implement these activities within a structured action plan and establish community communication mechanisms.

C. Risk Analysis – Post-Disaster Activities

SAIs verify that public authorities conduct damage and needs assessments to:

- Identify the impact of emergencies, disasters, or crises.
- Determine the location and needs of victims.
- Ensure that aid and assistance are effectively allocated.

D. Ensuring the Implementation of a Monitoring and Evaluation System

SAIs verify that entities regularly monitor risks and review risk management plans to ensure:

- The effectiveness of risk management systems.
- The efficiency of implemented approaches.
- The completeness and up-to-date status of risk registers.
- The continuous updating of risk assessments to reflect changes in an unstable environment.

E. Ensuring the Establishment of an Effective Communication Policy

SAIs emphasize that communication is a crucial element of crisis management. Providing the public with accurate and transparent information helps maintain control, institutional credibility, and faster crisis resolution.

SAIs also remind officials that crisis communication strategies should focus on:

- Recognizing and addressing the crisis early.
- Being honest and transparent, avoiding misinformation.
- Demonstrating integrity without seeking scapegoats.

Given the dominance of social media, SAIs highlight its impact on public perception. As Jacques Séguéla said, *"The internet can destroy a reputation in seconds."*

IV. The Impact of Reports and Recommendations on Risk Management Practices

This section focuses on analyzing the effectiveness of (SAIs) reports and recommendations and their impact on risk management practices within audited government entities. The findings are based on collected and analyzed data.

SAIs operate in accordance with international standards, such as the INTOSAI Framework of Professional Pronouncements (IFPP) and INTOSAI recommendations, which provide guidelines for risk auditing and management. To be effective, SAIs must fully comply with these standards.

By leveraging these professional guidelines, SAIs conduct risk management audits, whether as dedicated evaluations or as part of broader audits. Their audit programs in this field include:

- Establishing risk management systems within audited entities.
- Identifying, analyzing, and assessing risks by monitoring emerging issues.

1. Contributing to the Establishment and Maintenance of Risk Management Systems

SAIs issue recommendations based on their audit findings, assisting government entities in establishing and improving their risk management systems. They also provide best practices, performance standards, and expert guidance to support these entities.

When SAIs identify the absence of a risk management policy, strategy, or plan and issue recommendations that the audited entity implements, they directly contribute to the creation of a risk management system.

Additionally, SAIs enhance risk management efficiency and sustainability by identifying deficiencies, violations, or deviations from laws, standards, and best practices. Through audit reports and constructive recommendations, they help entities rectify weaknesses and improve overall risk management effectiveness.

Highlighting fraud, corruption, and Risk Management Weaknesses, Alerting officials to fraud, corruption, and mismanagement risks which often increase during crises helps identify vulnerabilities in risk management systems. These risks may include:

- Overestimating damages or manipulating victim numbers.
- Embezzlement, speculation, and misappropriation of assets.
- Failure to deliver essential services properly.

While government entities are primarily responsible for their own risk management, (SAIs) ensure that comprehensive and well-governed risk management policies are in place to mitigate short, medium, and long-term risks.

During audits, SAIs examine:

- Risk-prone areas and whether they have been prioritized and protected.
- Preparedness and mitigation responses to minimize risks.
- Employee awareness of potential risks and their roles in managing them.

SAIs then conduct assessments at all levels using agreed-upon standards to identify gaps, report findings, and recommend corrective actions.

2. Keeping Up with Emerging Issues and Enhancing Knowledge Sharing with Stakeholders

INTOSAI Principle 12 (INTOSAI-P12) states that SAIs must maintain effective communication with audited entities and relevant stakeholders and keep them informed about emerging audit-related issues.

SAIs play a crucial role in ensuring accountability and transparency in risk and crisis management at all stages before, during, and after crises. Their responsibilities include:

- Raising awareness about risk reduction, thus contributing to preventive efforts.
- Assessing the cost-effectiveness of risk mitigation measures.
- Auditing post-crisis assistance, rehabilitation, and recovery efforts, especially in contexts where pre-existing controls fail, operational procedures are not applied, or institutional mechanisms are weak.

The pre-crisis phase focuses on mitigation, prevention, and preparedness, while the post-crisis phase emphasizes recovery, relief, emergency response, and restoring operations.

A crisis is essentially an escalation of an emergency, characterized by increased instability, growing difficulties, and institutional disruptions. Most emergencies have the potential to develop into full-scale crises, making it crucial to recognize early warning signs, even if they seem minor. Once a crisis is identified, alerts must be issued, and crisis management strategies implemented following established standards like ISO 22301.

Crisis management is defined as “a set of organizational methods, techniques, and tools that enable an entity to prepare for, respond to, and learn from a crisis to improve processes and structures with a forward-looking approach.”

A crisis management plan consists of:

- Pre-crisis preparedness: Identifying scenarios and preventive measures.
- Crisis response phase: Managing and controlling the crisis on a day-to-day basis.
- Post-crisis phase: Learning from the event and responding to all crisis dimensions.

A Crisis Risk Management and Business Continuity Guide serves as a reference framework to help public and private institutions enhance resilience and absorb the impact of unexpected threats, shocks, and incidents**.**

It also provides a practical model for implementing business continuity plans**,** enabling organizations to maintain operations, strengthen human and organizational capacities, and ensure sustainability through a structured and flexible approach.

Recent crises, such as COVID-19, have demonstrated that organizations with proactive business continuity measures were the most resilient in mitigating disruptions and reducing risks**.**

V. Challenges and Difficulties

This section examines the various challenges and difficulties that SAIs may face in their role of improving and developing risk management systems within government entities.

These challenges can be categorized into two main areas:

- Challenges at the level of SAIs, related to their own institutional capacity and resources.
- Challenges at the level of audited entities, concerning their ability to implement and maintain effective risk management frameworks.

1. Challenges and Difficulties at the Level of Supreme Audit Institutions

SAIs face multiple challenges, including resource limitations, institutional resistance, and difficulties in implementing recommendations. The main obstacles can be summarized as follows:

- Lack of skilled auditors with the necessary expertise to conduct risk management audits effectively.

- Failure to lead by example, as SAIs themselves may lack a strong risk management culture.

- Absence of auditing methodologies, procedural manuals, and guidelines for evaluating risk management systems.

- Poor planning and misjudgment in selecting the appropriate type of audit (financial, compliance, or performance).

- Insufficient understanding of the audited entity’s operational environment, hindering proper risk assessment.

- Complexity in identifying key stakeholders and evaluating information systems used in risk management.

- Inability to recognize, analyze, and address risks effectively within audited entities.

- Challenges in detecting fraud, misstatements, or misleading information during risk analysis.

- Disagreement with audited entities on acceptable levels of risk exposure and mitigation measures.

- Difficulty in assessing the quality of risk identification processes within entities.

- Challenges in providing practical, cost-effective, and actionable recommendations aligned with organizational goals.

2. Challenges and Difficulties at the Level of Audited Entities

Certain institutional challenges within government entities may hinder SAIs from effectively improving risk management systems. These challenges include:

- Human judgment errors in risk-related decision-making and control design.
- Lack of a unified risk management framework, making it difficult to assess risk tolerance levels.
- Inability to adapt to rapid environmental changes due to inflexibility.
- Limited awareness and resistance to adopting a risk management culture.
- Non-compliance with SAIs' guidance and recommendations.
- Lack of training, capacity building, and professional development in risk management.
- Weak risk governance, including lack of clear vision, transparency, and strategic direction.
- Failure to prioritize critical risks, particularly hidden risks due to poor risk assessment.
- Weak internal controls, leading to inadequate monitoring and risk mitigation.
- General inflexibility in public sector institutions, affecting responsiveness.
- Lack of coordination among decision-making and implementation levels in risk management.

Conclusion

In an unstable economic, social, political, and environmental landscape, risks and crises pose increasing challenges for public institutions. It is up to leaders and decision-makers to prioritize risk management, crisis response, and business continuity strategies.

According to the 2023 INTOSAI Development Initiative (IDI) Global Assessment Report, 58% of SAIs have implemented emergency preparedness and continuity plans, up from 53% in 2020 a shift largely driven by the COVID-19 pandemic. However, 42% of SAIs still lack such plans, particularly in low-income countries. INTOSAI Principle 12 emphasizes that SAIs should set an example for public sector governance, making it essential for them to apply risk management to their own operations.

Establishing a business continuity system is now a strategic priority. Government entities must be able to maintain operations, protect data, and safeguard their reputations, as failing to meet public expectations could have severe consequences.

However, successful risk and business continuity management depends on more than just implementing solutions—it requires strong leadership and commitment. While many regulatory frameworks do not mandate risk management and continuity planning, recent crises, including COVID-19, highlight the need for a strategic commitment to integrating these principles, especially in critical public sectors.

Effective governance and public financial management require embedding a culture of crisis management, where public entities adopt risk management systems to enhance their resilience. A well-developed system enables public officials and stakeholders to overcome crises through proactive engagement at all levels.

Training programs and clearly defined roles during crises must be continuously maintained, ensuring readiness for emergency response and recovery. Establishing a business continuity

system is not only a tool for institutional resilience but also an opportunity to strengthen public sector sustainability and adaptability.

Finally, the concept of crisis itself suggests opportunity. In Greek (krisis), it means the ability to make decisions, while in Chinese (危机 wēi jī), it represents both danger and opportunity. The Petit Robert dictionary defines a crisis as a critical turning point requiring decisive action. This implies that risks can present opportunities, but success depends on adopting a mindset focused on transforming crises into positive outcomes.

Recommendations

Based on the findings of this study and the potential role of SAIs in enhancing risk management systems within government entities, the following recommendations can be proposed:

- SAIs, especially in the Arab region, should adopt risk management policies and implement governance-based systems to strengthen their resilience and accountability, setting an example in line with INTOSAI Principle 12.
- SAIs should leverage the INTOSAI Development Initiative (IDI) CRISP program to enhance their capabilities in risk management, business continuity, and crisis management.
- SAIs must increase audits on risk management systems within public entities, ensuring high-value, high-impact oversight based on recognized standards and best practices.
- Integrating risk management into performance evaluation frameworks would allow SAIs to better track strategy implementation, improve decision-making, and promote risk awareness.
- SAIs should intensify training programs to enhance auditors' skills, knowledge, and awareness of risk management.
- Given that disaster and crisis risk management involves multiple stakeholders from the government, private sector, and civil society, auditors must understand the legal and organizational frameworks in which these entities operate.
- SAIs should exchange knowledge and expertise both internally and with external specialists to improve risk assessments.
- Conducting risk assessments within audit environments is crucial for identifying high-risk areas, given the complexity and distinct nature of the public sector compared to the private sector.
- SAIs should expand audits on government IT systems and evaluate internal control frameworks to help improve risk management governance.
- Auditors should adopt a professional skepticism approach to identify fraud risks, including data manipulation during audits.
- SAIs must adhere to international auditing standards, INTOSAI’s guidance framework, and specialized risk management guidelines to ensure quality oversight.
- SAIs should actively engage in awareness and education efforts on risk management for government entities, viewing this as part of their governance responsibilities rather than interference in management.
- Government entities should engage positively with SAIs' findings and implement recommendations to strengthen risk management.
- Consideration should be given to establishing a legal framework requiring public institutions to develop risk management policies and systems, or at least formalizing risk and crisis management standards in an initial phase.

References

- INTOSAI Development Initiative (IDI) Documents on strengthening SAIs' capabilities in risk management, business continuity, and crisis management (CRISP).
- INTOSAI Principle 12 (INTOSAI-P12): The Value and Benefits of Supreme Audit Institutions – Making a Difference in Citizens' Lives.
- INTOSAI GOV 9100: Guidelines for Public Sector Internal Control Standards.
- GUID 5330: Disaster Management Audit Guide.
- ISO 31000 (2018): Risk Management Guidelines.
- INTOSAI Development Initiative (IDI) Reports: "Global SAI Assessment 2020 & 2023".
- ISO 22361: Crisis Management Standards.
- Business Continuity Management (National Emergency and Disaster Management Authority – UAE).
- Risk Management Guide (Consumer Protection Authority – Oman).
- Simon Ekin & Olivier Vélin: *Crisis Management - Corporate Response* (EFE 2006).

International Standards & Best Practices

- ISO 22301 (2019): Business Continuity Management System – Requirements.
- ISO 22313 (2020): Business Continuity Management System – Guidelines.
- ISO 31000 (2018): Risk Management – Guidelines.
- ISO 27005 (2018): Information Security Risk Management.
- ISO 27031 (2011): IT Security Techniques – Business Continuity Readiness.
- Business Continuity Planning Guide (SGDSN – France).
- Continuity & Recovery Planning Guide (DGSSI – Morocco).
- Essential Services Continuity Planning Guide (DRP Québec).
- ISO 22031-Based Business Continuity Planning (Adenium-brg).
- Implementation Guide for Business Continuity Management System (CCA – France).
- Business Continuity Plans (AMRAE – France).
- Business Continuity Management (GTAG –IIA).
- Enterprise Business Continuity Planning Guide (ISST).
- COVID-19 Pandemic Business Continuity Plan in Tunisia (UGTT).
- COSO ERM: Enterprise Risk Management Framework.

Research Summary: The Role of Supreme Audit Institutions in Developing Risk Management Systems in Government Entities

Throughout history, societies worldwide have faced various risks, crises, and disasters that disrupt government activities and hinder public service delivery. Effective governance and public financial management require governments to anticipate and mitigate risks, reducing reliance on improvised emergency solutions.

Given the diverse threats to government entities, establishing robust risk management systems is a critical priority. This research explores how Supreme Audit Institutions (SAIs) contribute to strengthening risk management frameworks, the tools they use to enhance risk control, their role in evaluating risk management effectiveness, and the impact of their reports and recommendations on government practices.

This study aimed to:

1. Highlight the role of SAIs in raising awareness about risk management.
2. Assess SAIs' contributions to evaluating government risk management systems.
3. Examine the impact of SAIs' reports and recommendations on risk management practices.
4. Identify challenges faced by SAIs in improving risk management frameworks.

The research is divided into five sections, covering risk management principles, SAIs' role in awareness and evaluation, their impact, and existing challenges. One key finding is that SAIs should actively promote a risk management culture, helping public entities view risks as opportunities. Therefore, SAIs should embrace their governance role without considering it interference in management.