The State Audit Bureau

State of Kuwait

The Role of Supreme Audit Institutions in Developing Risk Management Systems in Government Entities (*Field Study*)

A paper submitted to the General Secretariat of The Arab Organization for Supreme Audit Institutions (ARABOSAI) as part of participation in the 14th Scientific Research Audit Competition

Prepared by:

Dr. Abdulrahman Ahmed Al-Mukhaizeem

PhD in Accounting and Auditing

Technical Office Expert, the State Audit Bureau of Kuwait

2024

This award-winning research paper was originally written in ***Arabic*** *and has been translated into* ***English*** *for broader accessibility. In case of any discrepancies between the translated and original versions, the original Arabic version shall prevail.*

Translation Section – The State Audit Bureau of Kuwait
March 2025 ©

Acknowledgments

The Prophet of Allah (PBUH) said:

"Whoever treads a path seeking knowledge, Allah will ease his path to Paradise."

With the grace and success of Allah, I have concluded this paper, which, based on my circumstances, represents a humble effort. With the blessing of Almighty Allah, I hope this research will provide a valuable source of instrumental, practical, and qualitative perception that will contribute to the development of supreme audit institutions (SAIs).

I also extend my appreciation and gratitude to the General Secretariat of the Arab Organization of Supreme Audit Institutions (ARABOSAI) for supporting the notion of this scientific research. Additionally, my deepest appreciation goes to the President and the Undersecretary of the State Audit Bureau of Kuwait (SAB), along with my colleagues, for their support and rewarding guidance throughout the course of this study.

Allah is the arbiter of success

Table of Contents

List of Tables

Abstract

The research presented several important chapters that discussed **the role of SAIs in developing risk management systems in government entities**. Chapter 1 addresses the general framework of the study, which revolves around two topics. Theme 1 discusses previous studies, while Theme 2 explores the research's methodological framework. It describes and details the methods and approaches used. Chapter 2 explores the theoretical framework of the research. It includes four themes. The first theme of Chapter 2 revolves around **risk management tools in the face of changeable conditions**, while the second covers the **role of internal audit in raising the efficiency of risk management.** The third theme focuses on **SAIs and their role in implementing risk management**. On the other hand, the fourth theme tackles **the use of artificial intelligence and machine learning technologies in risk management**. Chapter 3 showcases **the field study** and the survey analysis using SPSS statistical software.

In light of the theoretical and practical results of the research, recommendations may be made regarding the use of leading manual and automated systems for risk management. The use of said systems may contribute to overcoming limitations and difficulties. The researcher has reached a number of recommendations, which can be summarized as follows:

1. It is important to consider risk management systems in government entities and pay heed to their advancement, as these systems are one of the main pillars for facing the changeable risks that these departments are likely to be exposed to.

2. There is a need for officials to be aware that risk management is centered on executive management, as modern internal audits provide assurance to senior management regarding the efficiency and effectiveness of risk management.
3. It is necessary to develop a comprehensive program to ensure and improve the quality of internal audit and risk management, considering audit risks and the risks arising from the organization, whether internal or external.
4. Auditors, external consultants, and SAIs need to commit to a regular evaluation of the internal audit and risk management methods due to their experience and independence from the organization.
5. It is vital to benefit from modern technologies and their positive outcomes. AI and machine learning have created a progressive environment in developing risk management. This is showcased through precise risk analysis, accurate prediction, and enhanced audit efficiency. These technologies can process large quantities of data promptly and unerringly. They also contribute to the early detection of potential risks, which reduces human errors and enhances a rapid response to emerging challenges in the work environment.
6. Upgrading and ensuring the preparedness of electronic systems' infrastructure, as well as protection and security programs, facilitate keeping pace with modern technologies while helping confront evolved viruses.

7. Issuing laws, legislations, and international standards to conduct risk management. That is to provide legal authority when implemented and comply with the automated systems considering the upgrade of such systems.

8. There is a need to issue a comprehensive guideline that regulates the policies of AI use to ensure favorable incomes and develop rules for professional and ethical conduct to achieve the objectives of control over risk management.
9. It is important to regularly organize training courses, systematic and practical orientations, and technical conferences regarding the latest trends in AI and Machine Learning technologies to develop risk management systems.
10. There is a need to integrate AI technologies into SAIs to achieve an advanced and more proactive risk management system in a way that enhances the sustainability and success of organizations. It is expected to witness further applications that enhance the competencies of risk management, making them more incorporated in a manner that contributes to enhancing long-term sustainability and prosperity.

Glossary of Terms

1. Government, Public, and Private Sectors [1]:

- **Government Sector:** It encompasses government departments and ministries that play a primary role within the state, managing specific areas such as security, defense, judiciary, education, and health. These ministries are subject to civil service and military systems and do not enjoy financial or administrative independence. They are also subject to the supervisory standards and financial regulations applied by the government as their expenses are financed by the state budget.

- **Public Sector:** It is a term used to describe a segment of the state economy. This sector encompasses government-owned enterprises that manage economic activities on behalf of the government. The capital of such enterprises may be owned wholly or partially by the state. Private sector companies are known for their resilience and administrative exemption from routine, as they operate under the laws that apply to the private sector, such as Kuwait Airways Company (KAC), Livestock Transport and Trading Company (Al Mawashi), and Kuwait Investment Company (KIC).

- **Private Sector:** It is the business sector associated with institutions and companies owned by individuals in a personal capacity and not affiliated with the State government or any of its institutions.

[1] Riyadh Economic Forum. (2006). *Developing the Relationship between the Government Sector, the Public Sector, and the Private Sector*.

2. **Senior Management [2]:** It is the highest administrative authority within a concerned entity (e.g., Minister, Undersecretary, Head of Department, Board of Directors, etc.)
3. **Audit Committee:** A committee formed by an entity's senior management to monitor the business of internal and external audits.
4. **Professional Competence of Internal Auditor [3]:** The auditor's ability to invest and make optimal use of his/her versatile capabilities in the best possible way. It includes the auditor's commitment to the technical and ethical standards of the profession, his/her constant endeavor to improve the efficiency of his/her job, fulfill his/her professional responsibility to the fullest, and strive for excellence in conducting professional responsibilities proficiently and devotionally.

[2] Abu Dhabi Accountability Authority. (2010). *Audit Management Manual.* Retrieved from https://shorturl.at/gzDFJ.

[3] Kazem, S. (2022). *The Scientific and Professional Competence of the Internal Auditor and Their Impact on Reducing Creative Accounting Practices to Produce Reliable Financial Reports* (Master’s thesis, College of Administration and Economics, University of Karbala). Retrieved from https://shorturl.at/TQyY1.

Chapter 1: General Framework

- **Theme 1: Previous Studies**

- **Theme 2: Methodological Framework of the Study**

Chapter 1: General Framework

Theme 1: Previous Studies

Introduction

Supreme Audit Institutions (SAIs) aspire to reinforce their audit capacity to keep pace with the latest developments per the best international professional audit practices. Such aspiration started when a growing interest in risk management was taken, especially after a series of global crises took a toll on economic units- of all kinds- for failing to prioritize internal and external risks surrounding such units. The Arab Organization of Supreme Audit Institutions (ARABOSAI) seeks to develop its members' control capacities to ensure that auditees are subject to the best professional audit practices.

Based on the above, this chapter presents the general framework of the study divided into two themes. The first (Theme 1) discusses previous studies related to SAIs' role in developing risk management systems in government entities. The second theme (Theme 2) revolves around the methodological framework used in this study. It details the study's research problem, questions, hypotheses, objectives, significance, and approach.

Theme 1: Previous Studies

Article (9) of this research competition stipulates that the submitted scientific papers must not exceed 25000 words. Therefore, it is only practical to exhibit the studies contemplated in this paper, which are:

1. Abdullah, S. (2023). *A Proposal on Disclosure of Accounting Information for Risk Management in the Egyptian Banks: An Applied Study in the Egyptian Context.* [In Arabic]
2. Alazemi, K. (2023). *The Impact of IT and Open Accounting Records Method on Improving Risk Management of Financial Information within Supply Chains for Cost Reduction.* [In Arabic]
3. Mohammed, M. E. (2019). *The Role of Internal Auditing in Analyzing and Enhancing the Levels of Risk Management and Its Impact on Organizational Performance and Reputation.* [In Arabic]
4. Abdullah, F. (2019). *Assessing the Impact of Internal Auditing to Ensure the Compliance of Banks with Sound Practices.* [In Arabic]
5. Amro, A. (2019). *A Proposed Framework for Enhancing the Role of Internal Audit Systems in Light of Recent Professional Guidelines to Promote and Support Risk Management.* [In Arabic]
6. Al-Fadhli, K., et al. (2022). *The Role of Internal Auditors in Assessing the Overall Risk Management of Business Organizations and Acquiring Practical Guidelines from Public and Regional Departments within Banks of Benghazi City.* [In Arabic]
7. Al-Batoush, et al. (2015). *The Role of Audit Committees in Improving Internal Audit Quality of Risk Management in Jordanian Electricity Companies.* [In Arabic]

This paper is dissimilar to the previous studies for the following reasons:

Risk management systems are essential in ensuring business continuity and success in various institutions, including government entities.

Despite the growing awareness of the significance of risk management, the existing studies and research papers heavily rely on investigating commercial and banking corporations subject to the control and supervision of the Capital Markets Authority in general. Nevertheless, previous studies have dealt with important elements mentioned in this current study, such as implementing and strengthening risk management. This paper details aspects of risk management systems in government entities and SAIs' role in developing these systems. In conformity with the researcher's perspective, these points demonstrate an innovative and meaningful contribution to the body of literature as this study attempts to detail.

Theme 2: Methodological Framework

Introduction

With the escalating pace of economic proceedings, the need to expand and grow business enterprises across continents has emerged. In conjunction with the increasing complexity and diversity of operational processes, especially in the era of rapid digital transformation, it has become necessary to enhance risk systems to ensure the fulfillment of strategic objectives and sustainable development. The study of risks is a critical issue that concerns societies, specifically after the series of successive financial, banking, and health crises that have struck the world during the past decades. Such critical times have shown the magnitude of having a comprehensive approach and an effective risk management system in institutions to ensure their continuity and fulfillment of objectives.

In this vein, risk management is considered a semi-ambiguous concept in the government sector as it fails to enjoy the attention it requires within organizational structures. The prevailing belief is that the government sector operates on the basis of legal frameworks, regulations, and directives; therefore, there is no urgent need to assess these risks. However, several challenges associated with this notion prevent institutions from fulfilling their goals. Failing to precisely detail conventional operations, the rigidness and lack of upgrade of such directives while repeatedly and formally embracing them make them inappropriate to face the surrounding irregularities. This notion has become outdated, notably after the rapid changes witnessed by institutions due to the successive developments in software, electronic computer systems, digital transformations, and the emergence of AI that advanced the internal and external environments of business.[4]

[4] Mahdi, N. & Al-Jabouri, N. (2016*). Enhancing the Performance of Public Internal Audit Units within the Government Sector in Light of the Risk Management Approach*. Journal of Administration and Economics. Volume 39. Issue 190.

Setting and developing mechanisms to fulfill the goals and meet beneficiaries' expectations towards its services, as well as applying early performance indicators to detect and address advert situations in a timely manner, shall help the government sector enhance and improve its performance. Risk management is considered one of the most significant indicators that strives to guarantee the continuity of operations in all fields. Its significance lies in its ability to identify and assess potential risks that may impact the objectives and proceedings of the government sector. It also revolves around taking necessary measures to reduce or adapt effectively to such risks by applying a comprehensive and integrated approach to risk management.

During the beginning of the current century, the internal audit profession witnessed tremendous developments, mainly after the Institute of Internal Auditors (IIA) incorporated the task of evaluating the effectiveness of risk management within Clause 2120 of its International Standards for the Professional Practice of Internal Auditing. Introducing this requirement ensures that institutions meet their strategic objectives, improve the use of resources, and enhance governance, transparency, accountability, and the trust of citizens.

SAIs play an essential role in monitoring and evaluating internal audits. SAIs may be considered crucial partners in enhancing the efficiency and effectiveness of risk management in the government sector. That is done by developing the necessary policies and procedures to effectively and innovatively face risks for a better implementation of internal audits.

Considering the aforementioned, this study attempts to explore and analyze the role of SAIs in developing risk management systems in government entities. Such systems improve government performance, efficiently achieve strategic objectives, and effectively protect and utilize public property.

Research Problem

Risk management has become the subject of attention for scholars, as it was recognized as a legitimate discipline in the 1950s. It was directly linked to insurance companies in an attempt to abstain people from disasters and damages associated with the misappropriation of property or exposure to accidents. Institutions are exposed to reputational risks in other domains, most notably in the business and financial sectors. Government entities have taken significant actions in response to the COVID-19 pandemic and with the advancement and growing use of computerization, digitalization, and algorithms. The pandemic has adversely impacted all economic, social, and healthy life forms. Consequently, governments were prompted to engage in risk management on a larger scale to improve public policy management and effectively achieve its goals towards enhancing its response to the growing challenges and risks of the modern era.

Moreover, internal audits play a pivotal role in reducing risks. IIA specified that risk management assessment is within the duties and competencies of internal auditors. Clause 2120 of its IPPF Standards states, “The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.” Likewise, SAIs play a critical role in supporting the internal audit function by evaluating the adequacy of internal control systems, issuing relevant directives and guidelines, reviewing applicable reports, and providing feedback on how to improve said function to enhance its efficiency and effectiveness and promote risk management in the government sector.

In light of the above, the research problem lies in the following main question:

How can SAIs enhance their role in developing risk management systems by assessing the capacity of internal audits to reduce risks in government entities and ensure effective operational control?

A number of sub-questions arose from this main question:

Sub-question 1: *Is there a statistically significant relationship at the significance level of (a=0.05) between auditors' academic qualifications and professional competence and the development of risk management systems in government entities?*

Sub-question 2: *Is there a statistically significant relationship at the significance level (a=0.05) between the review of internal audit management systems and regulations and the development of risk management systems in government entities?*

Sub-question 3: *Is there a statistically significant relationship at the significance level (a=0.05) between internal audit procedures and risk reduction in government entities?*

Sub-question 4: *Is there a statistically significant relationship at the significance level (a=0.05) between using AI and the development of risk management systems in government entities?*

Research Signification

As far as the researcher is aware, the importance of this research stems from the scarcity of studies on risk management in the government sector. The topic is original in the sense that it clarifies the latest norms within the field of risk management. This paper sheds light on SAIs' role in developing risk management systems by evaluating, implementing, and utilizing internal audits as feedback instruments that contribute to fulfilling the government entities' vision to add value and enhance their performance. This would aid in reinforcing their technical capabilities to perform their responsibilities and promote stability.

This research also carries a practical significance as it attempts to contribute to drawing SAIs' attention towards AI and discuss ways to benefit from modern technologies. Algorithms, machine learning, and systematic instruments simulating human mental capabilities are all examples of such technologies that are used to improve the accuracy and efficiency of risk management. This paper enriches the body of literature with contemporary and progressive knowledge that will serve both researchers and the audit profession.

Research Hypotheses

Hypothesis (1): There is no statistically significant relationship at the significance level (a=0.05) between auditors’ academic qualifications and professional competence and the development of risk management systems in government entities.

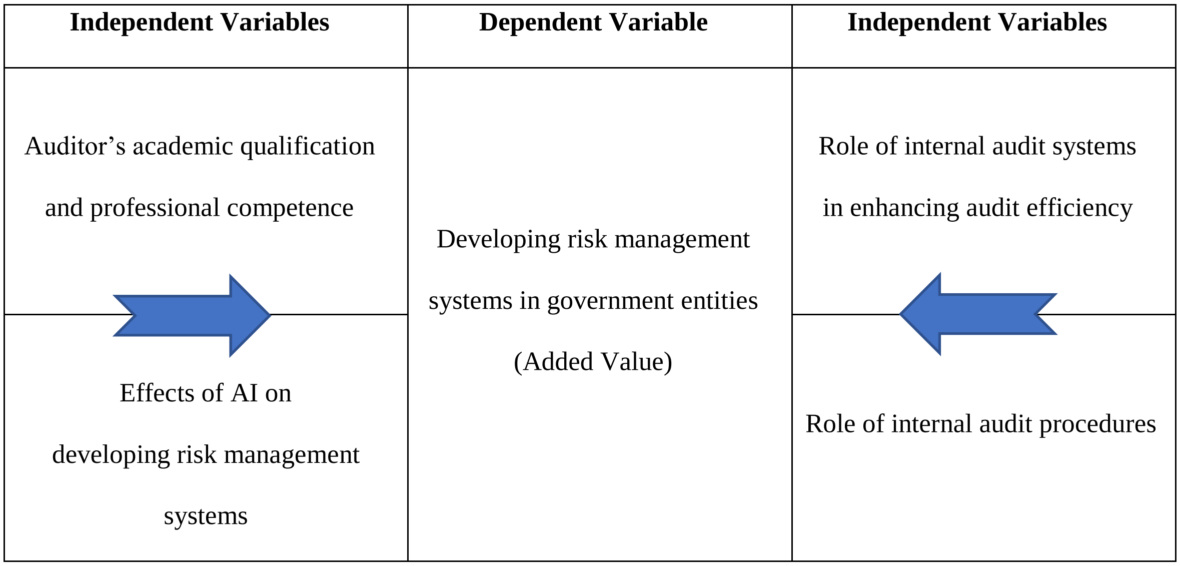
Hypothesis (2): There is no statistically significant relationship at the significance level (a = 0.05) between the review of internal audit management systems and regulations and the development of risk management systems in government entities.

Hypothesis (3): There is no statistically significant relationship at the significance level (a = 0.05) between internal audit procedures and risk reduction in government entities.

Hypothesis (4): There is no statistically significant relationship at the significance level (a = 0.05) between using AI and the development of risk management systems in government entities.

Research Model

To achieve the purpose of the study and reach its specific objectives, the researcher relied on a model to identify whether there is a correlation between the independent and dependent variables. The following figure shows the correlations between these variables.



Independent Variables	Dependent Variable	Independent Variables
Auditor’s academic qualification and professional competence	Developing risk management systems in government entities (Added Value)	Role of internal audit systems in enhancing audit efficiency
Effects of AI on developing risk management systems		Role of internal audit procedures

Figure 1

Research Objectives

In light of the lack of field studies on risk management in government entities, the researcher aims to achieve the following:

- Introduce the concept of risk management, its significance, and mechanisms.
- Formulate intellectual and theoretical aspects of risk management from a scientific perspective and explore to what extent they can be utilized to improve services and protect public properties, especially under the latest and most changeable conditions.

- Demonstrate the significance of SAIs in enhancing and improving internal audits in government entities through better monitoring of risk management and compliance with the approved standards and policies.
- Demonstrate the relevance of AI in developing risk management systems. Utilizing AI technologies improves prediction accuracy, accelerates analysis, and provides innovative solutions to contemporary challenges.
- Define SAIs' role in developing risk management systems in government entities to enhance efficiency and transparency and ensure compliance with the applied standards.
- Evaluate SAIs' effectiveness in supporting government entities in implementing risk management systems.
- Test the hypotheses, draw conclusions, and develop recommendations.
- Submit proposals to improve SAIs' role in supporting the development of risk management systems in government entities.

Research Methodology

To achieve the research objective, a historical documentary approach was used. This approach relies on collecting data and facts by resorting to periodicals, books, articles, and websites relevant to the research themes. In addition, a descriptive or exploratory approach was also used. This approach revolves around using questionnaires to collect data from specialists on the subject matter. It aims to clarify, showcase, and contemplate SAIs' role in developing risk management systems in government entities.

Research Limitations

The study was constrained by the following:

- **Objective limits:**

- The research has been developed for the ARABOSAI's 14th Scientific Audit Research Competition.
- This study was limited to exploring SAIs' role in developing risk management systems in government entities.

- **Spatial limits:**

- The study was limited to auditors of Arab SAIs.
- Using desk research, scientific journals, websites, and access to all information to identify SAIs' role in developing risk management systems in government entities.

- **Time Limitations:**

- This study was conducted from 31/1/2024 until 30/6/2024.

Research Plan

The research plan included the following:

- **Chapter 1** addresses the general framework of the study. It contains two themes; the first revolves around previous studies, while the second deals with the study's methodological framework. This theme presents an introduction and an illustration of the research problem, hypotheses, objectives, significance, limitations, methodology, and plan.

- **Chapter 2** deals with the research theoretical framework, which includes four themes. The first discusses risk management instruments in the face of changeable conditions, while the second discusses internal audits’ role in enhancing risk management efficiency. The third theme examines the role of SAIs in implementing risk management, and the fourth explores the use of AI and Machine Learning technology in the field of risk management.
- **Chapter 3** discusses the procedures of the field study and evaluates the validity of the hypotheses while drawing conclusions and recommendations.

Chapter 2: Theoretical Framework

- **Theme 1 - Risk Management Tools in the Face of Changeable Conditions**

- **Theme 2: The Role of Internal Auditing in Enhancing the Efficiency of Risk Management**

- **Theme 3: Supreme Audit Institutions and Their Role in Enhancing Risk Management**

- **Theme 4 :The Use of Artificial Intelligence and Machine Learning Technologies in Risk Management**

Chapter 2: Theoretical Framework

Theme 1: Risk Management Tools in the Face of Changeable Conditions

Preface

Societies face continuous and renewed risks in different fields such as health, environment, economy, and politics. As technology advances in various areas of life, the risks resulting from its use are increasing, prompting organizations to focus on risk management as one of the main pillars on which modern business depends. Accordingly, this study will discuss the concepts of risk and its management in the face of changeable conditions, as follows: [5]

1.1. The Concept of Risk

This term is widely used by the general public. It is coined to describe everything that is unpleasant to oneself. It is in every situation or condition where the potential for loss or damage is found. Whether this damage is material, physical, or even psychological, the risk can be intentional or accidental and may stem from natural conditions or manmade.[6]

1.2. Risk from a Social Science Perspective

The study of risk is the subject of many studies in social sciences, including Psychology, Statistics, Economics, Financial Management, and Actuarial Science. Each of these disciplines

[5] Tubasi, A. *Risk Management in Third Sector Organizations*. Retrieved from https://shorturl.at/bfhzB.

[6] Qandous, A. (2018). *Hedging and Risk Management: A Financial Approach*. E-Kutub Ltd.

defines its concept of risk in a unique direction. Despite all the theoretical complexities surrounding the study of risk, its significance does not outshine what these disciplines have illustrated. In this paper, the notion of risk from various disciplines is discussed, as follows:

- **Risk from a Legal Perspective**: It is the possibility of a future or uncertain incident occurring beyond the control of the contracting parties, potentially leading to harm or loss.

- **Risk from an Actuarial Perspective**: Risk is a potential subsequent incident that does not depend on the will of either party between whom the contract was made.
- **Risk from an Audit Perspective**: The likelihood of an auditor issuing an unqualified opinion on a case that involves fraud or serious misplacements.

- **Risk from a Financial Perspective**: The potential of facing future deviation leading to results that revoke what is expected and desired. It is the uncertainty of the succeeding financial outcome due to a decision taken at present based on the results collected by examining the aspects of former natural phenomena. [7]

- **Risk from an Economics Perspective:** Risk in Economics has several definitions, to mention a few:

  - Predicting variants in return between what was planned and what was expected.
  - The likelihood that the expected return will not be achieved.
  - A state of measurable uncertainty. [8]

[7] Saudi Center for Financial and Performance Audit. *Risk-Based Training Kit*. General Court of Audit of Saudi Arabia. Retrieved from https://shorturl.at/glxRX.

[8] Hammad, T. A. (2003). *Risk Management*. Al-Dar Al-Jami'iyah Press.

It can be argued that risk, regardless of its nature, is an integral part of contemporary life. Due to diversified activities, it has continued to grow until it has become an inherent feature of the modern world. This correlation makes it impossible to eliminate risks. However, it does not necessarily mean that risk impacts cannot be managed and mitigated with policies and strategies.

1.3. The Development of Risk Management

The term "Risk Management" was coined in the 1950s, particularly in a 1956 publication by Harvard Business Review. It has emphasized the importance of having an official within an organization to be in charge of risk management. The idea evolved with the establishment of the Institute for Risk Research in New York in 1932. Therefore, the National Insurance Buyers Association was founded in the 1950s, eventually becoming the American Society for Insurance Management.

The 1960s, on the other hand, witnessed a revolution in risk management, particularly after the invention of financial instruments that enabled the redistribution of financial risks according to investors' preferences. Changing the name of the Association of Insurance Buyers to the Risk Management and Insurance Association in 1975 contributed to the dissemination and spreading of risk management.[9]

Initially, risk management focused on industrial projects and was mainly associated with security and safety. Yet, in recent years, risk management has evolved into a scientific discipline

[9] - Al-Abbas, M. (2021). *Risk Management: How Has the Concept Evolved?*, Al-Eqtisadiah Newspaper. Retrieved from https://shorturl.at/prtPU

- Kamal, H. *What do you know about risk management?*. Edarati Magazine. Retrieved from www.edaratimagazine.com that discusses all types of risks, whether material risks (e.g., business losses) or moral risks (e.g., loss of reputation or lack of organizational resilience). Therefore, risk management has become a vital necessity for every institution.

1.4. Risk Management Concept

Risk management is a scientific method or approach to managing risk. It involves anticipating potential incidental losses and developing and implementing measures that will minimize the likelihood or financial impact of losses.

IIA has defined risk management as “a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.”

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) also clarified the main concepts of enterprise risk management (ERM) under its ERM Integrated Framework, stating that it is a process conducted by the organization's board of directors, management, and individuals to implement the strategy developed across the organization to identify potential events that may affect its performance to have it within the acceptable margin of risks.[10]

Therefore, risk management can be defined as a systematic and scientific approach for effectively identifying, evaluating, organizing, mitigating, and following up on risks according to proper strategies. This approach seeks to balance the risks that can be accepted

[10] Abdi, A. (2023). *The Contribution of Internal Audit to the Activation of Risk Management: Field Study*. Ibn Khaldoun University – Tiaret.

and those that are expected to support and achieve the organization's goals and strategy in a secure and sustainable manner.

1.5. Difference between Risk Management and Crisis Management

Risk and crisis management are two types of strategic management within an organization. Although they may share some aspects, they differ, as discussed below.

A. Risk Management:

- focuses on analyzing and assessing the potential risks that an organization may face in the future;
- aims to promptly identify and understand risks and develop plans to address and reduce their impact;
- analyzes and classifies risks and estimates their impact and likelihood of occurrence;
- implements measures and procedures to reduce risks and develop strategies to deal with them effectively; and
- includes activities such as insurance, organizing systems and procedures, and applying security and safety standards.

B. Crisis Management:

- deals with unforeseen and unfortunate events that threaten business continuity;
- requires an immediate response and coordination between all resources and efforts to deal with the crisis and reduce the damage;
- includes natural disasters (e.g., earthquakes and floods), environmental crises, fires, and health crises (e.g., epidemics);

- requires a pre-defined crisis plan that outlines the necessary actions and responsibilities in the event of a crisis; and
- aims to restore life back to normal and provide support and assistance to those affected.[11]

It can be concluded that risk management and crisis management complement each other in the preparedness and response to risks. To identify the difference between the two, risk is a concept that is more related to uncertainty. As for crisis, it is a notion that expresses something that has already happened, and the loss resulting from the risk is considered a potentiality. As for the crisis, the loss is certain to occur and the impact of the crisis is broader than the impact of the risk.[12]

1.6. Importance of Risk Management

Risk management is vital for any organization seeking to achieve success and sustainability in a challenging and potentially risky work environment. The following are the most prominent points that illustrate the importance of risk management:

a) **Anticipating potential problems:** This approach focuses on anticipating the likelihood of potential problems, identifying challenges in advance, and developing proactive plans to preserve time and money to ensure business continuity and long-term success.

[11] https://shorturl.at/eozK0

[12] Ahmed, A. (2024, May). *Experts Prepare for More in 2018: "Risk Management Challenges under Control"*. IPA Magazine, Issue 210. Retrieved from https://shorturl.at/Nu50E

b) **Avoiding catastrophic events:** Risk management includes preparedness for all types of risks, including minor disturbances that may affect daily business, with a focus on catastrophic events.

c) **Making better decisions:** Under this approach, potential risk factors are discussed in detail, especially when entities launch new policies, expand the scope of their activities, or deal with different challenges. It is important to help them develop an integrated framework that allows them to avoid these risks, which contributes to making better decisions and achieving their goals more successfully.

d) **Enabling government entities to achieve their objectives:** Government entities face multiple challenges in an ever-changing environment. They have to provide services efficiently and effectively to citizens while concurrently dealing with political, economic, and social accountability. In this context, risk management plays a critical role in adopting customized strategies to deal with risks. It enhances sustainability and stability in providing government services and improves efficiency and effectiveness in the use of available resources. Risk management promotes confidence and transparency among citizens. With its implementation, it becomes easier for organizations to effectively adapt to new challenges, whether related to technology, economic changes, or social conditions.

e) **Improving business methods:** Risk management requires collecting more information on a daily basis to analyze the business and search for matters that may be exposed to risks. This contributes to the structuring of methods that improve the quality of business.

f) **Better budgeting:** Risk management helps organizations manage their financial resources more effectively by examining the risks of financial statements and reducing the loss and waste in public property.

g) **Positive impact at the level of the entity:** It contributes to eliminating redundant operations, ensures the effective use of employees, reduces theft, and increases efficiency in providing services to the citizens.

h) **Increasing customer satisfaction:** Risk management in government entities aims to predict and solve potential problems before they occur. This approach contributes to improving customer experiences, increasing their satisfaction and loyalty. Therefore, it reflects the entity's eagerness to reach customer satisfaction**.** When a government entity successfully prevents potential problems, its reputation is enhanced due to positive feedback from customers.

i) **Securing the branding of a government entity:** It is a concept that employees, citizens, and society can trust and look to in providing services or activities and in preserving their public interests. Entities should develop a risk management plan tailored to changeable conditions to mitigate potential damage to the brand.[13]

1.7. Fundamental Principles of Risk Management

When developing a risk management framework, there are principles to be considered for guidance on the particularities and purpose of an effective risk management process, which are:

1. **Governance and leadership:** Risk management systems must be part of the organization's governance and leadership. They are essential in managing, directing, and monitoring work at all organizational levels. The organization must prepare a risk management governance scheme appropriate to the nature, scope, and culture of its business. This includes defining the roles and

[13] - https://shorturl.at/qBUY3

- Global Center for Strategy and Innovation. https://worldnetcs.com/services/

responsibilities of the concerned parties, the mechanism and methodology for managing its main risks and their recurrence, and monitoring and reporting on the status of risks.

2. **Integration:** Risk management should be integral to all organizational activities supporting decision-making to achieve strategic objectives.
3. **Collaboration and access to information:** Risk management must have the best available information, expertise, and resources. The organization should design a risk management framework that supports the overall vision of risks, decision-making, and governance requirements. Said framework is to implement risk management procedures on a regular and collaborative basis, drawing on the knowledge and opinions of experts and stakeholders.[14]

1.8. Risk Management Program

Developing a risk management program is an integrated roadmap that defines a safe path to deal with potential risks by highlighting the risk management steps that the organization puts in place. This is to ensure the proper functioning of the business at an appropriate level of risk accepted by an organization. [15]The risk management program includes many of the following steps:

First: Identification of Risks

Risk identification is a key pillar in the risk management system. It is the cornerstone of ensuring the safety and success of the organization. Risk identification is done through brainstorming or analysis with the aim of understanding and evaluating the potential risks that the organization may face in various aspects of its work, whether internal or external. It is a proactive

[14] - Ezzat, A. (2021). *A Program on the Role of the Internal Auditor in Governance and Risk Management*. Saudi Society.
- https://shorturl.at/UVj9z

[15] Rouqti, B. & Karkar, E. (2022). *Risk Management in the Algerian Healthcare System: A Field Study in Al-Hakim Okbi Hospital*. Faculty of Humanities and Social Sciences.

and continuous process that requires careful analysis and ongoing monitoring of the changing factors that may affect the organization. It uses a systematic approach that considers the strategic direction, operational objectives, factors vital to its success, and the opportunities and threats associated with achieving those objectives.

Second: Risk Analysis and Measurement

At this stage, potential risks are analyzed to measure their seriousness and reveal the reasons for their occurrence. [16]By looking at each type of risk, it is crucial to consider its three dimensions: a risk's size, duration, and probability of occurrence. Measuring risks correctly and in a timely manner is necessary to determine the value of expected losses based on mathematical methods and models. Said measurement is built on the size of the organization and the complexity of its operations. Risks can also be estimated using the qualitative method in terms of their probability of occurrence and potential results. Analyzing and measuring risks for the purpose of reviewing and controlling them will help the organization's management to achieve a clear forthcoming vision and determine the action plan to overcome such risks effectively. Combating risks improves the performance and cost of business in government entities.[17]

Third: Risk Assessment

The risk assessment process aims to understand the nature of risks profoundly, their levels of impact, and likelihood of occurrence. It also involves comparing the level of risk with the limits of risk tolerance and acceptance to identify additional procedures and controls required for risk

[16] - *Risk Concept and Risk Management: A Comprehensive Guide to Steps and Specialization*. Retrieved from https://shorturl.at/lnBL6
- Al-Krasnah, I. *Basic and Contemporary Frameworks in Bank Audit and Risk Management*. Arab Monetary Fund. Economic Policy Institute.

[17]Al-Khatib, S. (2005). *Measuring and Managing Risk in Banks*. Al-Maaref Establishment.

management. Said risks are to be shared with relevant stakeholders for their review and approval to obtain a complete view of all potential threats with varying degrees of severity. [18] There are several ways to assess risks. The appropriate method to do so can be chosen based on the type of project or activity and the level of detail required. Below are some common methods of risk assessment that can be applied jointly or individually:

a. Qualitative and Quantitative Assessment:

A qualitative assessment is typically used in the early stages of the risk assessment process, where there is insufficient data to make an accurate quantitative assessment. A quantitative assessment, on the other hand, is used when the information is sufficient to accurately analyze the risk and convert it into numerical measurements.

- Qualitative assessment: It is used to assess risks that cannot be measured in numbers, such as the risk of weather changes and earthquakes. The assessment must be neutral.
- Quantitative assessment: It is used to measure quantifiable threats, such as money and interest rates. It is the basic assessment used in financial affairs. [19]

b. SWOT Analysis:

It is a framework used to assess the status of an organization to identify its strengths and weaknesses, exploring opportunities and threats that the organization may be exposed to. This

[18] - *Risk Management Guide*. (2021). General Department of Governance, Risk and Compliance. Retrieved from https://shorturl.at/XtOWX
- Ministry of Planning and International Cooperation. *Risk Management Plan 2017-2019*. King Abdullah Award for Excellence in Government Performance and Transparency.

[19] - https://shorturl.at/uJ036
- https://shorturl.at/vHRX9

framework relies on internal and external assessments to evaluate the current situation and determine the upcoming courses. [20]

c. Cause and Effect Analysis:

The Cause and Effect analysis revolves around examining the factors that potentially lead to the occurrence of risks (causes) and the possible effects of these risks (consequences). This helps identify the aspects that should be focused on to reduce such risks and improve outcomes.

d. Process and System Analysis:

This form of analysis is conducted in the petroleum, chemical, and engineering industries. It focuses on assessing processes and systems to identify and classify potential risks and examine their impact and likelihood of occurrence.

e. Fault Tree Analysis:

It is used to analyze the events that may lead to a particular problem, helping analyze the factors that lead to the occurrence of risks and estimate the likelihood of their occurrence.

f. Hazard Analysis and Critical Control Point (HACCP):

HACCP is used in the food and other relevant industries. It aims to identify and assess potential risks associated with food safety and apply control measures.

[20] https://jadwa.om/blog/SWOT_Analysis

Fourth: Addressing risks

Addressing risks is the responsibility of all parties within an organization. It requires cooperation and coordination between various departments and sections, as discussions with managers, experts, and clients should be held to establish a solid foundation that offers proposed and appropriate solutions under the supervision of senior management. This notion helps address risks effectively and professionally so that the organization can achieve long-term success and sustainability and protect its interests, assets, and reputation.

Fifth: Risk Monitoring and Control

Risk monitoring and control is an ongoing process that aims to maintain an organization's resilience and ability to adapt to potential changes and challenges. It is done by regularly implementing effective monitoring and control procedures to ensure that risk strategies and methods work effectively, capturing any potential changeable conditions that may affect the organization’s activity. The organization can improve its ability to predict and respond to risks appropriately, which enhances its sustainability and long-term success. There are a number of significant steps in the process of monitoring and controlling risks, to mention a few:

a) **Updating evaluations regularly**: Regular reviews of the evaluations to ensure that they are in line with any recent circumstances or changes.

b) **Monitoring Key Performance Indicators (KPIs):** Identifying KPIs that illustrate the impact of risks on the project and identifying and analyzing their changes.

c) **Periodic communication**: Regular communication with the risk management team and other team members to share information and updates.

d) **Monitoring systems**: The use of tracking and monitoring systems to screen and detect risks constantly, such as using project management software.

e) **Updating response plans**: Update risk response plans based on new information and changes in the environment and ensure that sufficient resources are available to implement these plans.

f) **Assessing the impact of changes:** Assessing the impact of changes in the environment or a project on recognized risks along with adjusting strategies and plans based on these assessments.

Sixth: Supplementary Planning

Although risk management may seem like a prudent affair, unexpected incidents may take place during the project. Therefore, supplementary planning is vital in preparing an organization for worst-case scenarios and developing response plans. It specifies ways to deal with a distinctive risk event, including the allocation of resources. It ensures the work team is ready to deal with challenges without compromising the project's ultimate goals. [21]

By following these steps, you can ensure that risks are effectively monitored and controlled and that the project can successfully manage any risks that may arise during its development.

1.9. Types of Risk

Risks refer to the potentialities or threats that can adversely affect the achievement of objectives set by either an organization or an individual. Understanding the different types of risks helps to adopt appropriate strategies to manage and reduce their impact. Risks are classified into

[21] https://shorturl.at/qrCHT
https://shorturl.at/gluEK

various types based on their source, nature, and potential impact. The following are different types of risks that an organization is likely to encounter: [22]

a. **Systemic or public risks:** These are risks to which all sectors are exposed due to changes in general economic or political conditions that cannot be avoided or completely eliminated, and there is no radical solution to confront them. Examples include financial and economic crises, inflation, and political instability.

b. **Unsystematic or specific risks:** They are risks that affect a particular organization in a way that makes them exclusive to that organization. Examples include risks related to partners and suppliers, human behavior, and safety and security.

c. **Legal risks**: These risks arise through legal and regulatory obligations. Examples include compliance risks, non-contractual obligations, dispute risks, reputational risks, and contract and litigation risks.

d. **Organizational risks**: These risks arise due to ongoing internal uncertainties in the organizational process. They have an impact on all aspects of the organization. For instance, organizational risks intrude on the physical, strategic, reputational, legal, and operational aspects. The following are examples of organizational risks:

- The basic principles of the project were not adequately defined.
- Sudden changes may occur, such as changes to the project definition.
- The project was implemented based on vague procedures.
- Insufficient requirements set by the manager, client, or others.

[22] Jumaa, A. H. & Barghouti, S. *The Role of the Internal Auditor in Risk Management in Jordanian Commercial Banks: A Field Study*. 7th Annual International Scientific Conference on Risk Management and Knowledge Economy, 16-18 April. Al-Zaytouna University.

- Absence of agreement among parties involved in the project.
- Lack of internal coordination between subprojects (within the project as a whole.)

e. **Social risks**: They include businesses that affect the surrounding communities, such as labor issues and human rights violations within the workforce, as well as public health issues.

f. **Political risks:** Risks linked to changes in state policy and international relations, where decisions made by government leaders affect business. Examples include product boycotts, trade tariffs, labor laws, terrorism, people's actions, coups, wars, and political elections.

g. **Environmental risks:** This type of risk refers to the likelihood of an injury, illness, or death as a result of exposure to a potential internal hazard (i.e., water pollution, poor waste management, site pollution, air pollution, and/or noise).

h. **Financial risks:** They are risks associated with any form of financing that can result in adverse or uncertain returns on an investment. They are often called "Investment Risk." Examples of business-related risks include credit risk, liquidity risk, interest rate risk, foreign exchange rate risk, and market and operational risk.

i. **Non-financial risks:** This type includes a wide range of threats that can affect an organization's operational processes, reputation, compliance, and environmental and social sustainability. Yet, these risks are not directly related to financial matters such as liquidity, credit, and the market.

j. **Technological risks**: These risks are associated with the use of technology, including cybersecurity threats and IT failures.[23]

[23] Hull, J. C. (2015). *Risk Management and Financial Institutions*. Wiley.

1.10. Risk Management Features

When an organization is aware of the features of risk management, it can better identify and assess risks and develop strategies. It contributes to enhancing risk awareness within the organization and encouraging a culture of safety and risk control by identifying risks and addressing them appropriately to achieve stability and continuity in the face of shifting circumstances. Effective risk management is characterized by several features that help achieve its objectives. The following are some examples:

a. Fateful decisions to confront or resolve:

Risk management entails the ability to make difficult and critical decisions to effectively manage risks and reduce their impact. Examples include identifying new strategies for dealing with risks, allocating additional resources to strengthen security, or suspending an activity that poses risks without achieving tangible benefits.

b. Threatens the organization’s key objectives and the reputation of its decision-makers:

It requires striking a balance between achieving the organization's primary objectives and protecting the reputation of decision-makers. Implementing effective and sustainable risk management procedures is vital while considering transparency and accountability. Said procedures should also heed the challenges an entity faces in meeting its main objectives, such as financial risks, critical operational risks, or decision makers' reputations, especially in cases of failure or severe criticism.

c. Requires special processing and regulating structures:

Entities should establish an organizational framework and dedicated risk management structures that clarify the roles and responsibilities to ensure that the policies and procedures are implemented efficiently and effectively. These frameworks should establish mechanisms to regularly assess and analyze risks and make decisions that allow the organization to adapt to challenges in a way that aligns with its responsibilities and the nature of work. It is important to concurrently ensure the application of ethical principles and practices.

d. Complexity, entanglement, and overlap in its elements and causes:

A comprehensive and strategic analysis must be conducted, particularly against the complexity of potential risks due to the organization's exposure to factors such as internal policies, external environment, market variables, technology, and other risks. The risk management analysis process is a progressive challenge that requires a deep understanding of the correlation between different factors. Risks may be overlapping and unexpected. Secondary effects may arise as a result of the overlap of these risks.

e. Urgency in addressing the escalating risks:

Risk management requires a remarkable ability to work under pressure. It demands strong compliance with laws and regulations and familiarity with the latest technologies and instruments used in risk management. Risk management also implies rapid and correct decision-making and effective communication between different teams within the organization.

f. High level of risk undermines trust in proposed alternatives:

Increased risks can lead to doubts about the alternatives at hand. Growing risks can make officials hesitant or cautious in making decisions. This may be due to the fear of the possible adverse consequences of available options. Therefore, officials may be reluctant to take bold steps or attain high-risk choices. Moreover, increased risks can lead to increased tension and anxiety among officials, which may slow down or terminate the decision-making process altogether. In such cases, it becomes necessary to balance the understanding of risks, potential possibilities, and potential opportunities to achieve success and progress.

g. Organizational stability risks:

Uncontrolled risks may disrupt the operations of the organization and expose it to risk. For example, the leakage of sensitive data can severely affect the reputation of the organization.

h. Leveraging past situations and gaining experience

Government entities can take advantage of previous situations to gain experience and develop new procedures and policies, leading to greater risk management. This may be particularly relevant when facing critical circumstances such as natural disasters or public health crises.[24]

1.11. Risk Management Strategies

Selecting the most suitable strategy for risk management depends on the risk to be dealt with; these strategies include the following:

[24] - Boutros. S. (2011). *Modern Strategies for Crisis Management*. Dar Al-Raya for Publishing and Distribution.
- *Characteristics, Role and Objectives of Risk Management*. Retrieved from https://shorturl.at/mtyJZ
- Strategic Management Journal. Retrieved from https://onlinelibrary.wiley.com/journal/10970266

- **Risk Transfer:**

  This strategy involves getting another party to accept the risk, usually through contracts or financial protection and insurance.

- **Risk Avoidance**:

  Risk avoidance is the strategy of steering clear of any activities that lead to risks. This includes abstaining from buying a property or doing business to avoid legal responsibility. While avoidance seems to address all risks, it denies the concerned party the advantages and profits that could have been obtained from the avoided activity.

- **Risk Mitigation (Reduction):**

  This strategy includes approaches for mitigating the risk of losses. Examples of the adoption of a risk mitigation strategy include software development companies choosing to gradually develop their software to reduce risk.

- **Risk Acceptance (Retention):**

  This strategy involves the acceptance of losses when they occur. It is considered a reasonable strategy in the case of small risks in which the cost of insurance against the risk over time is greater than the total losses. All risks that cannot be avoided or transferred must be accepted; for example, it is impossible to insure against the effects of war. [25]

[25] Hindi, I. (2013). *Modern Perspectives on Risk Management: Financial Engineering Using Securitization and Derivatives*. Part II. Al-Maktab Al-Arabi Al-Hadith Publishing.

1.12. Challenges and Risks Facing Government Entities

Risk management in the government sector faces distinctive challenges owing to the special nature and environment in which government entities operate. Here are some of the key challenges facing government risk management:

a. **Complexity of bureaucracy:** The government sector usually includes complex bureaucratic structures, which makes it difficult to make decisions and implement procedures related to risk management.

b. **Funding Challenges:** The government sector faces financial challenges in allocating the resources needed to implement risk management programs effectively, especially when resources are limited.

c. **Dealing with political changes:** Government risk management can be significantly affected by political and regulatory changes, which can affect the priorities and resources allocated to them.

d. **Multiplicity of risks:** Government entities face a variety of risks, including financial, economic, environmental, political, and security risks.

e. **Difficulty in cooperation and coordination:** The implementation of government risk management programs requires cooperation and coordination between various government entities and concerned sectors to ensure the effectiveness of such procedures.

f. **Provision of public services:** Government entities must also ensure the continuous and effective provision of public services, which requires a balance between risk management and meeting the needs of citizens and society.

It can be said that risk management in government entities faces unique challenges due to the special nature of the public sector. However, it plays a crucial role in ensuring the stability and sustainability of public services and protecting the interests of citizens and society in general.

1.13. Importance of Risk Management in Government Entities

Risk management is vital and necessary for government entities, especially in light of their complex challenges in performing their tasks and achieving their strategic objectives. They are exposed to various challenges and risks, including financial and accounting risks; economic, political, environmental, social, and operational risks; technology risks; and digital transformation. As the role of governments requires meeting the needs of the entire society and providing essential services efficiently and effectively, the spread of business and rapid developments in the modern world have made it necessary to develop risk management strategies to ensure the continuity of these services and the effective fulfillment of government objectives.

With an effective understanding and assessment of various risks, government entities can develop innovative strategies to manage those risks and reduce their adverse impact on their performance and services. This helps to ensure the sustainability of government services and enhance resilience to achieve permanent shifts in the internal and external environments. [26]

[26] - General Department of Governance, Risk, and Compliance. (2021). *Risk Management Guide.*
- Ministry of Planning and International Cooperation. *Risk Management Plan 2017-2019*. King Abdullah Award for Excellence in Government Performance and Transparency.

Conclusion

Based on the aforementioned, it can be stated that:

Risks have become an inherent and evolving feature of contemporary life, requiring systematic and technical management to mitigate their severity. Effective follow-up is essential to achieve a balance between acceptable and expected risks, thereby supporting the attainment of the entity's objectives. This can be achieved by establishing an organizational structure associated with the entity's leading official to ensure the independence and effectiveness of risk management, as well as effective communication with stakeholders.

In light of the complex challenges' government entities face in performing their tasks and achieving their objectives, they are exposed to various risks in their internal and external environments. Since meeting the needs of society efficiently and effectively is a government duty, the government sector needs to develop robust risk management systems. This need is particularly pressing amid the rapid advancements in business and technology. Such systems are essential for ensuring the continuity of services within government entities, enhancing their resilience to constant internal and external transformations, and supporting them in achieving their objectives effectively.

The internal audit function assumes a pivotal role in the realm of risk management. It is instrumental in evaluating internal operations and systems, thereby ensuring their effectiveness and efficiency in addressing potential risks. Furthermore, internal audits serve to alert an organization's senior management or board of directors to potential risks through detailed reports submitted to senior leadership. This process is fundamental in enhancing internal operations and systems, ultimately facilitating the achievement of the organization's objectives carefully and ceaselessly.

In order to substantiate the preceding argument and expand upon the aforementioned statement, the following section (Theme 2) will delve into the theoretical framework that underpins internal audit and risk management.

Theme 2: The Role of Internal Auditing in Enhancing the Efficiency of Risk Management

Introduction

Professional organizations increasingly recognize the pivotal role of internal auditing as an independent evaluation mechanism that enhances effectiveness and efficiency. Internal auditing ensures compliance with laws, policies, and instructions and supports broader contemporary concepts such as systems governance, risk management efficiency, and the pursuit of quality and excellence.

In today's business environment, internal auditing has become essential for stakeholders, providing valuable insights into internal control systems within financial and operational processes. The internal auditor's report serves as a crucial source of information, guiding management and external auditors in their roles and helping them achieve comprehensive audit objectives effectively. Reflecting this importance,[27] the internal audit standards issued by the American Institute of Internal Auditors (IIA), referred to as IIA's Standards, emphasize the need to evaluate internal audit processes to ensure audit quality, strengthen independence, and enhance overall efficiency and effectiveness.[28]

This theme explores the role of internal auditing in improving the efficiency of risk management.

[27] https://shorturl.at/mnqPZ

[28] https://mail.almerja.com/reading.php?idm=196433

2.1 Concept of Internal Audit

The concept of internal auditing has significantly evolved with the advancement of social and economic norms. Initially, internal audits were limited to verifying accounting data and detecting errors, fraud, and manipulation. However, internal auditing has now expanded to encompass activities that assist management by integrating evaluation into its decision-making processes, particularly on how the organization shall implement its various activities to enhance overall effectiveness.[29]

Definitions of internal audit vary; among such are the following:

- **The American Institute of Internal Auditors (1999)** defines internal auditing as *"an independent evaluation activity established within a business organization to review processes as a service to management. It is an administrative control tool that measures and evaluates the effectiveness of other means of control."*
- The **Arab Society of Accountants** defines internal auditing as "*an internal function of the management aimed at establishing administrative and accounting controls to assess system consistency with management objectives and ensure optimal resource utilization."*
- The **International Federation of Accountants (IFAC)** defines internal auditing as *"an evaluation function within an establishment designed to serve management by testing and assessing the suitability and effectiveness of accounting and internal control systems."*
- The **French Institute of Auditing and Internal Consultants** defines internal auditing as *"an independent and objective activity aimed at providing assurance regarding an*

[29] Ezzat, A. (2021). *A Program on the Role of the Internal Auditor in Governance and Risk Management*. Saudi Society. Retrieved from https://shorturl.at/UVj9z

organization’s control over operations, offering recommendations for improvement, and contributing to value creation.”[30]

Based on these definitions, internal auditing extends beyond asset protection and financial reviews. It now encompasses financial and administrative auditing as well as advisory roles that ensure the integrity of financial statements in accordance with applicable standards and established accounting policies.

2.2 Objectives of Internal Auditing

The objectives of internal auditing are shaped by an organization`s specific goals but generally include:

- **Assurance of Compliance and Conformity:** Ensuring that an organization’s operations and policies comply with applicable laws, regulations, bylaws, and relevant standards.
- **Operational Efficiency Assessment:** Evaluating the effectiveness and efficiency of operations and identifying areas for performance improvement.
- **Risk Assessment:** Identifying and evaluating risks to implement effective management strategies.
- **Applying Governance:** Assessing an organization’s adherence to governance principles, ethical standards, performance management, and accountability. This is in addition to evaluating its commitment to communicating risk information and monitoring performance, creating effective communication between those in charge of oversight and internal and external auditors, and their relationship with management.

[30] https://uomustansiriyah.edu.iq/media/lectures/10/10_2019_10_23!09_17_41_PM.docx

- **Promoting Internal Control**: Evaluating and strengthening internal audit controls to safeguard assets and mitigate fraud and manipulation risks.
- **Management Support:** Providing guidance and advice to management on how to enhance operational processes and improve performance based on audit findings and observations.
- **Enhancing Trust and Transparency**: Fostering trust between management and stakeholders by providing transparent and reliable reports on the organization's status and performance.[31]

In light of the above, these objectives demonstrate that internal audit plays a crucial role in achieving comprehensive administrative, accounting, and operational control by providing data-driven evaluations and recommendations for effective risk management.

2.3 The Impact of Risks on Internal Auditing and Organizational Activities

Risks encountered by internal auditing can be categorized into two types:

Type I: Risks Arising from Internal Audit Processes (Audit Risks)

Adopting an integrated strategic risk management approach has become essential for assisting organizations in effectively assessing and mitigating risks. One of the most advanced and evolving approaches is risk-based auditing, which focuses on aligning audit activities with identified risks. Successful audit leaders acknowledge the need to continuously develop their skills to guide their organizations in adopting this approach. According to ISA 200,[32] audit risks include the

[31] https://shorturl.at/jvG24
[32] https://shorturl.at/cpxBN

possibility of issuing a qualified opinion, an adverse opinion, or a disclaimer of opinion due to inconsistencies between economic facts and audit results.[33]

Type II: Risks Threatening Organizational Stability and Growth (Operational Risks)

Internal auditing is a crucial element in risk management, as it enhances transparency and credibility in an organization's internal operations while improving the effectiveness and efficiency of control systems. Internal auditing involves independent risk assessments that require periodic reports and recommendations to help management evaluate and improve the effectiveness of risk management. Additionally, internal auditing plays a key role in improving organizational performance and achieving strategic objectives. The IIA's International Standards for the Professional Practice of Internal Auditing provide a structured framework and valuable guidelines for improving risk management practices within organizations. [34]

From the above, we can conclude the following:

It is essential to distinguish between the two types of risks: audit risks and organizational risks. Audit risks include those arising during internal audit processes, such as the excessive use of evidence in auditing, negatively affecting the reports' results.

Operational risks, on the other hand, relate to other risks facing an organization during the conduct of its basic business activities. These risks require auditors to have a comprehensive knowledge of both internal and external control systems, along with a sufficient understanding of the work environment and the nature of the organization's activities. To ensure business continuity

[33] *Risk Audit Guide*. SAI Iraq
[34] https://shorturl.at/vJh9F

and the achievement of audit objectives, auditors must conduct a preliminary risk assessment to identify high-risk areas, determine audit priorities, develop an audit plan, and set a specific timeline for the audit plan.

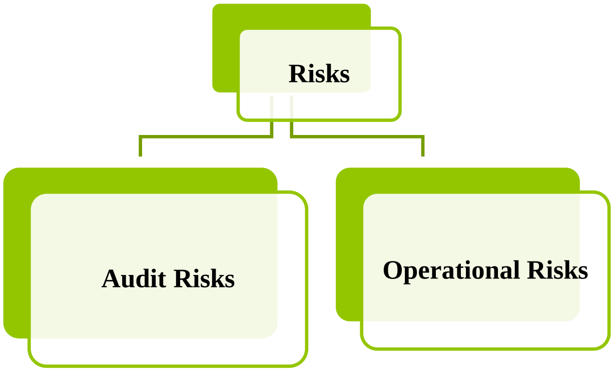


Figure 2

2.4 Risk-related Auditing Standards

Many internal audit procedures rely on auditors’ professional judgments, which may vary from one auditor to another based on their professional training and expertise. Recognizing the need to minimize discrepancies and enhance the objectivity of auditors' judgments, professional organizations have introduced numerous standardized guidelines. These internationally recognized auditing standards serve as a foundation framework upon which auditors rely when conducting their audit functions. International auditing standards provide a structured set of guidelines and rules that auditors must follow in their assessment and judgment processes. They are developed after a long process of logical reasoning and conclusions built upon supporting concepts and hypotheses.

The following are the key international auditing standards relevant to risk assessment and risk-based auditing:

a. International Standards for the Professional Practice of Internal Auditing (IIA's Standards)

- **Standard 2200 – Engagement Planning.** Internal auditors should develop and document a plan for each engagement.
- **Standard 2201 – Planning Considerations.**
- **Standard 2210 – Engagement Objectives.**
    - **2210. A1 –** The objectives of the consulting engagement must address the course of governance, risk management, and control within the agreement.
    - **2210. A2 –** The objectives of the consulting engagement must align with the organization's values, strategy, and goals.
- **Standard 2220 – Engagement Scope**. The established scope should be sufficient to satisfy the engagement's objectives.
- **Standard 2230 – Engagement Resource Allocation.**
- **Standard 2240 – Engagement Work Program**. Internal auditors should develop and record work programs that achieve the engagement's objectives.[35]

b. International Standards on Auditing (ISAs):

- **ISA 315** – Identifying and Assessing the Risks of Material Misstatement
- **ISA 320** – Materiality in Planning and Performing an Audit.
- **ISA 330** – The Auditor's Responses to Assessed Risks.
- **ISA 400** – Risk Assessments and Internal Control. [36]

c. The International Standards of Supreme Audit Institutions (ISSAIs):

- **ISSAI 1200 -** Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing.

[35] https://shorturl.at/bfzAZ
[36] https://socpa.org.sa/audit

- **ISSAI 1315** - Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment.
- **ISSAI 1320** - Materiality in Planning and Performing an Audit.
- **ISSAI 1330** -The Auditor's Responses to Assessed Risks. This standard requires internal auditors to prepare a detailed audit plan and design procedures for previously assessed risks.[37]

d. ISO Standards:

The International Organization for Standardization (ISO) has established an international standard for risk management (**ISO 31000**). This standard was developed in response to organizations' demand for standardized guidelines that ensure long-term success. Although achieving success requires continuous evaluation and updates to improve performance, risk assessment also plays a critical role in ensuring the continuity of an organization's excellence. [38]

2.5 Parties Responsible For Evaluating Risk Management Programs

Risk management programs are often evaluated by various parties, including the following:

a. **Senior management:** Senior management is responsible for periodically evaluating the effectiveness of the risk management program and ensuring its alignment with the organization's objectives and suitability for the environment.

b. **Audit and risk management committee**: This is the most prominent committee in companies' organizational structures compared to government bodies. It is formed by a company's board of directors and consists of non-executive members. The committee has a supervisory and

[37] https://shorturl.at/fABUY
[38] https://shorturl.at/mvyBG

regulatory role in auditing and reviewing accounting policies, as well as financial reporting processes and risk management.

c. **Internal auditors**: Internal auditors are responsible for independently evaluating the risk management program and ensuring compliance with the relevant international standards, including the IIA's International Standard for Professional Practices of Internal Auditing: Standard 1311- *Internal Assessments* and Standard 1312 -*External Assessments*.

d. **Third parties**: Organizations often engage external consulting firms or academic institutions to evaluate their respective risk management programs.

e. **Regulatory authorities**: Some organizations are subject to evaluating their risk management programs by competent regulatory authorities such as capital market authorities, Supreme Audit Institutions, and central banks.

2.6 Factors Defining the Parties Responsible for Risk Assessment

Evaluating and auditing the risk management program is necessary to ensure its effectiveness and the organization's overall safety. Several factors define which party is responsible for assessing and auditing the risk management program of an organization, including the following:

a. **Organization Size and Complexity**:

Large and complex organizations tend to have specialized internal audit departments, whereas small organizations often rely on third parties.

b. **Nature of Risks**:

Certain risks may require assessment by specialists with expertise in specific fields.

c. **Requirements of regulatory authorities:** Some regulatory authorities may impose specific requirements for evaluating and auditing the risk management program.[39]

2.7 Types of Audit Risks

Professional organizations place significant emphasis on risks. In 1970, the IIA issued Bulletin No.1 on audit risks, explaining how risks impact the nature of the audit process. The scope of an audit is defined based on the examination and assessment of internal controls, which directly affect audit procedures. The more systematic and structured the internal audit process, the lower the audit risks. This aligns with the internal auditor's objective of mitigating identified risks.[40]

Audit risk refers to the possibility that an auditor issues an incorrect audit opinion on financial statements due to failing to detect material misstatements[41]. There are three main types of internal audit risks, as outlined below:[42]

Types of Audit Risks

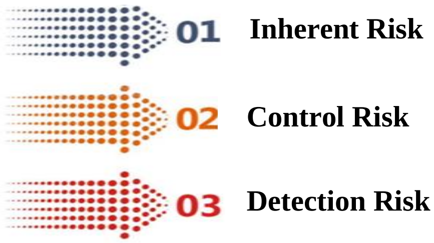


Figure 3

[39] Kheira, R. (2012). *The Role of Internal Audit in Enterprise Risk Management*. Hassiba Benbouali University. Faculty of Economics and Management Sciences.

[40] Moussa, A., & Futuhah, M. S. *Sectoral Specialization of Auditors and their Role in Mitigating Audit Risks*. University Bulletin. Volume 1. Issue 18.

[41] https://shorturl.at/loQV7

[42] https://shorturl.at/ctxyX

1. **Inherent Risk (IR)**:

These are risks associated with a specific function, activity, or element due to its nature and inherent characteristics. They are also called ‘intrinsic risks,’ which arise from the environment in which an organization operates. Inherent risks reflect the susceptibility of a particular activity or field to problems when no effective controls or risk management methods are in place. For example, an organization with significant goodwill is more vulnerable to inherent risks because goodwill is an intangible asset that depends on estimates and assumptions.

2. **Control Risk (CR)**:

These risks arise due to internal controls' inability to prevent or detect errors in a timely manner. For example, when weak internal controls increase the chances of material misstatements not being prevented or detected in a timely manner, leading to greater control risks.

3. **Detection Risk**:

These risks refer to the possibility of errors or misstatements remaining undetected despite detailed audit procedures. Detection risks may occur in financial balances or transaction chains, either independently or combined with other data errors. These risks consist of several specific types:

   a. **Analytical Review Risk:** This risk occurs when detailed analytical procedures, such as the analysis of significant ratios, trends, and abnormal items, fail to detect material errors or irregularities (e.g., embezzlement, manipulation, or false disclosures) that may not be prevented or detected by internal control procedures.

   b. **Risk of Detailed Tests:** This refers to the risk that the results of detailed tests may lead to incorrect acceptance of financial information when a material error has not been identified through the various control procedures.

c. **Sampling Risk:** This risk occurs when the auditor's conclusions drawn from a selected sample differ from the conclusions that would have been reached if the same audit procedures had been applied to the entire database.

d. **Inherent Risk:** It refers to the auditor's judgment-based assessment of whether there is a possibility of incorrect or misleading data before considering the effectiveness of internal controls.

e. **Audit Risk:** It represents the risk that the auditor is willing to accept when issuing an incorrect audit opinion on a set of financial data. [43]

Understanding audit risks requires internal auditors to be aware of other considerations potentially affecting the audit process and its results. This would help them determine the appropriate approach and take the necessary measures to implement audit procedures efficiently and effectively, ensuring that accurate information and reliable results are obtained[44]. These considerations include the following:

No.	Risk Category	Considerations
1	Non-Compliance Risks	Adherence to laws, legislations, circulars, regulations, procedures, and systems.
2	Financial Risks	Financial structures, financial liquidity, credit grants, fluctuations in foreign exchange rates, business downturns, and profitability challenges.
3	Operational and Organizational Risks	- The extent to which targeted performance objectives are achieved. - Diversity of activities or branches of an organization. - Competency of performance staff within an organization. - Risk of providing misleading or incorrect information in the decision-making process.
4	Strategic Risks	- Economic, social, or environmental factors. - Strategic objectives and trends.
5	Technological Risks	- Confidentiality or corruption of electronic data. - Information security concerns. - Regularity of applied automated programs.

Table 1: Risk Category Considerations

[43] *The Era of Risk-Based Auditing*. Saudi Center for Financial Audit and Performance Control. https://shorturl.at/sxEGO

[44] Al-Huwaidi, E., & Al-Nassar, A. (2019). *Training Program: Risk-based Audit (Auditor's Impact Training Project)*.

2.8 Internal Audit Risk Assessment [45]

Auditors' audit risk assessments vary due to differences in auditor competency, expertise, and auditing methodologies. Additionally, the absence of a universally accepted quantitative mathematical model further contributes to variations in risk assessments. The following are key types of risk assessments:

1. **Assessment of Inherent Risks:** This assessment focuses on risks that auditors cannot control or precisely measure, making them challenging to evaluate. Examples include exchange rate fluctuations, interest rate volatility, and management's integrity and objectivity.
2. **Assessment of Residual Control Risks:** This assessment evaluates the effectiveness of an organization's accounting and internal control systems. It includes assessing whether these systems can detect errors or misstatements and implement corrective measures.
3. **Assessment of Detection Risks:** This assessment is based on evaluating inherent risks.

2.9 Methods for Internal Audit Risk Assessment

When it comes to auditing, assessing audit risk is a critical step that all auditors must consider. Audit risk refers to the possibility that an auditor may issue an incorrect opinion on financial statements, potentially leading to misstatements or unreliable reporting. Therefore, auditors should implement audit risk assessment techniques to evaluate risks and plan audit procedures accordingly. Several techniques are used to determine audit risk. Below are some of the commonly applied methods:

[45] Moussa, A., & Futuhah, M. S. *Sectoral Specialization of Auditors and their Role in Mitigating Audit Risks*. University Bulletin. Volume 1. Issue 18.

1. **Analytical Procedures:** This method involves analyzing financial data to identify trends, ratios, and other financial relationships that provide insight into the risk of material misstatements. For example, an auditor may examine the revenue growth rates over the past few years to determine whether they align with industry trends or to compare current financial data with past performance.
2. **Inquiry:** It involves asking structured and targeted questions to management and relevant personnel within an organization to gain an understanding of the internal processes and controls. For example, an auditor may inquire about inventory management processes to determine whether they effectively prevent fraud.
3. **Observation:** This method includes actual monitoring of processes and controls at work. For example, an auditor may observe the movement of an organization's stock balance to determine whether inventory controls are being followed properly.
4. **Risk Assessment Surveys and Questionnaires:** This technique involves collecting structured data about an organization's operations to identify potential risk areas. For example, a questionnaire might assess how an organization uses estimates in financial reporting to determine whether there is a risk of material misstatement.
5. **Detailed Instructions (In-depth Walkthrough):** This technique involves tracing a transaction's entire journey through the accounting system from its origin to its final inclusion in financial statements. For example, an auditor might follow the process of recording a sale to determine if there are any vulnerabilities in the organization's internal controls.

Audit Risk Assessment Methods

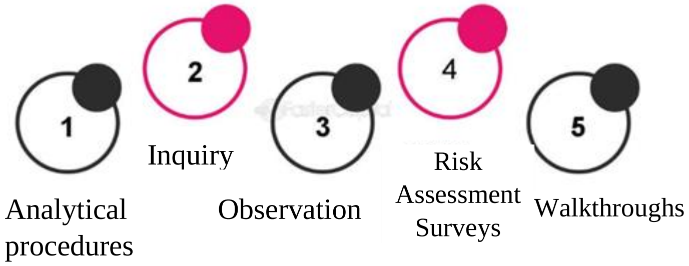


Figure 4

Although each technique provides valuable information to auditors when assessing audit risk, it is essential to note that no single technique can offer a complete assessment of audit risk. Therefore, auditors should employ multiple methods to evaluate risks and plan audit procedures accordingly. Adopting a multi-method approach ensures a more comprehensive and accurate audit risk assessment, ultimately enhancing the effectiveness of audit efforts.

2.10 The Role of Internal Auditing in Enhancing the Efficiency and Effectiveness of Risk Management

Internal auditing plays a crucial role in improving both the efficiency and effectiveness of risk management. It provides senior management with objective assurances regarding the effectiveness of internal control systems and activities and the efficiency of risk management within the organization.[46] The Institute of Internal Auditors (IIA) states that the primary role of internal audits is to provide independent assurance to senior management that key business risks are

[46] Al-Tamimi, H. (2004). *Introduction to Auditing: A Practical and Theoretical Approach*. Dar Wael for Publishing and Distribution.

managed appropriately and correctly while ensuring that risk management and internal control frameworks function effectively. Additionally, the IIA highlights that internal auditors should operate within their scope of competence, avoiding activities that could impair their independence and objectivity. It also clarifies that while risk management is the responsibility of an organization's management, the role of the internal audit activity is to provide independent assurance and supervisory services to support these processes. According to the IIA, internal auditors have a broad range of responsibilities, including the following:[47]

1. Preparing and evaluating supervisory audit reports for various units.
2. Developing a risk-based internal audit plan for different departments based on identified risks and classification criteria. This ensures effective prioritization of audit objectives and optimal allocation of resources according to risk likelihood and impact.
3. Conducting independent reviews of systems to assess the effectiveness, reliability, and validity of internal control procedures.
4. Ensuring that risk management functions efficiently and aligns with global best practices, as well as local and international regulatory requirements.
5. Assessing and evaluating the effectiveness of adopted policies and procedures by comparing them with applicable international and local standards and regulatory requirements, along with providing recommendations to enhance compliance and improve organizational performance.
6. Internal auditing has evolved beyond its traditional role of examination, confirmation, and evaluation. It now encompasses consultation and advisory services while ensuring

[47] https://www.theiia.org/Copyright

independence, mitigating conflicts of interest, developing necessary competencies, and enhancing resource management.

7. Communicating audit results and reporting any weaknesses or vulnerabilities in internal control procedures to management, enabling them to take the necessary actions to strengthen and improve processes while reducing potential risks.
8. Preparing an internal audit report, including a summary of the unit's control environment, an evaluation standard, and a comparative analysis of actual vs. expected performance.

2.11 Audit Procedures for Risk Management Programs

They are the steps through which a risk management program is evaluated and audited. Auditing a risk management program includes the following:

a. **Auditing risk management objectives and procedures**: This process involves reviewing the risk management programs approved by the organization to assess their impact on the sustainability and quality of the services provided, ensuring they meet their intended objectives. It also includes analyzing risk management objectives and evaluating their compatibility with the organization's service objectives and available financial resources. This evaluation determines the consistency between the intended objectives and the quality of services provided while also identifying potential areas for improvement. In addition, this process aims to assess the effectiveness and efficiency of service operations in relation to the financial resources available to the organization.

b. **Identifying and assessing risks:** It involves identifying current risks encountered by the organization and evaluating their impact. When significant risks remain unmanaged, it is crucial to establish corrective procedures and consider appropriate alternatives. However, if the organization fails to respond adequately to these risks, the internal audit activity should provide recommendations and action plans for an appropriate risk response.

c. **Evaluating decisions to address each risk:** This procedure examines the different methods available to effectively manage each identified risk. It includes reviewing approaches for accepting and mitigating risks while also assessing the feasibility of transferring or retaining certain risks within the organization.

d. **Evaluating the implementation of selected risk management methodologies**: This procedure involves reviewing previous decisions made by the organization's management regarding risk management strategies. It ensures that these decisions are fully implemented, evaluates the effectiveness of risk control procedures, and assesses their impact in accordance with the *International Standard for the Professional Practice of Internal Auditing 2120- Risk Management*, which states the following:

   - ➢ The internal audit activity must evaluate the effectiveness of risk management processes and contribute to their improvement.
   - ➢ The internal audit activity must assess the organization’s exposure to risks associated with its activities, operations, and information systems. This assessment ensures the reliability and security of financial and operational data, the efficiency and effectiveness of processes, and the protection of assets. It also includes ensuring compliance with applicable laws, regulations, and contractual obligations.

e. **Reporting and recommending improvements for the risk management program:** This procedure involves presenting a written report to senior management or relevant committees and stakeholders detailing the analysis findings on the risk management program. The report also includes recommendations for further improvements.

2.12 Internal Audit Quality Assurance and Improvement Program

The Quality Assurance and Improvement Program (QAIP) aims to ensure that internal audits meet professional quality standards and adhere to best practices. It includes both internal and external assessments to ensure the integrity of action plans, efficiency of audit procedures, and objectivity of reports. Assessments are conducted to ensure compliance with international standards, enhance the independence of internal audit activities, and identify potential risks. They also aim to provide corrective recommendations, improve performance and audit effectiveness, and promote confidence in internal audit reports. These procedures must be conducted in accordance with IIA's Standard 1300, which states: " *The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity*." Additionally, Standard 1310 states: "*The quality assurance and improvement program must include both internal and external assessments."*

According to Standard 1302, an external assessment shall be conducted at least once every five years by a qualified and independent external assessor or assessment team. This process includes evaluating performance, analyzing gaps, identifying potential risks, and making recommendations to enhance performance, improve audit effectiveness, and promote confidence in audit reports. [48]

[48] International Standards for the Professional Practices of Internal Auditing (Standards). Retrieved from https://shorturl.at/wEHSV

Conclusion

Based on the aforementioned, it can be stated that:

The rapid developments in the industry have led to a noticeable shift in the function of internal audit. It has broadened in scope beyond the auditing of financial statements. Internal auditing now encompasses more inclusive responsibilities, such as:

- Providing senior management with independent and objective advisory services on risk management, internal controls, and governance processes and
- supporting the organization in improving its operations and performance by providing consulting services.

However, internal auditing faces new challenges, the most prominent of which are:

- **Auditor's Risk:** The possibility of an auditor expressing an incorrect opinion on the validity of the organization's financial statements or other reports.
- **Financial, Strategic, and Technological Risks:** Risks that may threaten the business continuity of an organization and hinder the achievement of organizational objectives.

To enhance the effectiveness of internal auditing in light of these developments, it is recommended to:

- **Adopt a risk-based audit approach** by focusing on the organization's high-priority risks.
- **Raise internal auditors' awareness of the organization's risks** to help them gain a comprehensive understanding of the organization's internal and external systems and operating environment.

- **Leverage technology** by utilizing modern audit tools, such as audit assistant software and data analysis tools, automating repetitive audit tasks, and making use of available collaboration platforms to ensure effective communication and information sharing among internal auditors.
- **Develop and implement an internal audit quality assurance and improvement program (QAIP)**, which should include periodic internal and external assessments to meet professional quality standards.

Governance and risk management are essential pillars in ensuring the stability and prosperity of organizations. However, these objectives cannot be fully achieved without an effective internal audit system. Therefore, Supreme Audit Institutions (SAIs) play a pivotal role in assessing the quality and effectiveness of internal audit systems.

Delving further into the study, the next section will explore the theoretical framework of Theme 3, highlighting the role of SAIs in enhancing risk management systems by promoting internal audit activities within government entities.

Theme 3: Supreme Audit Institutions and Their Role in Enhancing Risk Management

Introduction

Supreme Audit Institutions (SAIs) play a vital and fundamental role in ensuring governments' compliance with laws and regulations. As the primary oversight bodies, SAIs uphold accountability to legislative authorities by monitoring the use of public funds. SAIs express an independent opinion on the quality and effectiveness of public sector management across all its activities through detailed reports submitted to the relevant authorities. Their role in safeguarding public funds extends beyond detecting financial crimes; it encompasses a broader spectrum of oversight functions that differ based on governance structures, regulatory frameworks, and audit methodologies unique to each country.[49]

SAIs strive to keep pace with rapid advancements in risk management. This notion has gained significant attention following a series of global crises that struck various economic sectors, particularly during the COVID-19 pandemic. Many organizations initially underestimated the severity of risks during these times. As a result, risk management has emerged as a critical tool for effectively addressing significant risks in the public sector despite its traditional prominence in the private sector. However, the public sector has since shown growing interest in integrating risk management practices into internal audit functions. Consequently, the role of SAIs has become increasingly essential in monitoring and assessing the adopted internal audit methodologies while also developing risk management systems within government entities[50]. Such institutions play a

[49] Al-Lanfawi, Kh., Al-Otaibi, R., & Al-Jabri, F. (2021). *The Impact of the General Audit Guide and Other Specialized Guides of the State Audit Bureau on Improving Audit Performance*. The 22nd Research Competition of the State Audit Bureau of Kuwait.

[50] General Department of Governance, Risk, and Compliance. (2021). *Risk Management Guide*.

pivotal role in enhancing entities' preparedness to address recurrent and emerging risks while ensuring the professional implementation of audit engagements.[51]

The following section presents the audit methodology used by SAIs to promote and enhance governments' readiness in their response to risks.

3. Audit Methodology and Risk Management Evaluation

Supreme Audit institutions (SAIs) adopt a systematic audit methodology to assess and enhance risk management practices. This is a continuous process designed to ensure government entities' readiness to address emerging challenges, in addition to providing the necessary tools to develop government systems and enhance compliance with high-quality audit practices. The methodology consists of a structured set of steps aimed at achieving higher levels of continuous improvement and development while ensuring greater efficiency and quality in audit procedures. These steps are also intended to facilitate an effective evaluation of risk management systems. The following section outlines the steps of the methodology under two primary phases:

3.1 Phase One: Assessing an Auditee's Current Situation and Designing the Audit Methodology

This phase consists of a structured process designed to assess an auditee's current situation and determine the effectiveness of its risk management system. It also involves the development of an audit methodology to identify and enhance key areas requiring further improvement through the following:

[51] Al-Humaimidi, N., & Al-Rashed, M. (2021). *Risk-based Audit*. The 21st Research Competition of the State Audit Bureau of Kuwait.

3.1.1 Understanding the Auditees

The purpose of collecting information and data provided by auditees at an early stage is to establish a comprehensive and reliable database that enhances auditors' understanding of the auditee's current situation and helps identify its strengths and weaknesses. This step includes the following:

- Identifying the auditee's work environment and nature of operations and examining the factors affecting its activities.
- Reviewing the auditee's general work plan and meeting minutes from senior management and various committees.
- Identifying the auditee's financial and administrative management systems as well as the authorities and delegations.
- Identifying the roles and responsibilities related to the governance of automated information systems.
- Assessing the effectiveness of internal control systems.
- Examining and evaluating the execution of risk management programs, their reports, and risk tolerance strategies to determine their effectiveness and alignment with the auditee's objectives and international or local risk management standards.
- Evaluating the tools and techniques used for risk analysis and assessment processes to assess their efficiency in identifying risks and applying preventive measures.
- Verifying the auditee's compliance with local and international laws and standards related to risk management while ensuring the alignment of processes and policies with these requirements.

- Assessing an auditee’s ability to identify potential risks and predict future changes, as well as evaluating its risk readiness and resilience.
- Assessing risk management maturity levels (High-Medium-Low) to determine the required level of maturity.
- Reviewing relevant articles published in newspapers that would help gain a more comprehensive understanding of an entity’s activities and risks.[52]

3.1.2 Understanding Internal Controls:

Understanding and documenting the procedures of the internal control system is essential for the initial assessment of control risk levels, particularly when relying on inputs from various systems and activities, along with their respective tests. This ensures that a structured control system is in place. This process helps verify the progress of control activities and assess their performance quality. It also enhances auditors’ understanding of how the organization manages and responds to risks. Additionally, such an understanding aids in determining the general approach to auditing the internal control system and identifying areas for improvement and recommendations.[53]

3.1.3 Understanding and Assessing the Risk Control Environment

According to INTOSAI GOV 9100, the control environment serves as the foundation of an organization’s internal control system. It encompasses a framework of governance, incorporating key elements such as policies and human resources practices. The control environment applies

[52] Al-Huwaidi, E., & Al-Nassar, A. (2019). *Training Program: Risk-based Audit* (Auditor’s Impact Training Project).

[53] Abdullah, H., & Al-Faraj, A. (2019). *Training Program: Methods and Procedures for Assessing Internal Audit Bodies Using a Risk-Based Approach.*

continuously across all levels and stages of an organization's operations. Therefore, the audit team must understand and assess the control environment for all risks to determine their impact, including the following:

a. Preventive Controls to Reduce Risks:

Preventive controls involve a robust risk management system and structured procedures for implementing risk mitigation plans and continuous monitoring. These measures enhance risk awareness, improve the efficiency of organizational performance, and secure compliance with applicable laws and regulations. Additionally, preventive controls contribute to effective governance, a proactive control approach, strengthening the organization's reputation, and maintaining a stable and secure operational environment. Risk monitoring is, therefore, considered a strategic investment that ensures the long-term sustainability and growth of the organization.

b. Corrective Controls to Minimize Impact:

Corrective controls include reactive measures that focus on mitigating the adverse effects of risks by implementing response strategies after an event has occurred. Their objective is to reduce the impact of risks, whether they involve financial losses, human injuries, or environmental damage. Examples of corrective controls include financial compensation for damages (e.g., full coverage insurance), emergency response systems, security and breach management systems, and performance quality assurance mechanisms.

3.1.4 Understanding Internal Audit

The audit teams should acquire a comprehensive understanding of the internal audit function, risk management system, and reporting mechanisms that identify key risks faced by the organization. This is achieved through reviewing the internal audit charter, assessing the effectiveness of planning and risk mitigation processes, and developing a thorough understanding of internal audit reports. The audit team should identify, analyze, measure, and evaluate risks within the organizations. The most effective control measures and corrective actions should be established, alongside evaluating the self-monitoring system adopted by the internal audit unit/department. Internal auditing also includes monitoring risk reports that highlight the organization's various activities and the adopted risk responses- whether to transfer, tolerate, or terminate risks. Additionally, it involves assessing the efficiency of the quality management system and evaluating the quality of training and development programs offered for internal auditors. Ultimately, internal auditors should recognize that an effective risk management system prioritizes high-impact risks with a high probability of occurrence over those with low impact or a lower probability of occurrence.[54]

3.1.5 Understanding and Evaluating the Effectiveness of Risk Management

In addition to the initial information reviewed by the audit team when forming an understanding of the internal audit process, as mentioned above, understanding and evaluating the effectiveness of risk management is essential to ensure that the risk management process continues efficiently and achieves the desired objectives. This step involves identifying strengths and

[54] https://shorturl.at/D070p

vulnerabilities within the risk management system and recognizing opportunities for improvement. The following section outlines the evaluation process:

a. **Effective Risk Management:**

It is essential to review the risk management records prepared and approved by the organization to ensure effective risk management. A matrix should then be developed to assess and classify areas of risk to be audited by SAIs` auditors based on their priority, severity, and impact.

- **Effective risk management** is a risk-oriented approach that directs its efforts to follow up on multiple priorities, ensuring that significant risks with high losses and high probability receive the highest priority in treatment first, while risks with lower probability or lesser severity are addressed later.
- **Unknown risk management** refers to handling newly emerging risks that have a 100% probability of occurrence but remain unaddressed by organizations due to their inability to recognize or accurately identify them.[55]

b. **Ineffective or Absent Risk Management**

Risk identification is based on the efforts of SAIs' audit teams, following various tools and methods to classify an auditee's activities and operations and pinpoint potential risks. These methods include the following:

- **Brainstorming Potential Risks:** This involves engaging audit team members in open discussions to address well-defined issues within a free-thinking environment. This method enables the team to generate more ideas, which can be built upon and refined into actionable insights.

[55] State Audit Bureau. (2022). *Guidance for the Planning Phase of Risk-based Audit*.

- **Interviews:** A valuable tool used to collect data from individuals, allowing interviewers to pose open-ended questions and explore the respondents' thoughts, insights, and emotions.
- **Field Observations:** They enhance auditing efficiency, enabling auditors to provide a reliable audit opinion on the accuracy of financial information. These observations facilitate a thorough data review and the collection of detailed insights into potential risks. They may include site and operational observations, behavioral observations, interactions affecting reputation or relationships, and the analysis of surveillance footage, audio recordings, and other relevant evidence.
- **SWOT Analysis:** This analysis helps auditors analyze an organization's strengths, weaknesses, opportunities, and threats.
- **Surveys:** A valuable tool for collecting information, facilitating effective communication with others, and conducting analyses to improve risk management within an organization.
- **Reviewing previous reports and studies** is an essential method that could help an audit team identify the risks encountered by the entity. [56]

3.1.6 Preparing the Risk Audit Plan

To develop a comprehensive risk audit plan, SAIs' audit team members should first analyze initial studies and data related to financial matters, operational processes, organizational decisions, or employee competence. Additionally, identifying misleading or incorrect information in the decision-making process is crucial. All these aspects should be considered within the context of economic, social, and environmental conditions, as well as the strategic objectives and directions. Audit team members should also review an auditee's risk management records, evaluate actions

[56] https://shorturl.at/gnvO4

taken in this regard, and assess digital risks. A roadmap and risk audit plan should then be developed, including improvement programs aimed at identifying gaps, establishing well-defined timetables, achieving the required maturity levels, and enhancing the entity's risk management capabilities.

When preparing risk audit plans, the following determinants shall be considered:

- **Financial Value or Material Impact:** This determinant focuses on the fact that the greater the financial size or impact, the higher the likelihood of being selected for audit. It is assessed by reviewing income statements, expense trends, return on investment, overall financial position, fluctuations in expenditures, or changes in assets and liabilities values.
- **Time Gap in the Audit Plan:** The longer the time since the last audit or review, the higher the probability of risks occurring and increasing.
- **Public Significance:** This determinant considers the social, economic, and environmental impact of the activity and its importance to the council of ministers, parliament, civil society, and individuals. It also considers the extent to which the subject matter is addressed in traditional and social media platforms.
- **Previous Reports:** Audit reports serve as key references for assessing risks facing an entity subject to audit. These include the SAI's previous reports, reports on assignments and published studies, internal audit reports issued by auditors of the entity, and any relevant reports or studies available to the audit team.

To effectively consider these determinants when identifying risks, internal audit team members must possess advanced professional skills. Additionally, the competence of internal auditors is crucial, as they are required to rank the priority of risk-related topics based on their severity- high, medium, or low- according to their assessment and analysis of the available data.

3.1.7 Key Considerations Relevant to the Implementation of the Audit Engagement

Audit leadership must assess the capabilities required to effectively conduct the audit engagement, taking into account the following considerations:

- **Audit Team Members**: The number of audit team members required to effectively implement the audit plan should be determined based on the size and complexity of the topics selected for the audit.
- **Level of Skills and Experience:** Audit leadership should identify the skills and expertise required for audit team members to effectively conduct the audit engagement and provide training and development if needed.
- **Audit Deadlines**: It is essential to establish realistic and achievable deadlines that align with the timeline of the project or program subject to audit.
- **Hiring Specialists:** It is necessary to assess whether external experts or specialists are needed to support specific areas of the audit.
- **Field Visits:** The sites to be visited or those requiring a field audit should be determined to ensure the necessary information is collected effectively.
- **Other Constraints**: Audit leadership should identify potential challenges or constraints that may arise during the audit engagement while considering their materiality.[57]

3.2 Phase Two: Establishing the Risk Management Framework and Infrastructure

SAIs play a pivotal role in assessing risk management governance, which is one of the key components in establishing an effective framework for risk management in government entities. This framework provides a comprehensive approach to defining the roles and responsibilities of all

[57] Dr. Al-Ghubari, A. (2011). *Training Program: Financial Risk Management and Assessment*.

parties concerned with risk management while ensuring continuous improvement and the adoption of practical techniques and best practices in this domain. Additionally, the framework clarifies the organizational structure and its linkage to supervisory committees, senior management, executives, and other external and internal stakeholders. A well-established risk assessment framework should ultimately ensure the achievement of SAIs' intended objectives.

3.2.1 The Important Role of SAIs in Understanding and Assessing the Risk Management System

The role of SAIs in understanding and assessing the risk management system within their auditees is essential for the following reasons:

- **Enhancing Governance:** SAIs contribute to the adoption of effective governance practices by overseeing the implementation of strategic risk management guidelines.
- **Improving Decision-Making:** SAIs provide their auditees' management with valuable insights and expertise on potential risks, enabling informed decision-making to mitigate threats.
- **Ensuring Effective Risk Management:** SAIs support the implementation of effective risk management plans, which help reduce financial losses, ensure resilience, and improve operational efficiency.
- **Promoting a Risk Management Culture:** SAIs play a key role in raising awareness of risk management practices among auditees' employees and fostering an organizational culture that emphasizes proactive risk identification and effective management.

3.2.2 Objectives and Tasks of Risk Management Units

To ensure integrated oversight of leadership, administrative, and operational functions, a dedicated risk management unit should be established and operate under the direct supervision of senior leadership within the government entity. This unit shall be responsible for periodically reporting on risks potentially facing the entity and effectively taking the necessary measures. Key tasks of a risk management unit include the following:

- Adopting a risk management strategy and policy;
- Reviewing risk reports and conducting risk assessments on a regular basis;
- Following up on the progress of the plans developed to address risks hindering the achievement of organizational objectives;
- Monitoring Key Risk Indicators (KRIs);
- Enhancing risk management to elevate an entity's risk management maturity level;
- Facilitating cooperation and enhancing coordination among the entity's units/departments;
- Managing common and overlapping risks efficiently;
- Monitoring the management of emerging risks; and
- Ensuring the independence of risk management functions and the availability of adequate resources and systems to operate them.

3.2.3 Designing a Robust Risk Management Organizational Structure

Designing a sound, robust organizational structure for risk management requires establishing a dedicated unit, often referred to as the Risk Committee, Risk Management Department, or Internal Audit and Risk Department. Although the names of these units may vary across countries due to differences in governance laws and regulations, they all serve the common purpose of supporting entities' senior management in achieving their strategic objectives. In addition, a well-defined organizational structure enhances the efficiency, effectiveness, and independence of risk management systems within entities. It also contributes to setting effective risk management policies, frameworks, and procedures. When designing a risk management organizational structure, the following key elements should be considered:

- **Clarity of Roles and Responsibilities:** The roles and responsibilities of participants in risk management should be explicitly and distinctly defined. In addition, communication and escalation channels should be systematic.
- **Centralized Decision-Making:** The decision-making process must be concentrated at the appropriate managerial level within the entity to ensure effective risk assessment and timely decisions.
- **Ensuring Expertise and Competencies:** The organizational structure should include individuals with high experience and qualifications in various risk areas, such as financial, operational, technical, and technological risks.
- **Flexibility and Adaptability to Challenges:** The organizational structure should maintain flexibility and adaptability to effectively respond to business environment challenges and emerging risks in a timely manner.
- **Ensuring Effective Communication and Cooperation:** The organizational structure should promote cooperation by incorporating efficient mechanisms for communicating and exchanging risk-related information.
- **Risk Management KPIs:** The organizational structure should ensure the identification and regular monitoring of risk management key performance indicators (KPIs).

3.2.4 Selection Criteria of Risk Management Unit Members

The designation and administrative affiliation of the risk management executives vary depending on the laws and regulations governing government entities in each country, which, as mentioned earlier, may decide to form its risk management unit under the name of a risk committee, risk management department, or internal audit and risk management department. Determining the criteria for selecting the members responsible for risk management is crucial to enhancing the efficiency and effectiveness of risk management processes and ensuring tighter risk control. The selection criteria may include the following:

- **Independence and Transparency:** Members must be completely independent from any internal or external influences, ensuring neutrality and credibility in risk management and decision-making processes.
- **Membership Balance:** When selecting members, it is essential to maintain a balance between external and internal members, ensuring that both internal knowledge of the entity and external best practices are integrated.
- **Distinctive Expertise**: Members must consist of individuals with accumulated experience and exceptional competencies in risk management who can accurately assess and analyze risks in depth and make informed strategic decisions.
- **Diversity of Insights and Ideas**: Members must represent diverse backgrounds and experiences across all sectors of the entity to ensure varied and rich perspectives in the risk management process.
- **Advanced Skills**: Members must possess advanced skills in multiple areas, such as (effective communication, accurate analysis, efficient problem-solving, and decisive decision-making).

- **Compliance and Regulatory Considerations**: When selecting members, it is crucial to ensure compliance with relevant legal and industry standards and regulations, such as financial regulations and international standards, to ensure operational efficiency and the achievement of strategic objectives.

In addition, a risk management unit must have the absolute authority and resources necessary to accomplish its tasks with exceptional efficiency and effectiveness.[58]

3.2.5 Risk Management Framework and Procedures

The risk assessment framework and procedures provide the government entity with the appropriate methodology and mechanisms to achieve optimal maturity levels, focusing on identifying, analyzing, and evaluating risks. Additionally, these frameworks and procedures help determine suitable strategies and plans to address potential risks, thereby reducing their likelihood and impact on the entity. There are four key requirements to consider when developing a risk management framework:

a. Understanding the approaches, vision, and objectives of the government entity and the state.

b. Forming an accurate and comprehensive understanding of general strategies and digital transformation strategies.

c. Reviewing the best practices and international standards to be adopted and adapted in line with the nature and size of the entity's business and organizational maturity.

d. Measuring the entity's strategic and operational performance indicators.

[58] SAB's Auditing Standards and Professional Guidelines Committee. (2022). *Proposed Model for Establishing and Developing a Risk Management Department*. The State Audit Bureau of Kuwait.

3.2.6 Measuring Risk Management Maturity

The strategic objectives of government entities are established based on a well-defined plan aligned with the entity's goals and strategies and, where applicable, the state's vision. An essential factor in developing an effective risk management system and achieving the entity's strategic objectives is the periodic and systematic evaluation of risk management maturity. This assessment should be based on key elements such as:

- Risk Governance and Culture.
- Strategy and Goal Setting.
- Risk Management Performance Evaluations.
- Reviews, Follow-ups, and Refinements.
- Information, Communication, and Reporting.

3.2.7 Risk Assessment and Analysis Methods

Risk assessment is a sensitive process that cannot be eliminated yet controlled through particular controls and regulations. Through effective risk analysis and assessment, government entities can achieve an acceptable level of risk tolerance. In addition to listing internal and external risks faced by the entity, a comprehensive risk assessment should consider the following elements:

a. **Identifying Risk Inputs:** Examining both internal factors (e.g., the nature of the activity, historical data, theoretical analysis, expert judgments, stakeholders' needs and expectations, and operational data) and external factors (e.g., technological developments, competition, and economic changes.) that influence the entity's risk landscape.

b. **Risk Analysis:** Assessing the likelihood of identified risks and determining appropriate risk response strategies.

c. **Key Outputs:** This includes:

- Linking risks to strategic objectives.
- Determining Key Risk Indicators (KRIs).
- Measuring the likelihood of risks or threats affecting the operations and procedures of the government entity.
- Measuring the impact of risks or threats on the operations and procedures of the government entity.
- Assessing risks or threats on an ongoing basis.
- Determining the risk controls and their effectiveness.
- Identifying inherent and residual risk levels.[59]

3.2.8 Risk Assessment Scales

Risk Assessment Scales are tools used to assess potential risks and threats an organization may encounter and determine the extent of their impact and probability of occurrence. There are several scales used for this purpose, including:

- **Probability and Impact Scale**: This scale assesses the likelihood of a specific event occurring and estimates the extent of its potential impact. The impact is typically categorized as low, medium, or high.
- **Relative Importance Scale**: This scale determines the urgency and priority of risks based on their potential impact and the need for immediate action. It helps classify risks

[59] https://shorturl.at/ioQV2

according to their strategic significance and effect on achieving organizational objectives.

- **Velocity Scale**: This scale assesses the speed at which risks develop and the extent of the organization's response, which helps decide the necessity for immediate actions to address emerging risks.
- **Risk Exposure Scale**: This scale evaluates an organization's exposure to specific risks based on several factors, such as geographic location, business activities, and infrastructure.
- **Adjusted Likelihood Scale**: It estimates the probability of an event occurring after considering existing controls and preventive measures. A higher score on this scale indicates that these measures are insufficient.
- **Quantitative Assessment Scale**: This scale converts relative risk estimates into measurable quantitative values, enabling more precise and data-driven risk analysis and assessment.

Risk assessment scales vary according to the needs and context of each organization. The appropriate tools should be employed to ensure a comprehensive and accurate risk assessment, empowering the organization to make optimal and well-informed decisions while enhancing overall risk resilience.

3.2.9 Classification, Determination of Risk Acceptance and Tolerance Levels, and Development of Risk Assessment Criteria

Risk classification and determining its acceptance level are key factors for effective risk management. They help identify appropriate preventive and corrective measures to manage risks efficiently. Therefore, a government entity should:

- gain a comprehensive understanding of the risks facing the entity;
- define the scope and sources of risks, whether internal or external;
- assess the impact of risks on strategic and operational objectives and set the criteria and methods to be used for the analysis and assessment of risks;
- review the internal and external environment, particularly the entity's strategy, objectives, and performance indicators, to establish risk acceptance thresholds.
- establish and develop a mechanism for assessing the adequacy of existing controls to facilitate the ranking and classification of residual risks;
- identify and establish criteria for assessing inherent risks by incorporating risk impact measurements aligned with risk appetite and tolerance thresholds while also integrating probability assessments for risk occurrence to ensure that risk calibration reflects verifiable likelihood estimates; and
- develop appropriate strategies, contingency plans, policies, and procedures to effectively manage identified risks.

3.2.10 Risks Encountered by Government Entities

A thorough understanding of the internal and external risk environment significantly contributes to the success of a risk management plan. The risk environment can be categorized into two main sections, as outlined below.

1. **Internal Sources**

Risks originating from within the government entity, such as:

- **Administrative and Organizational Challenges** (e.g., weak infrastructure, poor human resource management, ineffective strategic planning, and administrative corruption.)
- **Cybersecurity and Data Protection** (e.g., cyber threats and electronic breaches targeting government entities' data, posing a threat to an entity's data confidentiality and information security.)
- **Financial and Accounting Challenges** (e.g., financial waste, forgery, and fraud, as well as concerns related to the mismanagement of financial resources and ineffective financial planning.)
- **Non-Compliance with Laws and Regulations**: The failure of entities to comply with applicable laws and regulations, exposing them to legal penalties and negative consequences.
- **Inefficient Government Performance:** The inability of an entity to deliver governmental services effectively and in alignment with specified standards and expectations**.**

2. **External Sources**

Risks arising from external factors beyond the entity's control, such as:

- **Political Changes:**

Changes in internal or external policies may affect the work of government entities, posing challenges to planning and decision-making processes. Additionally, international and commercial relations, which influence government operations, increase levels of uncertainty and are considered a source of risk.

- **Financial Challenges:**

  These challenges may negatively impact the ability of government entities to provide essential services and meet society’s needs. Examples include budget deficits, insufficient funding, declining revenues, and increasing public debt.

- **Technological Changes:**

  The rapid evolution of technology can create new challenges for government entities, particularly in cybersecurity, artificial intelligence, data protection, privacy, and infrastructure vulnerabilities to cyberattacks.

- **Natural Disasters:**

  Environmental and climate changes pose significant risks to government entities, affecting the infrastructure and causing natural disasters such as floods, droughts, and severe storms. Effective risk management is essential to enhance public environmental sustainability.

- **Security Threats:**

  These threats include terrorism, organized crime, and other illegal activities that target critical infrastructure and databases, posing significant threats to government entities.

- **Demographic and Social Changes:**

  Changes can affect society’s needs and demand for government services. An increase in a particular age group within the population or a change in the society’s demographic composition may require changes in government policies and programs.

- **Economic and Financial Changes**:

  Fluctuations in the economy and financial markets can affect government entities' budgets and ability to deliver government services effectively. [60]

3.2.11 Developing Policies and Work Procedures for Risk Management

Risks are an inherent component of any system or process and cannot be entirely eliminated, as they often stem from uncertainty that is challenging to predict with absolute accuracy. Therefore, it is essential for internal auditors to possess a comprehensive understanding of processes, operations, and methods of risk management, along with strategies for their improvement. Additionally, auditors must be well-versed in the auditee's internal activities, operations, and organizational culture. They should also analyze external factors, assess past performance, and identify strengths and weaknesses to optimize and enhance the risk management process efficiently. There are key procedures enhancing internal auditors' understanding of risk management workflows, including:

- **Assessing risk management strategies** in light of the entity's fundamental mission, values, risk culture, and strategic objectives. This also includes defining the entity's SMART goals in risk management.
- **Assessing risk methodologies,** including defining risk categories encompassing the overall risks surrounding the entity and its strategic objectives.
- **Reviewing risk pool reports** on an entity's strategic level.

[60] *Enterprise and Government Risk Management: Key Components and Objectives*. Retrieved from https://shorturl.at/uvDEX

- **Reviewing high-risk plans** and the necessary reporting mechanisms, including the critical KRIs that affect the achievement of key strategic objectives.
- **Assessing risk monitoring methodologies** widely used to provide stakeholders with an assessment of maximum risk acceptance thresholds.
- **Analyzing mechanisms of decision-making** based on risk assessments of costs and benefits that help stakeholders decide on whether to accept or reject.
- **Defining roles and responsibilities** undertaken by all stakeholders in relation to risk management.
- **Defining the risk management terms of reference matrix,** which describes the functions with responsibilities and duties to be consulted and/or communicated for each risk management activity.
- **Ensuring risk unit communication,** which includes communication with all stakeholders, educating staff about risks, communicating with customers, suppliers, etc., and informing senior management of risks.
- **Monitoring and reviewing risk management processes** on a regular basis, including evaluating the effectiveness of policies and procedures, identifying and evaluating new risks, updating risk mitigation strategies, and making necessary adjustments to the risk management plan.
- **Ensuring the alignment of policies with** risk management strategies and objectives and their compliance with the adopted risk management standard (i.e., ISO 31000:2018 [61] or COSO 2017).[62]

[61] https://shorturl.at/gnoyo

[62] https://shorturl.at/EKNVM.

- **Developing and improving detailed work procedures** clarifying the key procedures for risk management, details of the followed steps, and the parties concerned for their implementation. These procedures should be aligned with risk management policies, standards, and operational models.

In summary, SAI auditors must develop a comprehensive understanding of risk management and conduct thorough assessments. This includes assessing risk strategies and methodologies, defining goals and responsibilities, monitoring performance, and updating procedures. Additionally, they should prioritize enhancing communication and interaction with all concerned parties to ensure the effectiveness, adaptability, and resilience of risk management processes.

Conclusion

To conclude, the following key points have been inferred:

- The public sector has witnessed an increasing interest in risk management and its integration with internal audit functions, necessitating periodic internal and external assessments to ensure that professional quality standards are met.
- Supreme Audit Institutions (SAIs) play a vital role in monitoring and evaluating the performance of internal audits as impartial and independent external oversight bodies. This role contributes to the development of risk management systems in government entities and raises their readiness to address recurring and emerging risks. It ensures that audit tasks are conducted with high professional quality using advanced audit and evaluation methodologies that correspond to an entity's evolving risks. Additionally, SAIs provide recommendations to improve internal audit and risk management practices within government entities, strengthening their risk systems and enhancing preparedness for emerging risks.
- Many leading companies are leveraging Artificial Intelligence (AI) and Machine Learning (ML) technologies to effectively identify, analyze, and manage risks, recognizing their substantial benefits in this field.
- The adoption of AI and ML technologies presents a valuable opportunity for organizations to enhance their capabilities and improve risk management practices. To further explore this topic, the role of these technologies in risk management will be discussed in the next section, under Theme 4 of this chapter.

Theme 4 :The Use of Artificial Intelligence and Machine Learning Technologies in Risk Management

Introduction

Risk management has become a fundamental component of organizational strategy in today's dynamic and complex work environment. Organizations are exposed to new and evolving risks that can significantly affect their operations, financial stability, administrative functions, reputation, and long-term sustainability. To mitigate these risks and facilitate the enhancement and automation of risk management and analysis processes, many audit firms have adopted Artificial Intelligence (AI) and Machine Learning (ML) technologies. The following section focuses on the concepts of AI and ML in risk management and explores how these technologies can effectively reduce risks while maximizing their benefits.[63]

4.1 History of Artificial Intelligence

In the mid-20th century, scientists began to explore innovative approaches to building intelligent machines. Advances in neuroscience and cybernetics have paved the way for the development of sophisticated computers and technological devices designed to replicate human cognitive processes. The term "Artificial Intelligence" (AI) was first coined in 1956 by John McCarthy at Dartmouth College, focusing on creating intelligent systems capable of solving complex problems. Since then, AI has experienced tremendous advancements, driven by progress in computing technology and the emergence of ML algorithms.[64]

[63] https://shorturl.at/Od4Y4

[64] https://shorturl.at/muoHp

4.2 Definition of Artificial Intelligence

Artificial Intelligence (AI) refers to the intelligence exhibited by machines and software that simulate human cognitive abilities and function patterns, including learning, reasoning, and responding to non-programmed situations. AI is also recognized as an academic discipline dedicated to the development of computers and software capable of exhibiting intelligent behavior.

Leading researchers define AI as "*the study and design of intelligent systems that assimilate their environment and take actions that increase their chances of success*." John McCarthy, who first coined the term in 1956, described AI as "*the science and engineering of making intelligent machines.*"

In recent years, AI technology has made great strides in mimicking human intelligence, with "deep learning" technology emerging as one of its most groundbreaking developments. Deep learning relies on artificial neural networks that replicate the structure and functionality of the human brain, enabling systems to experiment, learn, and self-improve without human intervention.[65]

4.3 Key Artificial Intelligence Tools

Key AI technologies encompass algorithms and computational tools designed to enable systems to simulate human cognitive abilities. These technologies include:

a. **Machine Learning (ML):** A branch of AI that focuses on developing algorithms to enable computers to learn from data rather than being explicitly programmed. Machine learning models are trained on large datasets to recognize patterns and make decisions. The primary types of machine learning include:

[65] https://shorturl.at/N3nvw

- **Supervised Learning:** The model is trained on labeled data, where inputs are mapped to corresponding outputs. It learns to identify relationships between inputs and outputs to predict future outcomes.
- **Unsupervised Learning:** The model is trained on data without labeled outputs, aiming to detect patterns or clusters within the dataset.
- **Reinforcement Learning:** The model learns decision-making through trial and error, receiving rewards for good decisions and penalties for bad ones.

b. **Deep Learning:** An advanced form of ML that uses artificial neural networks with multiple (deep) layers to process data and extract features. It helps process images, sound, and text, as it can accurately identify complex patterns.

c. **Natural Language Processing (NLP):** A branch that focuses on the interaction between computers and human languages. It enables machines to analyze texts, perform machine translations, and recognize speech. NLP technologies help machines understand and generate human language, facilitating more natural and effective human-machine interactions.

d. **Computer Vision:** A technology that enables computers to interpret and extract meaningful insights from images and videos. It includes face recognition, video analysis, and robotic vision. Computer vision heavily relies on deep learning to process and analyze images effectively.

e. **Robotics:** A multidisciplinary field that combines AI and engineering to develop machines capable of performing physical tasks in the real world. Robots use AI to interact with their surroundings and make independent decisions.[66]

[66] - https://www.argaam.com/ar/article/articledetail/id/1615530
- https://shorturl.at/7sAMa

4.4 Role of Artificial Intelligence and Machine Learning in Risk Management

AI and ML technologies have revolutionized the way organizations manage risks. By leveraging these technologies, they can now automate identifying, analyzing, and managing risk, leading to more accurate and efficient risk management strategies. AI and ML algorithms are capable of processing vast amounts of data in real-time, identifying patterns, and making predictions based on that data, enabling organizations to make well-informed decisions.

4.5 Role of Artificial Intelligence and Machine Learning in Risk Analysis

One key benefit of AI and ML in risk management is their ability to identify risks more efficiently. These technologies analyze large volumes of data from various sources, including historical data, past risk events, social media, and news outlets, to detect potential risks that humans might have overlooked. Additionally, AI and ML identify trends and patterns that offer valuable insights into the possible impact of a risk event.[67]

4.6 Application of Artificial Intelligence in Risk Management

AI applications in risk management are diverse and advanced, helping organizations predict, reduce, and manage risks more effectively. Below are some of the most prominent applications:

a. **Big Data Analysis:** AI is able to process and analyze vast amounts of data quickly and effectively, allowing organizations to detect hidden patterns and potential risks.

[67] https://shorturl.at/Psc03

b. **Fraud Detection:** AI employs deep learning techniques and neural networks to identify fraudulent activities quickly and efficiently. It continuously monitors financial transactions and recognizes unusual patterns that may indicate fraud. This capability helps reduce financial losses and protect public assets.

c. **Risk Prediction:** ML algorithms are used to predict future risks based on historical data. It enables organizations to take proactive measures to mitigate the impact of potential risks. For instance, predictive analytics can identify economic trends that adversely affect the state's public budget or financial performance.

d. **Internal Process Risk Management:** AI improves internal processes by analyzing workflows, identifying vulnerabilities, and predicting potential errors, whether human or technical. It enables organizations to take preventive measures, enhance efficiency, and reduce the likelihood of risks.

e. **Credit Assessment and Risk Management:** AI analyzes financial data to assess credit risk levels, identify client risks, and support more accurate decision-making.

f. **Cyber Risk Management:** AI is crucial in enhancing cybersecurity by detecting and responding to cyber threats. It identifies potential attacks before they occur and analyzes abnormal patterns to detect breaches. Additionally, it helps protect sensitive data while preventing cyberattacks that could cause significant harm.

g. **Health Risk Analysis:** AI analyzes health data in order to predict future health risks and potential epidemics. By examining medical histories and environmental factors, AI identifies patients at higher risk of certain health conditions, enabling the state and doctors to take early preventive measures.

h. **Environmental Risk Analysis:** AI analyzes environmental data to predict environmental hazards and natural disasters. These applications help identify areas prone to floods, earthquakes, and storms, facilitating planning and taking preventive measures to protect infrastructure and populations.

i. **Crisis Management:** AI analyzes data at an exceptional speed to provide effective recommendations for managing crises. It evaluates various scenarios and makes optimal decisions to address crises. For instance, AI can analyze weather and infrastructure data to guide efficient resource distribution when a natural disaster strikes.

j. **Behavioral Analysis:** AI analyzes employee and client behavior to identify unusual behaviors that may indicate potential risks.

k. **Social and Political Risk Analysis:** AI can analyze social and political data to predict events that could affect workflow. Predictive models identify social and political risks by analyzing data from social media and news outlets and suggest measures to mitigate their effects.

l. **Decision-making Support:** AI provides data-driven insights to support the decision-making process. By analyzing available data and delivering precise recommendations, AI enables decision-makers to make informed decisions, reducing risks associated with uninformed decisions based on insufficient information.[68]

4.7 Benefits of Artificial Intelligence and Machine Learning in Risk Management

The use of AI and ML provides numerous benefits that improve organizations' capacity to manage risks more effectively. These benefits are outlined below:

[68] https://www.argaam.com/ar/article/articledetail/id/1615530

a. **Prediction accuracy:** AI and ML can analyze large datasets with high precision, improving the accuracy of risk prediction. In addition, ML algorithms can identify hidden patterns in historical data and accurately predict future events.

b. **Early risk detection:** Intelligent systems enable continuous data analysis and early detection of abnormal patterns before risks escalate, allowing for timely take of preventive measures.

c. **Intelligent Process Automation (IPA):** AI automates processes related to risk management, reducing the need for human intervention and minimizing errors. It contributes to greater efficiency and faster responses to risks.

d. **Real-time data analysis:** AI enables data to be analyzed in real-time, allowing continuous monitoring and evaluation of risks. It supports faster decision-making and more informed work strategies.

e. **Efficient resource allocation:** AI helps allocate resources and prioritize them more effectively based on accurate risk assessments, directing them to areas of greatest need and increasing the efficiency of risk management.

f. **Improving customer experience:** AI applications help improve customer experience by detecting errors and fraud and offering safer and more reliable services.

g. **Adapting to dynamic changes**: AI can adapt to dynamic changes in the surrounding environment. Through continuous learning, intelligent systems respond effectively to unexpected changes in risks.

h. **Improving compliance with laws and regulations:** AI supports compliance with laws and regulations by monitoring processes and providing accurate compliance reports. It reduces legal and regulatory risks, safeguarding the organization from potential penalties.

i. **Enhancing innovation and development:** Advanced AI applications in risk management drive continuous innovation and development. By streamlining processes and delivering innovative solutions to complex challenges, these applications enable organizations to achieve sustainable progress and improve their competitiveness in the market.[69]

4.8 Comparison between Traditional Management and the Use of Artificial Intelligence in Risk Management

AI and ML technologies have brought revolutionary changes to risk management, introducing significant differences compared to traditional human-based approaches. While AI relies on programmed data, analytical rules, and algorithms for managing risks, traditional methods depend on human creativity and personal experiences from life and social interactions. These differences are summarized as follows:

a. **Data collection and analysis:** Traditional management relies on manual data collection and analysis or the use of basic systems, which are often limited and slow in handling large volumes of data. In contrast, AI employs intelligent machine learning technologies capable of collecting and analyzing large datasets quickly and efficiently, with the ability to self-improve.

b. **Prediction and decision-making:** Traditional management relies on managers' limited experience and simple statistical models to predict risks, which may not effectively address complex or uncertain data. In contrast, AI utilizes advanced algorithms to predict risks and make decisions, offering better handling of uncertainty and complexity while providing accurate recommendations.

[69] https://shorturl.at/Psc03

c. **Responsiveness and adaptability**: In traditional management, human responses can be slow in reacting to emergency changes and adapting to new situations. On the other hand, AI can respond rapidly to changes in surrounding conditions.

d. **Costs and efficiency:** In traditional management, human-based approaches are often more expensive and less efficient. AI reduces costs through automation and high efficiency in data analysis and risk management.

e. **Accuracy and comprehensiveness:** Traditional management relies on human estimations, which lack accuracy and comprehensiveness in risk analysis. Conversely, AI provides more accurate and comprehensive analytics due to its ability to process and analyze large datasets from multiple sources.[70]

In summary, utilizing AI in risk management offers high accuracy, speed, and efficiency. It enhances compliance monitoring and enables faster threat detection. It also reduces costs associated with human errors and corrective actions, ensuring more effective future risk prediction and better-informed decision-making.

4.9 Global Experiences in Using Artificial Intelligence Technologies

The world is witnessing a transformative shift driven by AI applications across various fields, including healthcare, industry, education, transportation, smart cities, and more. Below are some notable global experiences where AI technologies have been successfully adopted:

[70] https://shorturl.at/9rkwv

a. **McKinsey & Company** has developed a generative AI-powered virtual expert capable of providing tailored answers based on the company's proprietary information and resources. It allows for the development of similar tools that analyze transactions, detect warning signals, monitor market news, assess asset price changes, and more. These tools enable more precise decision-making in risk management and evaluate climate risks, offering detailed answers to stakeholders' inquiries.[71]

b. **Tesla** and **General Motors (GM)** utilize intelligent automation (IA), robotics, and intelligent risk management systems in the automotive industry. These technologies provide numerous benefits, such as improving the accuracy of risk prediction, reducing human errors, enhancing safety, and increasing operational efficiency. As a result, they contribute to lowering costs, increasing productivity, and improving profitability.

c. Hospitals like the **Mayo Clinic** and **Cleveland Clinic** use IA in healthcare to analyze medical data, improve disease diagnosis, and provide personalized treatment plans. In addition, **IBM Watson Health** offers AI-powered solutions to analyze medical records and improve patient care. These solutions improve diagnosis and treatment accuracy, reduce medical errors, optimize health data management, and provide predictive maintenance for medical devices. They also enhance safety and crisis management and improve operational efficiency and patient experience, thus minimizing health-related risks and improving healthcare quality.

d. **Deloitte** and **PricewaterhouseCoopers (PwC)**, among the world's largest professional services firms, use AI in auditing, reviewing, and consulting to improve auditing processes, analyze financial data, identify unusual patterns, and deliver advanced analytical insights.

[71] https://shorturl.at/F5AQF

e. **NASA** employs IA to execute scientific data analysis and space expeditions with greater precision. It also uses AI to enhance public sector services by improving accurate risk prediction, strengthening cybersecurity, enhancing crisis and emergency management, increasing operational efficiency, monitoring compliance, promoting transparency and accountability, and managing environmental risks. Additionally, **NASA** aims to improve the concept of citizen experience, contributing to more effective and responsive government services.

f. In telecommunications, **AT&T** uses IA to enhance customer services by handling technical inquiries and providing faster support. In addition, **Verizon** relies on IA to improve network operations and predictive maintenance, enabling early identification of potential malfunctions and ensuring service continuity. [72]

4.10 SAIs' Experiences in Using Artificial Intelligence Technologies

Supreme Audit Institutions (SAIs) have prioritized the use of modern technology tools in performing audit tasks to keep pace with global advancements. With the increasing reliance of government entities on electronic systems, manual auditing of such vast amounts of data has become increasingly challenging. It has created a growing need for electronic auditing tools that align with advancements in data storage methods and their immense volume. In addressing this challenge, SAI Jordan has implemented a mechanism for digital transformation across all its

[72] https://shorturl.at/XCk0u

- Arntz, M., Gregory, T., & Zierahn, U. *The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis*. OECD Social, Employment and Migration Working Papers.
- Frey, C. B., & Osborne, M. A. (2017). *The Future of Employment: How Susceptible are Jobs to Computerization?* Technological Forecasting and Social Change Journal. Volume 114.

operations, aiming to improve the quality of audit processes and outputs, enhance the work environment, and increase efficiency.[73]

On another note, the "UAE National Strategy for Artificial Intelligence 2031" was launched in 2017. Its goal is to enhance government performance, reduce risks, and cut costs across various state sectors by 2031. This strategy also aims to deliver high-quality audits as part of the transition from a traditional era to a digital one.[74]

EUROSAI has gradually introduced technologies such as automation, robotics, data analysis tools, and AI into the audit process. For instance, Denmark has analyzed big data and developed methods for presenting data within shorter timeframes.[75] SAI Norway used the R programming tool for data analysis, enabling integration between IT specialists, financial auditors, and IT auditors[76]. SAI Netherlands also identified that the predictive and learning algorithms employed by the government for decision-making were relatively simple and classified some algorithms as AI. [77]

4.11 Developing a Framework for SAIs to Audit Risk Management Systems Using AI

Developing strategies for SAIs to implement AI-powered risk management systems requires the adoption of a comprehensive and integrated framework for technology and infrastructure. Below are some strategies that can support this objective:

[73] Directorate of Information Technology of SAI Jordan. *Strategic Plan 2021/2023: Digital Transformation Project*.

[74] SAI UAE. *Artificial Intelligence: A Remarkable Advancement in Public Sector Audit (working paper).*

[75] *The 2nd Meeting of the INTOSAI Working Group on Big Data*. (2018, April 19-20). Washington, DC, USA.

[76] EUROSAI IT Working Group. (2020, November 12). *SAIs and the Digital Turn e-Seminar: Data Analysis and IT Auditing of SAI Norway*.

[77] Meijer-van Leijsen, E., Verhulst, J., Oosterwijk, P., & Pirkovski, M. *Developing an Audit Framework for Algorithms*. INTOSAI Journal. Spring 2021 Edition.

a. Technical Infrastructure:

Cloud computing platforms are used to store and process large volumes of data efficiently and effectively. A flexible and integrated data architecture is developed to allow for easy data collection, storage, and analysis from multiple sources.

b. ML Technologies:

Machine learning techniques are used to analyze big data, detect unusual patterns that indicate potential risks, and extract actionable insights to mitigate those risks. Deep learning techniques are also used to analyze complex data and improve the accuracy of predicting internal and external risks.

c. Risk Detection Systems:

This strategy involves developing advanced algorithms to promptly detect internal or external fraud risks and implementing continuous monitoring systems to identify unusual activities.

d. Data Management Enhancement:

It involves integrating data collected from various sources, such as financial systems, audit reports, and internal records, to improve the accuracy and comprehensiveness of analyses.

e. Continuous Evaluation and Improvement:

SAIs may employ Key Performance Indicators (KPIs) to monitor performance and evaluate the effectiveness of risk management systems, analyze outcomes, and update models and algorithms based on feedback and new data.

f. Compliance with Regulations and Standards:

SAIs should ensure that AI technologies comply with local and international regulations and standards and conduct regular legal and ethical assessments to ensure responsible and transparent use of AI.

g. **Change Management:**

This strategy involves raising employees' awareness of the importance and potential benefits of using AI in risk management and developing a comprehensive change management plan covering all aspects of digital transformation and the implementation of AI technologies.

h. **Developing Organizational Solutions**:

This includes creating customized solutions tailored to the needs of SAIs that integrate with existing systems, encouraging continuous innovation, and developing new AI-driven applications to meet evolving needs.

i. **Training and Human Resources Development:**

SAIs should organize continuous training programs and workshops for employees on AI and ML technologies and establish partnerships with universities and research centers to develop specialized training programs in AI.

j. **Enhancing Internal and External Cooperation:**

This strategy involves strengthening cooperation between various SAIs to ensure coordinated efforts and information exchange while establishing partnerships with technology companies and research institutions to develop innovative solutions in risk management.

Conclusion

From the above, we conclude the following:

AI and ML are potent tools for automating risk management. These technologies enable the analysis of vast amounts of data with speed and precision, aiding in predicting potential risks and supporting informed decision-making compared to traditional methods. They also enhance operational efficiency and reduce human error, increasing the ability to respond swiftly to sudden changes in the work environment.

Supreme Audit Institutions (SAIs) play a vital role in advancing risk management systems by integrating these modern technologies, which have become indispensable to many auditing organizations. Their application enhances the accuracy and efficiency of audit and review processes, allowing the early detection of threats and risks before they escalate into significant issues. Moreover, these SAIs contribute to setting recommendations, standards, and guidelines to ensure that AI and ML are utilized in ways that promote transparency and fairness.

By integrating AI into SAIs, a more advanced and proactive risk management system can be created, strengthening organizations' sustainability and success. The continued development of AI applications is expected to further enhance risk management capabilities, making them more integrated and contributing to long-term sustainability and success.

Alternatively, the following chapter addresses the field study and statistical analysis to assess the research hypotheses.

Chapter 3: Statistical Analysis

- **Theme 1: Field Study**

- **Theme 2: Validation of Study Hypotheses and Conclusions**

Chapter 3: Statistical Analysis

Theme 1: Field Study

Introduction

This chapter addresses key findings of the field study, enriching both the research topic and its scientific content while contributing to the achievement of the study's objectives. Following the field study methodology outlined in the research plan, which aims to collect data on the **role of SAIs in enhancing risk management systems in government entities**, the collected data were processed into tables and analyzed using specific statistical methods provided by the SPSS Statistical software. Below is an analysis of the study survey:

Descriptive Analysis of the Survey:

- **Study population**: The study population comprises a diverse group of professionals holding technical positions within the audit sectors of Arab SAIs.
- **Study sample:** The survey was distributed via email using a unique Google Drive survey link, allowing designated respondent groups to complete the survey online. A total of 120 participants from different Arab SAIs responded to the survey, yielding a 100% response rate. All responses were submitted via the automated system with no exclusions.
- **Study tool:** An online survey was employed to test the proposed hypotheses of the study. It comprised thirty-three close-ended questions, in addition to three questions related to personal information. The study survey was structured as follows:
  1. **Section One** consists of (3) statements covering respondents' personal information, which are (years of experience, academic qualifications, and professional certificates).
  2. **Section Two** (independent variables) comprises four parts:

- Part 1 consists of (6) statements addressing the impact of the auditor’s academic qualifications and professional competence on improving risk management.
- Part 2 consists of (7) statements addressing the effect of reviewing internal audit regulations on enhancing audit efficiency and improving risk management.
- Part 3 consists of (7) statements addressing how internal audit procedures contribute to mitigating risks in government entities.
- Part 4 consists of (7) statements addressing the impact of AI on developing risk management systems in government entities.

3. **Section three** (dependent variable) examines the role of SAIs in enhancing risk management systems in government entities.

Three-point Likert scale was used for the survey with the following options: (Agree - Neutral - Disagree).

Data analysis method:

The researcher used SPSS to arrive at both descriptive and inferential analysis results. The analysis evaluates the number and percentage of responses across different survey areas, assessing the validity and reliability of the study’s data collection tool (the online survey), and measuring the internal consistency of the study variables.

The researcher relied on the following statistical methods:

1. Scale Reliability Analysis Using Cronbach's Alpha

Scale reliability refers to how a test produces consistent results when reapplied to the same group of individuals. This implies that changes in external factors or conditions do not significantly affect the test. Cronbach's Alpha represents the correlation coefficient between various parts of the test, reflecting the scale’s internal consistency. To ensure the validity of the survey as a data collection tool for the study, the reliability of this tool was assessed using Cronbach's Alpha, as shown below:

	Study Variables and Dimensions	Number of Statements	Cronbach's Alpha
1	Impact of academic qualification and professional competence on developing risk management systems	6	93.9%
2	Impact of reviewing internal audit management systems and regulations on developing risk management systems	7	90.6%
3	Impact of internal audit procedures on mitigating risks in government entities	7	92 %
4	Impact of using AI on developing risk management systems in government entities	6	91.2%
5	SAIs’ role in developing risk management systems in government entities	6	92 %
	Overall Scale	33	93.4%

Table 2: Reliability Level of Study Variables

The table above indicates that the reliability of individual dimensions- ranging from (1) to (5)- exceeds 90%, while the overall reliability for the survey is 93.4%. This demonstrates that the scale is reliable for measuring the study’s dimensions, given that a reliability threshold of 60% is considered acceptable for generalizing results in such studies.

2. Measures of Central Tendency

- **Arithmetic Mean**: Represents a value around which a set of data points converge, providing a basis for evaluating the relative importance of the statements included in the survey.

- **Standard Deviation:** A measure of statistical dispersion that indicates the extent to which data points are spread out within a dataset. It is calculated as the square root of variance and indicates the extent to which values are distributed within the dataset.

- **Simple Linear Regression Analysis:** A method to predict unknown data values based on related data points. It involves creating a mathematical model for the relationship between the dependent and independent variables as a linear equation.

3. Descriptive Statistics

Descriptive statistics involve a set of processes used to describe the fundamental characteristics of data within the study variables. These include:

- **Percentages**: Used to extract trends in categorized data, supporting or refuting the primary hypotheses.

- **Frequency Distribution Tables**: A measure used to reflect the dispersion or spread of frequency distributions.

4. Measurement of Study Variables

With regards to the thresholds adopted in this study for interpreting the variables' arithmetic mean in the research model, three measurement levels are defined (Low, Medium, and High), as detailed below:

Level	From	To
Low	1	1.66
Medium	1.67	2.33
High	2.33	3

Table 3: Measurement of Study Variables

Theme 2: Validation of Study Hypotheses and Conclusions

This section presents the findings derived from the application of the statistical methods employed in the analytical study.

Since this study focuses on SAIs' role in developing risk management systems in government entities and testing their implementation across SAIs, a random sample of employees (auditors) working in SAIs was selected. This sample was chosen to highlight specific facts about its members and their characteristics, given the large size of the study population and the desire to reduce the time and costs associated with data collection. Below are the details of the study sample:

1. Characteristics of the Study Sample

First: Years of Experience

Characteristic	Categories	Frequency	Percentage
Years of Experience	Less than 5 years	31	26%
	5 – 15 years	28	23%
	16–20 years	29	24%
	More than 20 years	31	27%

Table 4: Characteristics of Study Sample

The table above indicates a relatively even distribution of years of experience among the categories of auditors from the entities under study. The largest category consists of auditors with over 20 years of experience, totaling 31 individuals, representing 27% of the sample. The second largest category includes those with less than 5 years of experience, accounting for 26% of the sample. Auditors with 16-20 years of experience account for 24% of the sample, while those with

5-15 years of experience represent 23%. The researcher interprets that the distribution of participation across the experience categories is relatively balanced, which aligns with the study's objectives.

Second: Academic Qualification

Characteristic	Categories	Frequency	Percentage
Academic Qualification	Diploma	3	3%
	Bachelor's	101	84 %
	Master's	11	9%
	Doctorate	5	4%

Table 5: Academic Qualification

The table above indicates that the majority of the study sample, consisting of SAI auditors, holds a bachelor's degree, accounting for 84%. Respondents with a master's degree constitute 9%, followed by those with a doctorate at 4%. Lastly, diploma holders represent 3% of the sample.

The researcher finds that the number of SAI auditors with bachelor's degrees represents the most prominent category among the academic qualification categories. A high level of education is a fundamental requirement, especially since the nature of risk management demands diverse academic degrees that equip auditors with the required skills to address the rapid developments in risks and methods for effective management.

Third: Professional Certificates

Characteristic	Categories	Frequency	Percentage
Professional Certificates	CFA	5	4%
	CISA	6	5%
	CMA	5	4%
	CPA	3	3%
	CIA	6	5%
	No Certification	95	79%

Table 6: Professional Certificates

Table (6) shows that the majority of the study sample, representing 79% of the total, lack professional certifications. Meanwhile, individuals holding various professional certifications count for 21% of the sample.

The researcher interprets the finding as an indication that professional qualifications are essential in the field of auditing. Such qualifications equip auditors with in-depth knowledge and advanced skills in auditing and risk management. They also enable auditors to understand and implement best practices and international standards, enhancing their ability to effectively evaluate risk management systems and audit processes. These competencies allow auditors to identify challenges and vulnerabilities at an early stage and address them proactively.

2. Testing Data Normality for Study Dimensions (Descriptive Statistical Analysis):

The researcher conducted a descriptive statistical analysis of the study dimensions to evaluate the effect of each independent variable individually. The findings were as follows:

a. Findings Related to the (Independent) Variable: Academic Qualification and Professional Competence of Internal Auditors

	Variables	Mean	Standard Deviation	Rank	Role Level
1	Helping auditors keep up with developments in international auditing standards	2.35	0.706	3	High
2	Significantly helping improve work quality and precision	2.30	0.830	5	Medium
3	Enabling the fulfillment of professional responsibilities efficiently and effectively	2.47	0.579	1	High
4	Enhancing auditors’ understanding of professional behavior, ethics, and compliance	2.37	0.685	2	High
5	Improving auditors’ efficiency and effectiveness in risk management	2.31	0.742	4	High
6	Enhancing auditors’ understanding of their legal rights and responsibilities	2.28	0.769	6	High
	Overall Dimension Level	2.35			High

Table 7: Arithmetic Means and Standard Deviations for the Variable: Academic Qualification and Professional Competence of Internal Auditors

The table above presents study sample responses regarding the independent variable "Academic Qualification and Professional Competence of Internal Auditor," along with the corresponding arithmetic means and ranking. The results indicate that the variable "Enabling the fulfillment of professional responsibilities efficiently and effectively" ranked first, with the highest mean score of (2.47). In contrast, the variable "Enhancing auditors’ understanding of their legal rights and responsibilities" ranked last, with a mean score of (2.28). Overall, the arithmetic means for all variables related to the academic qualifications and professional competence of internal auditors were rated at a high level of (2.35), reflecting a generally high level of importance as perceived by the study sample.

b. Findings Related to the (Independent) Variable: Importance of Reviewing Internal Audit Management Regulations

No.	Variables	Mean	Standard Deviation	Rank	Role Level
1	Reviewing contributes to assessing risk management and providing recommendations for its improvement.	2.08	0.842	7	Medium
2	Ensures the linkage of internal audit management to higher levels as a key element in enhancing risk management control.	2.37	0.647	5	High
3	Reviewing the internal audit charter contributes to improving audit activities and mitigating control risks.	2.54	0.564	1	High
4	Increases internal auditors’ understanding of the risk culture surrounding the entity and enhances their awareness.	2.42	0.656	4	High
5	Periodical evaluation of auditors contributes to motivating their performance and enhancing the efficiency of risk management control.	2.46	0.634	3	High
6	Ensures the alignment of frameworks with laws and regulations consistent with the nature and size of activities.	2.20	0.795	6	Medium
7	Requires senior management to monitor and develop risk management.	2.49	0.594	2	Low
	Overall Dimension Level	2.36			High

Table 8: Arithmetic Means and Standard Deviations for the Variable: Importance of Reviewing Internal Audit Management Regulations

Table (8) demonstrates the responses of the participants regarding the independent variable, "Importance of Reviewing Internal Audit Management Regulations," along with corresponding arithmetic means. The statement "Reviewing the internal audit charter contributes to improving audit activities and mitigating control risks" ranked first with the highest mean score of (2.54). In contrast, the statement, "Reviewing contributes to assessing risk management and providing recommendations for its improvement," ranked seventh with a mean score of (2.08). Overall, the arithmetic mean for the statements associated with this variable was (2.36), indicating a high level of importance as perceived by the study sample.

c. Findings Related to the (Independent) Variable: The Contribution of Internal Audit Procedures to Mitigating Risks in Government Entities

No.	Variables	Mean	Standard Deviation	Rank	Role Level
1	Adopting the International Standards for the Professional Practice of Internal Auditing (IIA's Standards) to develop a comprehensive risk audit plan.	2.70	0.460	1	High
2	Identifying and analyzing risk levels based on clear criteria in coordination with management.	2.18	0.840	7	Medium
3	Studying the entity's future risk strategy and ensuring its timely management.	2.35	0.644	5	High
4	Periodically evaluating and monitoring the effectiveness of internal control systems for risk management.	2.41	0.655	4	High
5	Following up on senior management decisions regarding risk response and their implementation.	2.25	0.833	6	Medium
6	Monitoring the promptness of executive management in implementing appropriate corrective actions.	2.52	0.622	2	High
7	Considering risks highlighted in reports from external SAIs.	2.45	0.620	3	High
	Overall Dimension Level	**2.40**			**High**

Table 9: Arithmetic Means and Standard Deviations for the Contribution of Internal Audit Procedures to Mitigating Risks in Government Entities

Table (9) outlines the responses of the study sample regarding the independent variable, "The Contribution of Internal Audit Procedures to Mitigating Risks in Government Entities," along with the corresponding arithmetic means. The statement "Adopting the International Standards for the Professional Practice of Internal Auditing (IIA's Standards) to develop a comprehensive risk audit plan" ranked first, achieving the highest score of (2.70). Whereas the statement, "Identifying and analyzing risk levels based on clear criteria, in coordination with management," ranked last with a score of (2.18). Overall, the findings suggest that internal audit procedures significantly contribute to mitigating risks in government entities, as reflected by the overall mean score of (2.40), indicating a high level of importance according to the study sample.

d. Findings Related to the (Independent) Variable: The Use of AI in Enhancing Risk Management Systems

No.	Variables	Mean	Standard Deviation	Rank	Role Level
1	Applying AI technologies in control systems enhances the effectiveness of risk monitoring and assessment in government entities.	2.08	0.842	3	High
2	SAIs' role should include supporting the development of risk management systems using AI technologies.	2.37	0.647	5	Medium
3	Government entities are adequately prepared to adopt AI technologies in risk management systems.	2.46	0.634	4	High
4	Employees of SAIs should receive training in using AI technologies to develop risk management systems.	2.42	0.656	2	High
5	Using AI in risk management systems increases efficiency and reduces risks.	2.54	0.564	1	High
6	Utilizing AI technologies in a risk management system contributes to reducing costs or increasing profitability.	2.20	0.795	6	High
	Overall Dimension Level	**2.34**	**0.351**		**High**

Table 10: Arithmetic Means and Standard Deviations for the Use of AI in Enhancing Risk Management Systems

Table (10) outlines the responses of participants regarding the independent variable, "The Use of AI in Enhancing Risk Management Systems," along with the corresponding arithmetic means. The statement, "Using AI in risk management systems increases efficiency and reduces risks," ranked first with the highest mean (2.54). Conversely, the statement, "Utilizing AI technologies in risk management systems contributes to reducing cost or increasing profitability," ranked sixth with a mean of (2.20). The overall findings indicate that the use of AI in enhancing risk management systems is perceived at a high level, with an overall arithmetic mean of (2.34), reflecting the perspectives of the study sample.

e. Findings Related to the (Dependent) Variable: The Development of Risk Management Systems in Government Entities

No.	Variables	Mean	Standard Deviation	Rank	Role Level
1	Linking risk management performance with the entity's performance, employees, and executive management.	2.70	0.460	1	High
2	Ensuring leadership support, participation, and commitment in implementing the risk management strategy and framework.	2.18	0.840	7	Medium
3	Understanding, analyzing, assessing, and proactively managing internal and external risks.	2.35	0.644	5	High
4	Identifying and managing overlapping and shared risks with internal and external shareholders in an integrated and systematic manner.	2.41	0.655	4	High
5	Adopting a phased approach to implementing the risk management framework.	2.25	0.833	6	Medium
6	Focusing on implementing a methodology for identifying, analyzing, and assessing risks rather than solely addressing current challenges.	2.52	0.622	2	High

No.	Variables	Mean	Standard Deviation	Rank	Role Level
7	Using a risk management guide improves decision-making, enhances accountability, transparency, and efficiency, ensures compliance, raises awareness, and elevates the reputation of the government entity.	2.45	0.620	3	High
	Overall Dimension Level	**2.40**	**0.361**		**High**

Table 11: Arithmetic Means and Standard Deviations for the Development of Risk Management Systems in Government Entities

Table (11) outlines the participants' responses regarding the dependent variable, "The Development of Risk Management Systems in Government Entities," along with the corresponding arithmetic means. The statement, "Linking risk management performance with the entity's performance, employees, and executive management," ranked first with the highest mean score of (2.70). Conversely, the statement, "Ensuring leadership's support, participation, and commitment in implementing the risk management strategy and framework," ranked last with a mean score of (2.18). Overall, the findings indicate that the development of risk management systems in government entities is considered significant, with an overall mean of (2.40). This result reflects the perspectives of the study sample.

3. Descriptive Statistics for the Combined Independent Variables of the Study

This study sought to address the research questions and hypotheses that constitute the core of the research problem. Arithmetic means, and standard deviations were calculated for all questions related to the independent variables concerning the role of SAIs in developing risk management systems in government entities. The following table summarizes the results for the combined independent variables:

No.	Variables	Mean	Standard Deviation	Rank	Role Level
1	Academic qualifications and professional competence of internal auditors.	2.345	0.408	3	High
2	Importance of reviewing internal audit management regulations.	2.364	0.345	2	High
3	Contribution of internal audit procedures to mitigating risks in government entities.	2.408	0.361	1	High
4	Use of AI in enhancing risk management systems	2.343	0.351	4	High
	Overall Dimension Level	**2.379**	**0.327**		**High**

Table 12: Arithmetic Means and Standard Deviations for the Combined Independent Variables of the Study

Table (12) demonstrates the arithmetic means and standard deviations for the combined independent variables related to the role of SAIs in developing risk management systems in government entities. The results indicate that all independent variables were evaluated at a high level, with an overall mean of (2.379). These findings reflect the perspectives of the study sample.

4. Testing the Validity of the Study Hypotheses (Using SPSS Statistical Software)

Testing the Primary Hypothesis (Simple Linear Regression Test)

a. **Hypothesis (1)**: There is no statistically significant relationship at the significance level (a=0.05) between auditors' academic qualifications and professional competence and the development of risk management systems in government entities.

The following table outlines the results of the statistical analysis of this relationship using the simple linear regression test:

Statement	R (Correlation Coefficient)	R² (Coefficient of Determination)	T (Calculated)	B (Beta Coefficient)	Sig (Significance Level)
Auditors’ academic qualifications and professional competence influence the development of risk management systems in government entities.	.586	.344	7.861	.510	0.000

Table 13: Hypothesis (1) Statistical Analysis Using Simple Linear Regression Test

Table (13) demonstrates the impact of auditors’ academic qualifications and professional competence on the development of risk management systems in government entities. The statistical analysis reveals that the calculated T-value (T) is (7.861), exceeding the tabulated value of (1.645). Furthermore, the significance level (Sig) is (0.000), while the correlation coefficient (R) is (0.586) at the significance level (a=0.05). The coefficient of determination (R^2) is (0.344), while the Beta coefficient value (B) is (0.510), indicating a positive relationship between the independent and dependent variables. These findings lead to rejecting the null hypothesis and accepting the alternative hypothesis, affirming that "auditors’ academic qualifications and professional competence influence the development of risk management systems in government entities."

b. **Hypothesis (2):** There is no statistically significant relationship at the significance level (a = 0.05) between the review of internal audit management systems and regulations and the development of risk management systems in government entities.

The following table presents the results of the statistical analysis of this relationship using the simple linear regression test:

Statement	R (Correlation Coefficient)	R² (Coefficient of Determination)	T (Calculated)	B (Beta Coefficient)	Sig (Significance Level)
Reviewing internal audit management systems and regulations impacts the development of risk management systems in government entities.	.728	.530	11.525	.761	.001

Table 14: Hypothesis (2) Statistical Analysis Using Simple Linear Regression Test

The above table illustrates the impact of reviewing internal audit management systems and regulations on the development of risk management systems in government entities. The statistical analysis indicates that the calculated T-value is (11.525), exceeding the tabulated value of (1.645). Sig is (0.001), and R is (.728) at the significance level (a = 0.05). R² is (.530), while B is (.761), indicating a positive relationship between the independent and dependent variables. These results lead to rejecting the null hypothesis and accepting the alternative hypothesis, affirming that "reviewing internal audit management systems and regulations impacts the development of risk management systems in government entities."

c. **Hypothesis (3):** There is no statistically significant relationship at the significance level (a = 0.05) between internal audit procedures and risk reduction in government entities.

The following table presents the results of the statistical analysis of this relationship using the simple linear regression test:

Statement	R (Correlation Coefficient)	R² (Coefficient of Determination)	T (Calculated)	B (Beta Coefficient)	Sig (Significance Level)
Internal audit procedures have an effect on risk mitigation in government entities.	.988	.977	7.82	.920	0.000

Table 15: Hypothesis (3) Statistical Analysis Using Simple Linear Regression Test

Table (15) illustrates the effect of internal audit procedures on risk mitigation in government entities. The statistical analysis shows that the calculated T-value is (7.82), exceeding the tabulated value of (1.645). Sig is (0.000), while R is (.988) at the significance level (a = 0.05). R² is (.977), while B value is (.920), indicating a positive relationship between the independent and dependent variables. These results lead to rejecting the null hypothesis and accepting the alternative hypothesis, affirming that "Internal audit procedures have an effect on risk mitigation in government entities."

d. **Hypothesis (4):** There is no statistically significant relationship at the significance level (a = 0.05) between using AI and the development of risk management systems in government entities.

The following table presents the results of the statistical analysis of this relationship using a simple linear regression test:

Statement	R (Correlation Coefficient)	R² (Coefficient of Determination)	T (Calculated)	B (Beta Coefficient)	Sig (Significance Level)
Using AI has an impact on the development of risk management systems in government entities.	.667	.445	9.728	.686	.001

Table 16: Hypothesis (4) Statistical Analysis Using Simple Linear Regression Test

Table 16 illustrates the impact of using AI on developing risk management systems in government entities. The statistical analysis shows that the calculated T-value is (9.728), exceeding the tabulated value of (1.645). Sig is (0.001), and R is (.667) at the significance level (a = 0.05). R^2 is (.445), while B value is (.686), indicating a positive relationship between the independent and dependent variables. These results lead to rejecting the null hypothesis and accepting the alternative hypothesis, affirming that "Using AI has an impact on the development of risk management systems in government entities."

Findings of Hypothesis Testing

Testing the Primary Hypothesis:

The primary hypothesis states, "There is no statistically significant relationship at the significance level (a=0.05) between SAIs' role and the development of risk management systems in government entities." To test this hypothesis, the researcher employed multiple linear regression analysis to evaluate this effect. The results are presented in the following table:

Statement	R (Correlation Coefficient)	R^2 (Coefficient of Determination)	F-Value	B (Beta Coefficient)	df (Degrees of Freedom)	Sig (Significance Level)
SAIs play a significant role in the development of risk management systems in government entities.	.991	.982	4.47	.228	4 115 119	0.00

Table 17: Multiple Linear Regression Analysis

Table (17) illustrates SAIs' role in developing risk management systems in government entities. The analysis shows that the calculated F-value is (4.47), exceeding the tabulated value (1.645), Sig is (0.000), and R is (.991) at the significance level (a = 0.05). R^2 is (.982), while B value is (.228), indicating a positive relationship between the independent and dependent variables. These findings lead to the rejection of the null hypothesis and the acceptance of the alternative hypothesis, which confirms that SAIs play a significant role in developing risk management systems in government entities based on the perceptions of the study sample.

Chapter 4: Conclusions and Recommendations

Chapter 4: Conclusions and Recommendations

Examining the theoretical framework outlined in the previous chapters provided the essential foundation for constructing a systematic fieldwork approach to explore the role of SAIs in developing risk management systems within government entities. To achieve this, the researcher formulated a set of hypotheses to assess the development of risk management systems using both traditional and AI-based methods. The validity of these hypotheses was evaluated through a survey tool based on the metrics applied to each dimension of the study. The researcher then processed the survey responses into data tables, analyzed the findings, and extracted key conclusions. The main conclusions and recommendations are summarized as follows:

1. Conclusions

The research reached a set of theoretical and field conclusions, which can be summarized as follows:

1. Risks are an integral part of human activity, regardless of its nature, and cannot be entirely eliminated. However, they can be addressed and managed through a systematic and scientific approach that measures and assesses the risks an organization may face effectively. This approach relies on strategies that make the effects and consequences of risks more manageable, whether by transferring them to another party, mitigating their negative impacts, or accepting some or all of their consequences in pursuit of the organization's objectives.
2. Government entities encounter risks in both internal and external environments, particularly in the face of complex challenges and rapid developments in business, digital transformation, and other areas. Therefore, developing their risk management systems is essential to ensure service

continuity, enhance adaptability to ongoing changes in the risk environment, and effectively achieve their objectives.

3. The Institute of Internal Auditors (IIA) has identified government entities as responsible for risk management. The primary role of internal auditing is to provide objective assurance and support senior management by ensuring that business risks are managed appropriately and effectively. Furthermore, internal auditing confirms that risk management processes and internal control frameworks function efficiently and effectively.
4. The internal auditing profession faces two types of challenges. The first is the audit risk, which arises when an auditor issues an incorrect opinion regarding the organization’s data or reports. The second challenge stems from risks associated with the organization’s internal or external activities, which may threaten its continuity and ability to achieve its objectives.
5. There is an urgent need to establish a comprehensive program to ensure and enhance quality in the field of internal auditing and risk management. This program should include the following elements:
   a. Demonstrating the ability to undergo continuous development to keep pace with changes in the organizational environment and emerging risks.
   b. Conducting periodic internal assessments within the organization to identify strengths and weaknesses in internal auditing and risk management processes.
   c. Performing evaluations by qualified and independent external assessors at least once every five years to ensure objectivity and provide valuable insights and recommendations for performance improvement.
   d. Identifying potential risks and providing appropriate recommendations to address them effectively.

e. Enhancing audit effectiveness and strengthening confidence in risk reports.

6. Failure to integrate AI and ML technologies into risk management processes- unlike many leading auditing firms- limits the ability to benefit from their advantages. These technologies enable rapid, accurate, and efficient analysis of vast amounts of data, assist in predicting potential risks, facilitate swift responses to sudden changes in the business environment, and provide recommendations with transparency and objectivity. Moreover, AI and ML improve auditing and review processes while minimizing human errors compared to traditional auditing methods.

7. Several obstacles hinder the adoption of AI and ML to improve risk management systems. The most significant obstacles include:

   a. The high costs of adopting and developing AI and ML technologies.

   b. The limited availability of specialized and qualified personnel to handle these technologies.

   c. The difficulty of keeping pace with rapid technological advancements and the continuous need to update the knowledge and skills required for AI and ML technologies.

   d. The challenges of integrating legacy systems with modern technologies, exposing organizations to various difficulties and risks.

   e. The deficiencies in legal and regulatory frameworks and standards related to data protection, privacy, and security threats. Additionally, there are raising concerns about cybersecurity and associated risks.

   f. The internal resistance to change and the adoption of new technologies due to fear of the unknown, job insecurity, or the absence of effective change management strategies to help employees' transition and adapt to new technologies.

g. The size and complexity of data preparation to be usable in AI models require significant time and effort.

h. The lengthy data collection and preparation process before it can be effectively used in AI models.

8. The Supreme Audit Institutions (SAIs) play a vital role in monitoring and evaluating the performance of internal auditing. They contribute to the development of risk management systems in government entities and enhance their preparedness to address emerging risks. However, the audit profession faces several challenges related to the following aspects:

a. SAIs focus on candidates with academic qualifications (bachelor's degrees) without encouraging the pursuit of professional certifications or advanced academic degrees. This limitation weakens in-depth expertise and advanced skills in auditing and the development of risk management systems.

b. Lack of specialized training programs, academic and practical qualifications, and comprehensive knowledge of IT systems to keep pace with technological advancements and effectively engage with them.

c. Limited cultural awareness and reluctance to adopt modern systems among individuals accustomed to traditional auditing methods.

d. The need to issue a comprehensive policy and procedure guide for oversight using AI technologies to support the achievement of intended objectives, along with a code of professional conduct to mitigate professional and ethical risks when conducting automated monitoring.

9. The first alternative hypothesis of the study was accepted, indicating a statistically significant effect of auditors’ academic qualifications and professional competence on the development of risk management systems in government entities.
10. The second alternative hypothesis of the study was accepted, indicating a statistically significant effect of reviewing internal audit management systems and regulations on the development of risk management systems in government entities.
11. The third alternative hypothesis of the study was accepted, indicating a statistically significant effect of internal audit procedures on risk mitigation in government entities.
12. The fourth alternative hypothesis of the study was accepted, indicating a statistically significant effect of using AI on the development of risk management systems in government entities.

2. Recommendations

Building upon the theoretical and practical findings of this study, several recommendations are proposed to enhance risk management within government entities by leveraging both traditional advanced systems and AI technologies. These recommendations aim to address existing limitations and improve the overall effectiveness of risk management. Based on the research conclusions, the key recommendations are as follows:

1. Emphasize the importance of developing and enhancing risk management systems in government entities, as they serve as a fundamental pillar in addressing evolving risks and ensuring institutional resilience.

2. Ensure that decision-makers are aware that risk management is primarily the responsibility of executive management, and that modern internal auditing provides assurance to senior management regarding the efficiency and effectiveness of risk management practices.
3. Establish a comprehensive framework to enhance the quality of internal auditing and risk management. This framework should focus on audit risks and risks arising from the entity's internal and external environments. Additionally, it should incorporate a self-assessment approach for controls and risks, actively involving employees across the entity to foster a proactive risk culture. This approach offers numerous advantages in achieving objectives and selecting appropriate control strategies.
4. Ensure the periodic evaluation of internal auditing and risk management by auditors, external consultants, and SAIs, taking into account their expertise and independence from the organization.
5. Utilize modern technologies to leverage their positive outcomes. AI and ML have contributed to creating an advanced environment for risk management systems by enhancing the accuracy of risk analysis and prediction. Additionally, the use of AI and ML improves the efficiency of audit processes by enabling the rapid and precise processing of large volumes of data. These technologies also aid in the early detection of potential risks, reduce human errors, and facilitate swift responses to emerging challenges in the work environment.
6. Ensure the readiness and continuous updating of electronic system infrastructure while optimizing IT and communication tools to facilitate work processes and simplify procedures. Additionally, internal control systems should be developed to align with digital transformation and IT advancements. Protection and security programs must also be implemented to counter evolving viruses and keep pace with modern technologies.

7. Issue laws, regulations, and international standards to govern risk management tasks, ensuring their legal enforceability upon implementation, aligning them with automated systems, and ensuring periodic updates.
8. Develop a comprehensive guide to regulate policies on AI usage to ensure its successful implementation. This guide should also include a professional and ethical code of conduct to mitigate ethical risks and personal biases, thereby achieving the oversight objectives in risk management.
9. Establish an electronic resource hub within SAIs to meet the auditors’ needs in carrying out their assigned tasks.
10. Conduct regular training programs, conferences, and continuous academic and practical qualifications on modern trends in the use of AI and ML for developing risk management systems.
11. Ensure the integration of AI within SAIs to develop a more advanced and proactive risk management system, strengthening organizational resilience and excellence. This integration is expected to drive further advancements in risk management applications, making them more comprehensive and effective in fostering long-term sustainability and success.

References

- **Arabic References:**

1. Riyadh Economic Forum. (2006). *Developing the Relationship between the Government Sector, the Public Sector, and the Private Sector*.
2. Abu Dhabi Accountability Authority. (2010). *Audit Management Manual*. Retrieved from https://shorturl.at/gzDFJ.
3. Kazem, S. (2022). *The Scientific and Professional Competence of the Internal Auditor and Their Impact on Reducing Creative Accounting Practices to Produce Reliable Financial Reports* (Master’s thesis, College of Administration and Economics, University of Karbala). Retrieved from https://shorturl.at/TQyY1.
4. Mahdi, N., & Al-Jabouri, N. (2016). *Enhancing the Performance of Internal Audit Units within the Government Sector in Light of Risk Management Approach*. Journal of Administration and Economics. Volume 39. Issue 190.
5. Tubasi, A. *Risk Management in Third Sector Organizations.* Retrieved from https://shorturl.at/bfhzB.
6. Qandous, A. (2018). *Hedging and Risk Management: A Financial Approach*. E-Kutub Ltd.
7. Saudi Center for Financial and Performance Audit. *Risk-based Training Kit*. SAI Saudi Arabia. Retrieved from https://shorturl.at/glxRX.
8. Hammad, T. A. (2003). *Risk management*. Al-Dar Al-Jami’iyah Press.
9. Al-Abbas, M. (2021). *Risk Management: How has the concept evolved?* Al-Eqtisadiah Newspaper. Retrieved from https://shorturl.at/prtPU
10. Kamal, H. *What Do You Know About Risk Management?* Edarati Online Magazine. Retrieved from www.edaratimagazine.com

11. Abdi, A. (2023). *The Contribution of Internal Audit to the Activation of Risk Management: A Field Study*. Ibn Khaldoun University – Tiaret.
12. Ahmad, A. (2024, May). *Experts Prepare for More in 2018: "Risk Management Challenges under Control.*" IPA Magazine, Issue 210. Retrieved from https://shorturl.at/Nu50E.
13. Global Center for Strategy and Innovation. Retrieved from https://worldnetcs.com/services
14. Ezzat, A. (2021). *A Program on the Role of the Internal Auditor in Governance and Risk Management.* Saudi Society. Retrieved from https://shorturl.at/UVj9z
15. Rouqti, B., & Kerkar, E. (2022). *Risk Management in the Algerian Healthcare System: A Field Study at Al-Hakim Okbi Hospital.* Faculty of Humanities and Social Sciences.
16. *Risk Concept and Risk Management: A Comprehensive Guide to Steps and Specialization.* Retrieved from https://shorturl.at/lnBL6
17. Al-Karasneh, I. *Basic and Contemporary Frameworks in Bank Audit and Risk Management.* Arab Monetary Fund, Economic Policy Institute.
18. Al-Khatib, S. (2005). *Measuring and Managing Risks in Banks.* Al-Maaref Establishment.
19. General Department of Governance, Risk, and Compliance. (2021). *Risk Management Guide.* Retrieved from https://shorturl.at/XtOWX
20. Ministry of Planning and International Cooperation. *Risk Management Plan 2017-2019.* King Abdullah Award for Excellence in Government Performance and Transparency.
21. Jumaa, A. H. & Barghouti, S. *The Role of the Internal Auditor in Risk Management in Jordanian Commercial Banks: A Field Study*. The 7th Annual International Scientific Conference on Risk Management and Knowledge Economy, 16-18 April. Al-Zaytouna University.
22. Boutros. S. (2011). *Modern Strategies for Crisis Management*. Dar Al-Raya for Publishing and Distribution.

23. *Characteristics, Role and Objectives of Risk Management*. Retrieved from https://shorturl.at/mtyJZ

24. *Strategic Management Journal*. Retrieved from https://onlinelibrary.wiley.com/journal/10970266

25. Hindi, I. (2013). *Modern Perspectives on Risk Management: Financial Engineering Using Securitization and Derivatives*. Part II. Al-Maktab Al-Arabi Al-Hadith Publishing.

26. General Department of Governance, Risk, and Compliance. (2021). *Risk Management Guide.*

27. Ministry of Planning and International Cooperation. *Risk Management Plan 2017-2019.* King Abdullah Award for Excellence in Government Performance and Transparency.

28. Ezzat, A. (2021). *A Program on the Role of the Internal Auditor in Governance and Risk Management.* Saudi Society.

29. SAI Iraq. *Risk Audit Guide*.

30. Kheira, R. (2012). *The Role of Internal Audit in Enterprise Risk Management.* Hassiba Benbouali University. Faculty of Economics and Management Sciences.

31. Moussa, A., & Futuhah, M. S. *Sectoral Specialization of Auditors and their Role in Mitigating Audit Risks.* University Bulletin. Volume 1. Issue 18.

32. Saudi Center for Financial Audit and Performance Control. *The Era of Risk-based Auditing.* Retrieved from https://shorturl.at/sxEGO

33. Al-Huwaidi, E., & Al-Nassar, A. (2019*). Training Program: Risk-based Audit (Auditor's Impact Project).*

34. Moussa, A., & Futuhah, M. S. *Sectoral Specialization of Auditors and their Role in Mitigating Audit Risks.* University Bulletin. Volume 1. Issue 18.

35. Al-Tamimi, H. (2004). *Introduction to Auditing: A Practical and Theoretical Approach*. Dar Wael for Publishing and Distribution.

36. International Standards for the Professional Practices of Internal Auditing (Standards). Retrieved from https://shorturl.at/wEHSV.

37. Al-Lanfawi, Kh., Al-Otaibi, R., & Al-Jabri, F. (2021). *The Impact of the General Audit Guide and Other Specialized Guides of the State Audit Bureau on Improving Audit Performance.* The 22nd Research Competition of the State Audit Bureau of Kuwait.

38. General Department of Governance, Risk, and Compliance. (2021). *Risk Management Guide.*

39. Al-Humaimidi, N., & Al-Rashed, M. (2021). *Risk-based Audit.* The 21st Research Competition of the State Audit Bureau of Kuwait.

40. Al-Huwaidi, E., & Al-Nassar, A. (2019). *Training Program: Risk-based Audit (Auditor's Impact Training Project).*

41. Abdullah, H., & Al-Faraj, A. (2019). *Training Program: Methods and Procedures for Assessing Internal Audit Bodies Using a Risk-Based Approach.*

42. State Audit Bureau. (2022). *Guidance for the Planning Phase of Risk-based Audit.*

43. Dr. Al-Ghubari, A. (2011). *Training Program: Financial Risk Management and Assessment.*

44. SAB's Auditing Standards and Professional Guidelines Committee. (2022). *Proposed Model for Establishing and Developing a Risk Management Department.* The State Audit Bureau of Kuwait.

45. *Enterprise and Government Risk Management: Key Components and Objectives.* Retrieved from https://shorturl.at/uvDEX.

46. Directorate of Information Technology of SAI Jordan. *Strategic Plan 2021/2023: Digital Transformation Project.*

47. SAI UAE. *Artificial Intelligence: A Remarkable Advancement in Public Sector Audit* (Working Paper).

- **English References:**

1. Hull, J. C. (2015). *Risk Management and Financial Institutions*. Wiley.
2. *The 2nd Meeting of the INTOSAI Working Group on Big Data*. (2018, April 19-20). Washington, DC, USA.
3. EUROSAI IT Working Group. (2020, November 12). *SAIs and the Digital Turn e-Seminar: Data Analysis and IT Auditing of SAI Norway*.
4. Meijer-van Leijsen, E., Verhulst, J., Oosterwijk, P., & Pirkovski, M. *Developing an Audit Framework for Algorithms.* INTOSAI Journal. Spring 2021 Edition.
5. Arntz, M., Gregory, T., & Zierahn, U. *The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis.* OECD Social, Employment and Migration Working Papers.
6. Frey, C. B., & Osborne, M. A. (2017). *The Future of Employment: How Susceptible are Jobs to Computerization?* Technological Forecasting and Social Change Journal. Volume 114.

- **Websites:**

1- https://shorturl.at/OOZUj
2- https://shorturl.at/eozK0
3- https://shorturl.at/qBUY3
4- https://shorturl.at/uJ036
5- https://shorturl.at/vHRX9
6- https://jadwa.om/blog/SWOT_Analysis
7- https://shorturl.at/qrCHT
8- https://shorturl.at/gluEK
9- https://shorturl.at/mnqPZ
10- https://mail.almerja.com/reading.php?idm=196433
11- https://shorturl.at/p9pjB
12- https://shorturl.at/jvG24
13- https://shorturl.at/cpxBN
14- https://shorturl.at/vJh9F
15- https://shorturl.at/bfzAZ
16- https://socpa.org.sa/audit
17- https://shorturl.at/fABUY

18- https://shorturl.at/mvyBG
19- https://shorturl.at/loQV7
20- https://shorturl.at/ctxyX
21- https://www.theiia.org/Copyright
22- https://shorturl.at/D070p
23- https://shorturl.at/gnvO4
24- https://shorturl.at/ioQV2
25- https://shorturl.at/gnoyo
26- https://shorturl.at/EKNVM
27- https://shorturl.at/Od4Y4
28- https://shorturl.at/muoHp
29- https://shorturl.at/N3nvw
30- https://shorturl.at/1awh6
31- https://shorturl.at/7sAMa
32- https://shorturl.at/Psc03
33- https://www.argaam.com/ar/article/articledetail/id/1615530
34- https://shorturl.at/Psc03
35- https://shorturl.at/9rkwv
36- https://shorturl.at/F5AQF
37- https://shorturl.at/XCk0u