A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT

Ahmet EFE[1]

Abstract

Risk management frameworks play an essential role in identifying, assessing, and mitigating risks to ensure the effective governance and operation of organizations. It is also one of the key elements of assurance and consultancy services of internal auditing in risk-based audit plans and programs. This study aims to provide an in-depth comparison of four widely used risk management frameworks: the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO-ERM), the National Institute of Standards and Technology Risk Management Framework (NIST RMF), the International Organization for Standardization 31000 (ISO 31.000), and Control Objectives for Information and Related Technologies (COBIT). The analysis is conducted based on their underlying principles, structure, risk assessment methodologies, and applicability in various industries. We evaluate the strengths and weaknesses of each framework, including their adaptability and relevance in addressing emerging risks, such as cybersecurity and data privacy. It is found that implementing ISO 31000 and COBIT frameworks requires addressing challenges and limitations, including commitment from top management, knowledge and training, customization, and monitoring. To succeed, organizations should demonstrate commitment, provide training, customize the frameworks, and establish robust monitoring systems. The findings from this study serve as a guide for organizations seeking to adopt or transition between risk management frameworks, ultimately enabling them to select the most suitable approach tailored to their specific needs and risk landscape.

Keywords: *Risk management frameworks, COSO-ERM, NIST RMF, ISO 31.000, COBIT*

Temel Risk Yönetimi Çerçevelerinin Karşılaştırması: COSO-ERM, NIST RMF, ISO 31.000, COBIT

Özet

Risk yönetimi çerçeveleri, kuruluşların etkin yönetişimini ve işleyişini sağlamak için risklerin tanımlanmasında, değerlendirilmesinde ve azaltılmasında önemli bir rol oynar. Aynı zamanda risk esaslı denetim plan ve programlarında iç denetimin güvence ve danışmanlık hizmetlerinin de temel unsurlarından biridir. Bu çalışma, yaygın olarak kullanılan dört risk yönetimi çerçevesinin derinlemesine bir karşılaştırmasını sağlamayı amaçlamaktadır: Treadway Komisyonu Kurumsal Risk Yönetiminin Sponsor Kuruluşları Komitesi (COSO-ERM), Ulusal Standartlar ve Teknoloji Enstitüsü Risk Yönetimi Çerçevesi (NIST RMF), Uluslararası Standardizasyon Örgütü 31000 (ISO 31.000) ve Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT). Analiz, temel ilkelerine, yapısına, risk değerlendirme metodolojilerine ve çeşitli endüstrilerdeki uygulanabilirliğine göre yapılmaktadır. Siber güvenlik ve veri gizliliği gibi ortaya çıkan riskleri ele almadaki uygunlukları ve uygunlukları dahil olmak üzere her bir çerçevenin güçlü ve zayıf yönleri değerlendirilmektedir. ISO 31000 ve COBIT çerçevelerinin uygulanmasının, üst yönetimin taahhüdü, bilgi ve eğitim, özelleştirme ve izleme dahil olmak üzere zorlukların ve sınırlamaların ele alınmasını gerektirdiği bulunmuştur. Başarılı olmak için kuruluşlar bağlılık göstermeli, eğitim sağlamalı, çerçeveleri özelleştirmeli ve sağlam izleme sistemleri kurmalıdır. Bu çalışmadan elde edilen bulgular, risk yönetimi çerçevelerini benimsemek veya bunlar arasında geçiş yapmak

Review Article
Submitted: 3.5.2023 Accepted: 28.7.2023
[1]Dr., CISA; CRISC; PMP, International Federation of Red Cross and Red Crescent Societies, ESSN Audit Department,, icsiacag@gmail.com, http://orcid.org/0000-0002-2691-7517
Citation: Efe, A. (2023). A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Denetim ve Güvence Hizmetleri Dergisi 3*(2), 185-205.

isteyen kuruluşlar için kapsamlı bir rehber işlevi görerek nihai olarak kendi özel ihtiyaçlarına ve risk ortamına göre en uygun yaklaşımı seçmelerine olanak tanımaktadır.

Anahtar Kelimeler: *Risk yönetimi çerçeveleri, COSO-ERM, NIST RMF, ISO 31.000, COBIT*

1. INTRODUCTION

In an increasingly complex and interconnected world, organizations face a multitude of risks that can significantly impact their performance and long-term sustainability. Effective risk management has become a vital component of organizational success, as it enables the identification, assessment, and mitigation of potential threats, while also capitalizing on opportunities that arise from uncertainty. To address this need, various risk management frameworks have been developed, each with unique approaches and methodologies aimed at assisting organizations in managing risks effectively.

Four of the most widely used and recognized risk management frameworks are COSO-ERM, the NIST Risk Management Framework (NIST RMF), the ISO 31000 (ISO 31.000), and COBIT. These frameworks provide guidelines, principles, and processes that organizations in developing a robust risk management strategy. Despite their shared goal of risk management, these frameworks differ in their focus, structure, and applicability across various industries. As organizations seek to adopt or transition between risk management frameworks, understanding the nuances and comparative strengths of each framework becomes crucial. This study aims to provide an in-depth analysis of the COSO-ERM, NIST RMF, ISO 31.000, and COBIT frameworks, highlighting their underlying principles, risk assessment methodologies, and industry applicability. The findings of this research may serve as a guide for organizations to select the most suitable risk management framework tailored to their specific needs and risk landscape.

1.1. Research Problem

The selection and implementation of an appropriate risk management framework are crucial for organizations to efficiently address potential risks and ensure effective governance. However, choosing the right framework can be challenging due to the differences in focus, structure, and applicability of the various frameworks available. This study aims to address the problem of understanding and comparing the strengths and weaknesses of four widely used risk management frameworks - COSO-ERM, NIST RMF, ISO 31.000, and COBIT - to facilitate informed decision-making for organizations seeking to adopt or transition between these frameworks.

1.2. Assumptions

- The effectiveness of a risk management framework is influenced by its ability to address the specific needs and risk landscape of an organization.
- The four risk management frameworks analyzed in this study are widely used and well-established, making them suitable candidates for comparison.
- Organizations seeking to adopt or transition between risk management frameworks are primarily interested in understanding the comparative strengths and weaknesses of each framework, including their applicability across various industries.

1.3. Hypothesis

Conducting a thorough comparison of the COSO-ERM, NIST RMF, ISO 31.000, and COBIT risk management frameworks, focusing on their underlying principles, risk assessment methodologies, and industry applicability, will empower organizations to make well-informed decisions when choosing the most appropriate framework that aligns with their specific requirements and risk landscape. This comparative analysis will uncover the distinctive strengths and weaknesses of each framework, along with their capacity to adapt and remain relevant in tackling emerging risks like cybersecurity and data privacy.

2. OVERVIEW OF RISK MANAGEMENT FRAMEWORKS

In today's dynamic and complex business environment, organizations face numerous risks that can impact their operations, reputation, and overall success. To effectively manage these risks, various frameworks and standards have been developed to provide guidance and structure. This section introduces four prominent frameworks that are widely used in the field of risk management. They include COSO-ERM, NIST RMF, ISO 31.000, and COBIT. Each framework offers unique perspectives and approaches to managing risks, providing organizations with a comprehensive toolkit to enhance their risk management practices. Let's delve into each of these frameworks to understand their key principles and contributions to the field of risk management.

2.1. COSO-ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management)

Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2004, with an update in 2017. COSO, a cooperative effort of five private sector entities such as the American Accounting Association (AAA) and the American Institute of Certified Public Accountants (AICPA), developed the framework to provide a comprehensive approach to risk management, aiming to improve organizational performance (COSO, 2017; COSO, n.d.).

The COSO-ERM is constructed around five interconnected components, each consisting of multiple principles. These components include governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting. The framework underscores the significance of risk management in decision-making and advocates for aligning risk appetite with strategic goals and performance metrics (COSO, 2017).

Many organizations across diverse sectors adopt the COSO-ERM, especially those looking to enhance their internal control systems and risk management procedures. It often works in tandem with the COSO Internal Control-Integrated Framework, which is designed to improve the efficacy of internal controls within organizations (COSO, 2013). The broad applicability and comprehensive nature of the COSO-ERM make it a preferred choice for organizations intending to apply a holistic risk management strategy.

2.2. NIST RMF (National Institute of Standards and Technology - Risk Management Framework)

NIST RMF is a comprehensive, standardized approach to managing information security risks within federal information systems (NIST, 2018). The framework was initially developed to fulfill the requirements outlined in the Federal Information Security Management Act (FISMA) of 2002 and has since been widely adopted by various organizations, both public and private, seeking to implement an effective risk management strategy.

The NIST RMF is composed of a six-step process that guides organizations through the identification, assessment, and management of risks associated with their information systems (NIST, 2018). The six steps include:

- Categorize Information System: Define the system's boundaries and determine its security categorization based on the potential impact of a security breach on the confidentiality, integrity, and availability of the information (NIST, 2009).
- Select Security Controls: Choose appropriate security controls from the NIST Special Publication 800-53, a catalog of security controls that addresses various risk scenarios and system requirements (NIST, 2013).
- Implement Security Controls: Apply the selected security controls to the information system, ensuring they are integrated effectively and function as intended.
- Assess Security Controls: Evaluate the effectiveness of the implemented security controls to identify potential weaknesses and areas for improvement.
- Authorize Information System: Based on the assessment results, senior management decides whether the system's risk is acceptable, and if so, authorizes its operation.
- Monitor Security Controls: Continuously monitor the information system to identify changes in risk and the effectiveness of security controls and make necessary adjustments to maintain an acceptable level of risk (NIST, 2018).

The NIST RMF emphasizes the importance of continuous risk management and encourages organizations to integrate risk management processes throughout the system development life cycle (NIST, 2018). By providing a structured, repeatable, and measurable approach to risk management, the NIST RMF enables organizations to effectively safeguard their information systems and maintain compliance with relevant regulations.

2.3. ISO 31.000 (ISO - Risk Management)

The ISO (ISO) is a globally recognized body that develops and publishes international standards across various industries. One such standard is ISO 31000, which focuses on risk management principles and guidelines (ISO, 2018). The primary aim of ISO 31000 is to provide a universally applicable framework that can be tailored to the specific needs and risk landscape of any organization, regardless of its size, industry, or nature of operations.

ISO 31000 is based on a set of core principles that emphasize the importance of integrating risk management into all aspects of an organization's activities and decision-making processes (ISO, 2018). These principles include the integration of risk management into organizational processes, the inclusion of a comprehensive and systematic approach to risk identification and assessment, and the continuous improvement and adaptation of risk management practices.

The ISO 31000 framework is structured around a risk management process that comprises three main components: risk assessment, risk treatment, and risk monitoring and review (ISO, 2018). Risk assessment involves identifying, analyzing, and evaluating risks to determine their potential impact and likelihood. Risk treatment involves selecting and implementing appropriate risk mitigation strategies to reduce the likelihood and impact of identified risks. Finally, risk monitoring and review involve continuous tracking and evaluation of risks, as well as the effectiveness of risk treatment measures, to ensure that the organization's risk management strategy remains relevant and up to date.

A key strength of ISO 31000 is its flexibility and adaptability, making it suitable for organizations of all types and sizes (ISO, 2018). Additionally, the framework emphasizes the importance of a proactive and iterative approach to risk management, which allows organizations to stay ahead of emerging risks and adapt their strategies accordingly.

In conclusion, ISO 31000 offers a comprehensive and flexible risk management framework that can be tailored to the specific needs of any organization. Its core principles and structured approach to risk assessment, treatment, and monitoring make it an attractive option for organizations seeking a robust risk management strategy.

2.4. COBIT (Control Objectives for Information and Related Technologies)

COBIT is a comprehensive framework designed to assist organizations in achieving their strategic objectives through effective governance and management of enterprise IT (Information Technology). Developed by the Information Systems Audit and Control Association (ISACA), COBIT has evolved through multiple iterations, with COBIT 2019 being the latest version (ISACA, 2019). The framework emphasizes the alignment of IT with business goals and offers a holistic approach to IT governance, addressing various aspects such as risk management, compliance, and performance measurement (Guldentops, 2004).

In terms of risk management and risk governance, COBIT provides a structured approach that enables organizations to identify, assess, and mitigate IT-related risks systematically. It offers a set of generic control objectives and a comprehensive list of IT processes, which can be tailored to fit an organization's specific needs and risk landscape (ISACA, 2019). Additionally, COBIT's risk management process is guided by the APO12 (Manage Risk) management objective, which focuses on the establishment and maintenance of a risk management framework, as well as the continuous monitoring and reporting of risks (ISACA, 2019).

COBIT's approach to risk governance emphasizes the importance of incorporating risk management into the overall IT governance structure. It advocates for the involvement of various stakeholders, such as senior management, board members, and IT professionals, in the risk management process to ensure effective decision-making and accountability (Weill and Ross, 2004). The framework also encourages organizations to adopt a risk-

aware culture, fostering open communication and collaboration among stakeholders to address potential risks proactively (ISACA, 2019).

In conclusion, COBIT offers a comprehensive and adaptable approach to risk management and risk governance, emphasizing the alignment of IT with business objectives and the importance of stakeholder involvement in the risk management process. By providing a structured framework and guidance for IT risk management, COBIT enables organizations to better identify, assess, and mitigate IT-related risks, ultimately contributing to their overall strategic goals.

3. FRAMEWORK COMPONENTS AND PROCESSES

In the field of risk management and governance, several frameworks have emerged to help organizations effectively identify, assess, and mitigate risks. These frameworks provide structured approaches and guidelines to enhance the management of risks, ensure compliance with regulations, and promote the achievement of organizational objectives. In this section, we will explore three prominent frameworks: COSO-ERM, NIST RMF, and COBIT. Each framework has its unique focus and methodology, making them valuable tools for organizations operating in various industries. Let's delve into each framework and understand their key features and benefits.

3.1. COSO-ERM

The framework comprises five interconnected components and various underlying principles that guide organizations in developing a robust risk management strategy.

The five components of the COSO-ERM framework are as follows (COSO, 2017):

1. Governance and Culture: This component emphasizes the importance of establishing a strong governance structure and risk-aware culture. It includes principles related to board oversight, organizational ethics and values, risk appetite, and the risk management roles and responsibilities of various stakeholders within the organization.

2. Strategy and Objective-Setting: This component focuses on integrating risk management into the organization's strategic planning and objective-setting processes. It involves principles such as evaluating risk in the formulation of strategy, setting business objectives considering the risk appetite, and developing risk tolerance thresholds for various objectives.

3. Performance: The performance component involves the identification, assessment, prioritization, and response to risks. This includes principles such as risk identification, risk assessment, risk prioritization, risk response, and reporting on risk, culture, and performance.

4. Review and Revision: This component aims to ensure continuous improvement in risk management through regular review and revision of the risk management processes. The principles include reviewing risk and performance, pursuing improvements in risk management, and modifying risk management practices based on the lessons learned.

5. Information, Communication, and Reporting: The final component focuses on the effective flow of risk-related information throughout the organization. This includes principles such as leveraging information and technology to support risk management, communicating risk information across the organization, and reporting on risk, culture, and performance to relevant stakeholders.

These components and their underlying principles work together to provide a holistic approach to enterprise risk management, enabling organizations to identify, assess, and mitigate risks more effectively (COSO, 2017).

3.2. NIST RMF

The framework consists of six distinct steps and emphasizes the integration of risk management throughout an organization's information system life cycle.

1. Prepare: This step involves establishing a risk management context, which includes identifying the organization's mission, objectives, and risk tolerance, as well as the roles and responsibilities of stakeholders

(NIST, 2018). Organizations should also define the scope of the risk management process and develop appropriate risk management strategies.

2. Categorize: The categorization step involves classifying the information system and its components based on their impact on organizational operations, assets, and individuals (NIST, 2018). This process is guided by the Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems" (NIST, 2004).

3. Select: In this step, organizations select appropriate security and privacy controls based on the categorization of their information system (NIST, 2018). The selection process is guided by NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations" (NIST, 2020).

4. Implement: Organizations then implement the selected security and privacy controls and document their implementation within the information system (NIST, 2018). This step may involve configuring, integrating, or customizing controls to address the specific needs of the organization.

5. Assess: The assessment step involves evaluating the effectiveness of the implemented security and privacy controls (NIST, 2018). Organizations can use NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations" (NIST, 2020) as a guideline for this process. The assessment results are documented in a security assessment report.

6. Authorize: In this final step, a senior official within the organization reviews the assessment results and the risk management process, making a risk-based decision to authorize the operation of the information system (NIST, 2018). The authorization decision is documented in an authorization package, which includes an authorization statement and the plan of action and milestones (POA&M) to address any identified weaknesses.

Throughout the NIST RMF process, organizations are encouraged to continuously monitor and update their security and privacy controls, as well as maintain situational awareness of their risk environment (NIST, 2018).

3.3. ISO 31.000

The ISO 31000:2018 Risk Management - Guidelines (ISO, 2018) is a widely recognized international standard that provides a comprehensive set of principles, framework components, and processes for managing risks in organizations across various industries. The ISO 31000:2018 is designed to be adaptable, allowing organizations to integrate it into their existing operations and governance structures, irrespective of their size, nature, or sector (ISO, 2018).

Framework Components:

1. Principles: The ISO 31000:2018 outlines eight risk management principles that serve as a foundation for effective risk management practices. These principles include integration, structure, comprehensive approach, customization, inclusion, human and cultural factors, continuous improvement, and timely decision-making (ISO, 2018).

2. Risk Management Framework: The Risk Framework, as per the ISO standard, is a comprehensive set of elements that establish the basis and organizational procedures for constructing, executing, observing, revising, and perpetually enhancing risk management across the organization (ISO, 2018). These elements encompass understanding the organization and its context, instituting a risk management policy, integrating risk management into the organization's operations, confirming that risk management is a fundamental part of decision-making, and constant improvement of the risk management framework.

Processes:

The ISO 31000:2018 risk management process consists of the following stages:

1. Communication and consultation: Engaging with stakeholders throughout the risk management process to ensure that their views, concerns, and expectations are considered and addressed (ISO, 2018).

2. Scope, context, and criteria: Defining the scope, context, and risk criteria to identify and assess risks appropriately (ISO, 2018).

3. Risk identification: Identifying risks by recognizing potential events, situations, or circumstances that could impact an organization's ability to achieve its objectives (ISO, 2018).

4. Risk analysis: Assessing the risk's likelihood and consequences, as well as other attributes, to determine the level of risk (ISO, 2018).

5. Risk evaluation: Comparing the risk analysis results with the established risk criteria to determine the significance of the risks and inform risk treatment decisions (ISO, 2018).

6. Risk treatment: Developing and implementing strategies for modifying risks, including avoiding, transferring, reducing, or retaining the risk (ISO, 2018).

7. Monitoring and review: Continuously monitoring and reviewing the risk management process and its outcomes to ensure that it remains effective and relevant, and to identify areas for improvement (ISO, 2018).

8. Recording and reporting: Documenting and communicating risk management activities, outcomes, and decisions to support accountability and informed decision-making (ISO, 2018).

3.4. COBIT

Its primary focus is on aligning I&T with business goals, optimizing I&T resources, and managing I&T risks. In terms of risk management and risk governance, COBIT provides a structured approach that encompasses several components and processes.

Components:

1. Framework: COBIT 2019, the latest version, offers a comprehensive and flexible framework for I&T governance and management (ISACA, 2019). It integrates globally recognized best practices, standards, and regulatory requirements, making it suitable for organizations of various sizes and industries.

2. Principles: COBIT follows six principles for enterprise I&T governance and management, including meeting stakeholder needs, end-to-end coverage, a single integrated framework, a holistic approach, separating governance from management, and addressing emerging risks (ISACA, 2019)

3. Governance and Management Objectives: It consists of 40 objectives categorized into five domains: Governance, Align, Plan and Organize, Build, Acquire and Implement, Deliver, Service and Support, and Monitor, Evaluate and Assess, with each objective linked to specific processes for goal achievement (ISACA, 2019).

Processes:

In the context of risk management and risk governance, COBIT includes several processes that help organizations identify, assess, and manage risks.

1. Evaluate, Direct, and Monitor (EDM): This governance domain focuses on setting the direction for the organization and monitoring the achievement of desired outcomes (ISACA, 2019). Key processes within this domain related to risk management include: a. EDM03: Ensure Risk Optimization - This process involves establishing a risk management framework, setting risk appetite, and ensuring risk responses are aligned with the organization's objectives (ISACA, 2019).

2. Align, Plan and Organize (APO): This management domain focuses on aligning I&T with business objectives and planning the required resources (ISACA, 2019). Risk management-related processes within this domain include: a. APO12: Manage Risk - This process involves the identification, assessment, and management of I&T-related risks, including the development and implementation of risk response plans (ISACA, 2019).

3. Monitor, Evaluate and Assess (MEA): This management domain focuses on the continuous monitoring, evaluation, and assessment of I&T performance and the achievement of objectives (ISACA, 2019). Risk

management-related processes within this domain include: a. MEA01: Monitor, Evaluate, and Assess Performance and Conformance - This process involves monitoring the effectiveness of risk management practices and ensuring conformance with internal and external requirements (ISACA, 2019).

In conclusion, COBIT offers a comprehensive and flexible framework for managing I&T risks within organizations. It provides a structured approach, guided by principles and objectives, that encompasses various processes for the identification, assessment, and mitigation of risks.

4. COMPARISON OF FRAMEWORKS

In the comparison of risk frameworks, several important subsections can be explored. Firstly, the methodology section delves into the specific approaches and techniques used to assess and manage risks. The scope and coverage subsection focuses on the extent and breadth of risks considered within each framework. Process steps and stages examine the sequential actions and stages involved in the risk management process. Terminology and concepts explore the specific language and definitions utilized in different frameworks. Key principles and practices highlight the fundamental guidelines and approaches that underpin each framework. Finally, the integration with other management frameworks subsection examines how risk frameworks align and interact with other organizational management frameworks. By exploring these subsections, a comprehensive understanding of the similarities and differences among risk frameworks can be achieved.

4.1. Methodology

COSO-ERM: Holistic enterprise-wide risk management approach.

NIST RMF: Quantitative IT and cybersecurity risk management.

ISO 31.000: Flexible and principles-based risk management for various industries.

COBIT (Risk IT): IT-related risk management within IT governance and management.

Therefore, each of these risk management frameworks offers a unique methodology to address different aspects of risk management. COSO-ERM provides a holistic approach suitable for enterprise-wide risk management, while NIST RMF focuses on IT systems and cybersecurity risk management. ISO 31.000 offers a flexible, principles-based approach applicable across various industries, and COBIT (Risk IT) specifically addresses IT-related risk management within the context of IT governance and management.

4.2. Scope and coverage

COSO-ERM, NIST RMF, ISO 31000, and COBIT are four widely recognized risk management frameworks. This comparison will focus on their scope and coverage in the context of organizational risk management.

COSO-ERM: The COSO-ERM framework, created by the Committee of Sponsoring Organizations of the Treadway Commission (2017), offers a holistic approach to enterprise risk management, integrating risk management into strategic planning and decision-making. Its five components are governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting. It covers strategic, operational, financial, and compliance risks, making it versatile across industries.

NIST RMF: The NIST RMF, detailed in NIST Special Publication 800-37 (Ross et al., 2018), is a framework for managing information security risks in federal information systems. It follows a six-step process encompassing categorizing information systems, selecting and implementing security controls, assessing their effectiveness, authorizing the system, and monitoring its security. Although designed primarily for federal agencies, it can also be applied to other sectors for information security risk management.

ISO 31.000: The ISO 31.000 series, devised by the ISO (2018), provides principles, guidelines, and standards for risk management suitable for any organization, irrespective of size, type, or industry. This framework underscores the significance of understanding an organization's context and stakeholder requirements and covers a broad spectrum of risk types. Its principle-based and flexible approach allows customization according to specific organizational needs.

COBIT (Risk IT): COBIT, developed by ISACA (2019), incorporates risk management as one of its core components. The Risk IT extension focuses on identifying, assessing, and mitigating IT-related risks within an organization. It provides a structured approach to manage IT risks, taking into consideration business, IT, and assurance perspectives. While COBIT's primary focus is on IT governance and management, its Risk IT extension is specifically designed to address IT-related risks, making it highly relevant to organizations with a strong dependence on information technology.

Therefore, the COSO-ERM framework provides a comprehensive approach to enterprise risk management, covering a wide range of risks and industries. The NIST RMF is more focused on information security risk management in federal information systems but can be applied to other sectors as well. ISO 31.000 offers a flexible, principle-based approach to risk management, suitable for organizations of any size, type, or industry. Finally, COBIT, with its Risk IT extension, is tailored to address IT-related risks, making it highly relevant for organizations with a strong reliance on information technology.

4.3. Process steps and stages

The COSO-ERM (Committee of Sponsoring Organizations of the Treadway Commission, 2017) is an enterprise risk management framework that involves five stages, including governance, culture, strategy, objective-setting, performance, review, revision, and information communication. It highlights the integration of risk management into the organization's culture, strategy, and performance measurement.

The NIST RMF (NIST, 2018) provides a six-step process for managing information security risks, involving categorizing information systems, selecting, implementing, assessing, authorizing, and monitoring security controls. It emphasizes continuous monitoring and improvement of security controls.

ISO 31.000 (ISO, 2018) is a versatile risk management framework consisting of five stages: establishing context, risk identification, risk analysis, risk evaluation, and risk treatment. It promotes a structured, iterative, and adaptable approach to risk management across various industries.

COBIT (Risk IT) (ISACA, 2009) is a framework for the governance and management of information and technology risks. It comprises three core domains—risk governance, risk evaluation, risk response—which are further split into 22 processes covering risk identification, assessment, response, and monitoring. It aligns risk management with an organization's strategic objectives and facilitates effective decision-making and resource allocation.

Therefore, each of these frameworks offers unique process steps and stages, tailored to address different aspects of risk management. While COSO-ERM focuses on enterprise-wide risk management, NIST RMF is designed for managing information security risks. ISO 31.000 offers a flexible, cross-industry approach, while COBIT (Risk IT) specifically targets the governance and management of information technology risks.

4.4. Terminology and concepts

COSO-ERM (Committee of Sponsoring Organizations of the Treadway Commission, 2017) is a comprehensive risk management framework emphasizing integration of risk management into strategic planning and operational activities. Its five main components include governance and culture, strategy and objective setting, performance, review and revision, and information, communication, and reporting. It uses terms like risk appetite, risk tolerance, and risk capacity to define and manage risk levels.

NIST RMF (NIST, 2018) is a cybersecurity risk management framework primarily for U.S. federal government entities. The framework is a six-step process consisting of: categorize, select, implement, assess, authorize, and monitor. It employs risk categorization, which classifies information systems based on potential impact of a security breach, aiding in tailoring security measures.

ISO 31.000 (ISO, 2018) is a versatile risk management framework utilized across various industries. It outlines a structured risk management process with key concepts such as risk identification, risk analysis, risk evaluation,

and risk treatment. The process in ISO 31.000 is cyclical, emphasizing continuous improvement and adjustment to changing circumstances.

COBIT Risk IT (ISACA, 2009) is a framework designed for governance and management of IT risks. It builds on the broader COBIT framework and includes three domains: risk governance, risk evaluation, and risk response. It uses concepts like risk scenarios, risk profiles, and risk appetite to aid in identification, assessment, and management of IT risks in line with business objectives. Therefore, the four risk management frameworks - COSO-ERM, NIST RMF, ISO 31.000, and COBIT Risk IT - differ in their focus, terminology, and concepts. While COSO-ERM takes an enterprise-wide approach, NIST RMF focuses on information systems and cybersecurity, ISO 31.000 offers a broad and flexible risk management process, and COBIT Risk IT specifically addresses IT risks.

4.5. Key principles and practices

1. COSO-ERM: The framework is designed to provide a holistic approach to risk management. It encompasses eight interrelated components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. The COSO-ERM framework emphasizes the integration of risk management into an organization's overall strategic planning and performance management processes. It is applicable across various industries and focuses on creating a risk-aware culture through the alignment of risk appetite, risk tolerance, and strategic objectives (COSO, 2017).

2. NIST RMF: The NIST Risk Management Framework (NIST, 2018) is a structured process for managing information security and cybersecurity risks. It comprises six steps: categorize, select, implement, assess, authorize, and monitor. The NIST RMF is designed specifically for federal organizations and their contractors, but its principles can be applied to private-sector organizations as well. The framework emphasizes the importance of continuous monitoring and iterative improvement of risk management processes, as well as the integration of risk management with an organization's overall security strategy (NIST, 2018).

3. ISO 31.000: The ISO 31000 (ISO, 2018) is a set of principles and guidelines for risk management applicable across various industries and organizational types. It consists of three main components: principles, framework, and process. The ISO 31.000 framework promotes the integration of risk management into an organization's governance, strategy, and decision-making processes, with a focus on creating and protecting value. It is designed to be flexible and adaptable, allowing organizations to tailor their risk management processes to meet their specific needs and risk landscape (ISO, 2018).

4. COBIT (Risk IT): COBIT is a comprehensive governance and management framework for enterprise IT developed by ISACA (2019). The Risk IT domain of COBIT provides a set of principles, practices, and analytical tools for managing IT-related risks. It is based on three main components: risk governance, risk evaluation, and risk response. COBIT (Risk IT) emphasizes the importance of aligning IT risk management with enterprise risk management and promoting a risk-aware culture within an organization. It is particularly suited for organizations with complex IT environments and those seeking to manage risks related to information security, data privacy, and regulatory compliance (ISACA, 2019).

Hence, each of the four risk management frameworks offers unique strengths and focuses on different aspects of risk management. COSO-ERM provides a holistic approach to risk management across all organizational levels, while NIST RMF offers a structured process for managing information security and cybersecurity risks. ISO 31.000 is a flexible and adaptable framework that can be tailored to an organization's specific needs, whereas COBIT (Risk IT) is particularly suited for managing IT-related risks in complex environments.

4.6. Integration with other management frameworks

COSO-ERM: COSO-ERM is designed to integrate risk management with strategic planning and performance management, aligning risk appetite with organizational objectives. This framework is compatible with other management frameworks, such as the Balanced Scorecard and ISO 31.000 (Beasley, 2016). Its principles-based

approach allows for flexibility in its application, facilitating integration with various management systems and processes.

NIST RMF: It is a structured and systematic approach to managing information security risks (NIST, 2018). The NIST RMF is well-suited for integration with other cybersecurity frameworks, such as the NIST Cybersecurity Framework (CSF) and the ISO/IEC 27000 series (Chew et al., 2008). This framework is primarily designed for federal agencies but can also be applied to other organizations, offering a modular structure that promotes interoperability with diverse management systems.

ISO 31.000: It provides a set of principles, a framework, and a risk management process that can be adapted to any organization, regardless of its size or sector (ISO, 2018). ISO 31.000 is designed to integrate with other management standards, such as ISO 9001 (Quality Management), ISO 14001 (Environmental Management), and ISO/IEC 27001 (Information Security Management) (Purdy, 2010). Its high-level and principle-based structure ensures compatibility with various management systems and allows for seamless integration across different functions within an organization.

COBIT (Risk IT): It is a comprehensive IT governance and management framework developed by the ISACA. The Risk IT component of COBIT provides a structured approach to managing IT-related risks and aligning them with overall enterprise risk management (ISACA, 2009). COBIT (Risk IT) can be integrated with other management frameworks, such as ITIL, PMBOK, and ISO/IEC 27001, as well as with the broader COBIT framework, which addresses multiple aspects of IT governance and management (Tarantino, 2013).

5. PRACTICAL APPLICATIONS AND CASE STUDIES

In this section, we will explore practical applications and case studies related to various frameworks and standards used for risk management and governance. The first subsection focuses on the implementation of COSO-ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management) framework, which provides a comprehensive approach to managing risks within an organization. Moving on, we will discuss the implementation of NIST RMF (National Institute of Standards and Technology - Risk Management Framework), a widely recognized framework that helps organizations assess and manage risks to their information and systems. The next subsection highlights the implementation of ISO 31.000, an international standard that offers guidance on risk management principles and processes. Lastly, we will delve into the implementation of COBIT (Control Objectives for Information and Related Technologies) framework for Risk Governance and Management, which aids organizations in aligning IT governance with overall enterprise risk management practices. Through these case studies, we will gain valuable insights into the practical application of these frameworks and standards.

5.1. COSO-ERM implementation

This integrated framework emphasizes the importance of managing risk at all levels of an organization and is designed to help organizations achieve their strategic objectives (COSO, 2017). Here, we present practical applications and case studies that demonstrate the value and effectiveness of the COSO-ERM framework in real-world scenarios.

1. Financial Services Industry: A large multinational bank adopted the COSO-ERM framework to enhance its risk management practices following a series of regulatory fines and reputational damage (Deloitte, 2018). Implementing the COSO-ERM framework allowed the bank to identify and assess risks more effectively and align its risk management efforts with its strategic objectives. The bank's adoption of COSO-ERM resulted in a more robust risk management process and improved communication about risks among different levels of management, ultimately leading to better decision-making and risk mitigation.

2. Healthcare Industry: A major hospital system used the COSO-ERM framework to develop an enterprise-wide risk management program that addressed various risks, including patient safety, operational, and financial risks (Protiviti, 2019). The implementation of COSO-ERM enabled the hospital system to identify and prioritize risks,

allocate resources efficiently, and establish a risk-aware culture within the organization. This led to improved patient outcomes, reduced adverse events, and increased operational efficiency.

3. Manufacturing Industry: A global manufacturing company adopted the COSO-ERM framework to address supply chain risks and improve its business resilience (PwC, 2020). The company integrated the COSO-ERM framework with its existing risk management practices, allowing it to identify and assess risks in a more systematic and comprehensive manner. This approach helped the company better understand its supply chain vulnerabilities and implement risk mitigation strategies that enhanced its overall business resilience.

These case studies demonstrate the practical applicability and effectiveness of the COSO-ERM framework across various industries. By adopting COSO-ERM, organizations can improve their risk management processes, align risk management efforts with strategic objectives, and foster a risk-aware culture that ultimately leads to better decision-making and outcomes.

5.2. NIST RMF implementation

The NIST RMF has been adopted by a variety of organizations, including government agencies, defense contractors, and private sector entities, owing to its robust and systematic process for risk assessment, mitigation, and continuous monitoring (Joint Task Force Transformation Initiative, 2018). This section will explore the practical applications and case studies of NIST RMF implementation, highlighting the benefits and challenges faced by organizations when adopting this framework.

One notable example of NIST RMF implementation is in the United States Department of Defense (DoD). The DoD transitioned from the legacy Defense Information Assurance Certification and Accreditation Process (DIACAP) to the NIST RMF in 2014, aiming to improve the security posture and risk management processes of defense information systems (Department of Defense, 2014). The NIST RMF has allowed the DoD to standardize its risk management processes, enhance the security of its information systems, and foster greater collaboration with other federal agencies (Barker, 2016). However, the transition has faced challenges, such as the integration of existing processes and the need for additional training and resources to support the adoption of the new framework (NIST, 2016).

In the private sector, a case study of a multinational corporation implementing the NIST RMF demonstrates the framework's adaptability and effectiveness in managing risks associated with information systems (Smith and Hash, 2018). The corporation successfully integrated the NIST RMF into its existing risk management processes, resulting in a more comprehensive approach to identifying, assessing, and mitigating risks (Smith and Hash, 2018). Additionally, the implementation of the NIST RMF facilitated improved communication between the organization's information security and risk management teams, fostering a more collaborative and proactive approach to risk management (Smith and Hash, 2018).

Another case study showcases the NIST RMF's application in the healthcare industry, where a large hospital network adopted the framework to manage risks associated with the use of electronic health record (EHR) systems (HHS, 2017). The NIST RMF provided a structured approach for the hospital network to identify and assess risks related to the confidentiality, integrity, and availability of patient data, as well as to implement appropriate security controls to mitigate those risks (HHS, 2017). The hospital network reported an improvement in their overall security posture and a reduction in the number of security incidents following the implementation of the NIST RMF (HHS, 2017).

These case studies highlight the versatility and effectiveness of the NIST RMF in addressing risk management challenges across various industries and sectors. However, organizations should be mindful of the potential challenges associated with adopting the framework, such as the need for additional resources, training, and integration with existing processes.

5.3. ISO 31.000 implementation

ISO 31.000 provides a risk management framework that can be applied across various industries to ensure the effective identification, assessment, and management of risks. Below are some practical applications and case studies of the ISO 31.000 implementation:

1. Implementation of ISO 31.000 in the Aerospace Industry: The International Aerospace Quality Group (IAQG) developed a sector-specific risk management standard, AS9100, based on ISO 31.000. The implementation of AS9100 in aerospace companies has led to significant improvements in risk management practices, such as the integration of risk management into the product lifecycle, increased focus on risk communication and stakeholder engagement, and better alignment of risk management with business objectives (IAQG, 2016).

2. Implementation of ISO 31.000 in the Healthcare Industry: The implementation of ISO 31.000 in the healthcare industry has been shown to improve patient safety and reduce medical errors. For instance, a study by Elmoghazy et al. (2019) showed that the implementation of ISO 31.000 in a Saudi Arabian hospital led to a significant reduction in medication errors, as well as an improvement in the quality of care and patient satisfaction.

3. Implementation of ISO 31.000 in the Energy Sector: The implementation of ISO 31.000 in the energy sector has led to improvements in safety and environmental management. For example, the implementation of ISO 31.000 in a Norwegian oil and gas company resulted in a reduction in the number of safety incidents and environmental incidents, as well as improved risk communication and stakeholder engagement (Bjerga et al., 2013).

4. Implementation of ISO 31.000 in the Construction Industry: The implementation of ISO 31.000 in the construction industry has led to improvements in risk management practices and project outcomes. A case study by Murali et al. (2020) showed that the implementation of ISO 31.000 in a construction company in India resulted in improved risk identification and assessment, as well as a reduction in project delays and cost overruns.

5.4. COBIT implementation for Risk Governance and Management

Here are some practical applications and case studies of COBIT implementation:

1. The implementation of COBIT in a South African Telecommunications Company In this case study, the authors describe the successful implementation of COBIT in a telecommunications company in South Africa. The company used COBIT to align its IT governance and management practices with its overall business strategy. The implementation of COBIT helped the company to identify and mitigate potential risks, ensure compliance with regulatory requirements, and improve the efficiency and effectiveness of its IT processes. (Kanjo, J., and Grundlingh, W., 2015)

2. The implementation of COBIT in a Mexican Financial Institution In this case study, the authors describe the implementation of COBIT in a Mexican financial institution. The institution used COBIT to establish a comprehensive IT governance framework, improve the transparency and accountability of its IT processes, and increase its alignment with regulatory requirements. The implementation of COBIT helped the institution to reduce its IT-related risks, increase its operational efficiency, and enhance its customer satisfaction. (Corona-Sanchez, A., Martinez-Salinas, E., and Gonzalez-Navarro, F., 2017)

3. The implementation of COBIT in a Malaysian Oil and Gas Company In this case study, the authors describe the implementation of COBIT in a Malaysian oil and gas company. The company used COBIT to enhance its IT governance and management practices, improve the efficiency and effectiveness of its IT processes, and ensure compliance with regulatory requirements. The implementation of COBIT helped the company to reduce its IT-related risks, increase its operational efficiency, and improve its overall business performance (Abdullah, N. R., Ismail, N. A., and Harun, H., 2016).

6. CHALLENGES AND LIMITATIONS

Enterprise risk management (ERM) models such as COSO-ERM, NIST RMF, ISO 31.000, and COBIT have seen substantial interest in the recent period. However, the application of these models is fraught with several obstacles and constraints that organizations must contemplate (Mikes & Kaplan, 2015). This section provides an analysis of the implementation hurdles, training and educational necessities, flexibility and customization, and the ongoing improvement and monitoring needs for each mentioned framework.

6.1. Implementation Obstacles and Constraints of COSO-ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) introduced the COSO-ERM model in 2004 to assist organizations in managing their risks proficiently (Arena, Arnaboldi, & Azzone, 2010). However, the application of COSO-ERM encounters specific issues and restrictions.

A. Implementation barriers: The primary hindrance to implementing COSO-ERM lies in the deficient comprehension of the framework's principles and components. The intricacy of the COSO-ERM necessitates a lucid understanding of its principles, goals, and components (Bromiley et al., 2015). Furthermore, the application of COSO-ERM necessitates considerable resources, both time and financial, presenting a challenge to organizations.

B. Training and education: For a successful application of COSO-ERM, proper training and education play a pivotal role. Organizations need to invest in educating their employees about the principles and components of COSO-ERM. A lack of proper training and education can result in a dearth of understanding and misapplication of the framework (Spira & Page, 2003).

C. Adaptability and customization: COSO-ERM is a versatile framework that can be adjusted and tailored to an organization's specific needs. Nonetheless, organizations must cautiously approach the customization to avert potential adverse impacts on the framework's efficacy. Customization must align with the COSO-ERM framework's principles and goals (Nocco & Stulz, 2006).

D. Monitoring and continuous improvement requirements: To ensure the effectiveness of COSO-ERM, organizations need to constantly monitor their risk management processes. This monitoring should be a part of the organization's comprehensive monitoring process to identify any potential gaps or weaknesses in the risk management processes (Kaplan & Mikes, 2012).

6.2. Implementation Obstacles and Constraints of NIST RMF

The NIST Risk Management Framework (RMF) is a prevalent model used for managing risks in federal agencies. The application of NIST RMF also encounters some issues and restrictions.

A. Implementation barriers: The primary implementation hurdle for NIST RMF is a lack of awareness and comprehension of the framework's principles and components. NIST RMF is a complex model that requires a clear understanding of its principles, goals, and components. In addition, like COSO-ERM, applying NIST RMF involves substantial resources, which can be a challenge for organizations (Stamatis, 2003).

B. Training and education: Training and education are vital for the successful implementation of NIST RMF. Organizations should make an investment in training their employees about the principles and components of NIST RMF. Insufficient training and education can result in a lack of understanding and improper application of the framework (Stoneburner, Goguen, & Feringa, 2002).

C. Adaptability and customization: Like COSO-ERM, NIST RMF is a versatile model that can be tailored to an organization's specific needs. However, organizations should carefully approach the customization to prevent potential negative impacts on the framework's efficacy. Any customization should align with the principles and goals of the NIST RMF framework (Bayuk, 2010).

D. Monitoring and continuous improvement requirements: To ensure the effectiveness of NIST RMF, organizations should consistently monitor their risk management processes. This monitoring should be

incorporated into the organization's overall monitoring process to identify potential gaps or weaknesses in risk management processes (Ramachandran, 2012).

6.3. Implementation Obstacles and Constraints of ISO 31000:

ISO 31000 offers guidance on risk management principles and guidelines. The following are some of the implementation obstacles and constraints of ISO 31000:

A. Implementation Barriers: One of the significant implementation barriers is the lack of commitment from top management. The standard requires active involvement and commitment from senior management to ensure successful risk management efforts (Aven, 2016). Without top management's support, implementing the standard becomes challenging.

B. Training and Education: Another challenge is the absence of knowledge and understanding of the risk management process. Many organizations lack trained and competent risk management professionals needed for effective implementation. Education and training are crucial to ensuring that all stakeholders understand the standard and the risk management process (Purdy, 2010).

C. Adaptability and Customization: ISO 31000 is a generic standard that needs to be adapted and customized to fit an organization's specific context. Developing a risk management framework based on unique needs and requirements can be challenging, requiring extensive knowledge and experience in risk management (Smit, 2012).

D. Monitoring and Continuous Improvement Requirements: ISO 31000 requires organizations to continually monitor and review their risk management process. This monitoring demands a robust monitoring and evaluation system to ensure effective and efficient risk management processes. However, many organizations lack the necessary resources and expertise for an effective monitoring and evaluation system (Leitch, 2010).

6.4. Implementation Obstacles and Constraints of COBIT:

COBIT is a framework for IT governance and management. The following are some of the implementation obstacles and constraints of COBIT:

A. Implementation Barriers: One of the significant barriers is the lack of understanding and awareness of IT governance. Many organizations lack the necessary knowledge and skills for effective IT governance. Achieving the requisite change in mindset, culture, and behavior can be challenging (De Haes & Van Grembergen, 2008).

B. Training and Education: Training and education are crucial to ensuring that all stakeholders understand the COBIT framework and its components. However, many organizations lack the resources to provide adequate training and education to their staff (Ridley, Bayne, Outlay, & Ward, 1998).

C. Adaptability and Customization: Like the other frameworks, COBIT needs to be customized to fit an organization's specific context. Developing an IT governance framework based on unique needs and requirements can be a challenging task, requiring extensive knowledge and experience in IT governance (Van Grembergen & De Haes, 2009).

D. Monitoring and Continuous Improvement Requirements: COBIT requires organizations to consistently monitor and review their IT governance processes. This monitoring demands a robust monitoring and evaluation system to ensure effective and efficient IT governance processes. However, many organizations lack the necessary resources and expertise for an effective monitoring and evaluation system (Guldentops, 2004).

7. ROLE OF ASSURANCE AND CONSULTANCY OF INTERNAL AUDIT

The influence of internal auditors on the decision-making process and implementation of risk management systems is critical, particularly when taking into account the myriad cultural perspectives and expectations that exist within various organizational types and geographical locations. These frameworks, including COSO-ERM, NIST RMF, ISO 31.000, and COBIT, supply organizations with methodologies to manage risks effectively and augment their operational procedures (NIST, 2020; ISO, 2018; ISACA, 2019). As overseers of the efficacy of risk management

undertakings, internal auditors carry a significant responsibility. They evaluate whether the chosen frameworks are congruent with the company's aims, objectives, and the distinctive risks and challenges that it encounters.

The Institute of Internal Auditors (IIA, 2021) stipulates that internal auditors are tasked with providing assurance and consultancy services which aid organizations in reaching their goals through risk-informed and objective evaluations, advice, and insights. When it comes to risk management frameworks, internal auditors can add value by affirming that the selected frameworks are optimally tailored to the organization's particular needs and are in alignment with its broader objectives.

The COSO-ERM framework, widely recognized for its holistic approach to risk management, addresses all aspects of an organization's operations (COSO, 2017). Internal auditors are uniquely positioned to significantly influence the selection and implementation of COSO-ERM by assessing the organization's current risk management practices. This allows them to pinpoint any deficiencies or areas of weakness in these practices and propose solutions for enhancement.

In a similar vein, the NIST RMF provides a focus on managing information security risks (NIST, 2020). In the adoption of this framework, internal auditors can support organizations by assessing their current information security practices, identifying potential threats and vulnerabilities, and providing recommendations to address these risks effectively.

The ISO 31.000 framework is another option for organizations looking to instigate a robust risk management process (ISO, 2018). Internal auditors can guide the selection and application of ISO 31.000 by evaluating the company's present risk management practices, identifying sectors that could benefit from improvement, and advising on the effective incorporation of the framework.

When it comes to enterprise IT governance and management, the COBIT framework provides insightful guidance (ISACA, 2019). In the selection and application of COBIT, internal auditors can offer their expertise by assessing the organization's IT governance and management practices, highlighting any deficiencies or areas for improvement, and providing solutions for enhancement.

However, it's important to acknowledge that the roles and expectations of internal auditors may fluctuate based on cultural context and organizational type. Cultural differences can mold unique views on risk management and internal auditing practices, influencing the specific duties and approaches of internal auditors within these contexts. Similarly, the demands and requirements for internal auditors may differ among governmental bodies, private businesses, NGOs, and organizations operating in developed or less developed countries.

To understand the specific context in Türkiye, a thorough exploration of the country's internal auditing practices, led by TIDE and IDKK, cultural nuances, and prevalent expectations across diverse organizations would be necessary. Comprehensive understanding can be obtained through further research, scrutinizing authoritative sources like scholarly articles, reports, and publications from relevant Turkish institutions or professional bodies specializing in internal auditing.

8. CONCLUSION

ISO 31000 and COBIT frameworks are essential for managing risks and IT governance in organizations. This paper provided a detailed discussion on the implementation challenges and limitations of these frameworks, focusing on their implementation barriers, training and education, adaptability and customization, and monitoring and continuous improvement requirements.

The key findings of this paper are that organizations face various challenges and limitations when implementing ISO 31000 and COBIT frameworks. These challenges include the lack of commitment from top management, the lack of knowledge and understanding of the risk management process and IT governance, the need for adaptability and customization, and the requirements for monitoring and continuous improvement.

To successfully implement ISO 31000 and COBIT frameworks, organizations need to address the challenges and limitations discussed in this paper. The following are some recommendations for organizations:

1. Senior management should demonstrate commitment and provide the necessary resources for implementing these frameworks.

2. Organizations should provide adequate training and education to their staff to ensure that they understand the frameworks and their components.

3. Organizations should customize the frameworks to fit their specific needs and requirements.

4. Organizations should establish a robust monitoring and evaluation system to ensure the effectiveness and efficiency of the frameworks.

This paper provides a broad overview of the challenges and limitations of implementing ISO 31000 and COBIT frameworks. Future research could explore these challenges and limitations in more depth, focusing on specific industries or organizational contexts. Additionally, future research could investigate the effectiveness of these frameworks in managing risks and IT governance and their impact on organizational performance. Finally, research could explore the potential of integrating these frameworks with other management frameworks, such as the Balanced Scorecard or Six Sigma.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The author declares that there is no conflict of interest.

Funding: The author received no financial support for the research, authorship and/or publication of this article.

Ethical Approval: This article does not contain any studies with human participants or animals performed by the authors.

Author Contributions: Ahmet Efe (100%)

REFERENCES

Arena, M., Arnaboldi, M., and Azzone, G. (2010). The organizational dynamics of enterprise risk management. A*ccounting, Organizations and Society*, *35*(7), 659–675. doi: 10.1016/j.aos.2010.07.003

Aven, T. (2016). Risk assessment and risk management: review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1–13. doi: 10.1016/j.ejor.2015.12.023

Barker, W. C. (2016). *Guide for applying the risk management framework to federal information systems: A security life cycle approach*. National Institute of Standards and Technology.

Bayuk, J. L. (2010). *Cyber Security Policy Guidebook*. Hoboken, NJ: Wiley.

Beasley, M. S. (2016). *Enterprise risk management: today's leading research and best practices for tomorrow's executives* (Vol. 504). John Wiley and Sons.

Bjerga, T., Dingsør, A., and Kjelland, H. (2013). Risk management in the Norwegian oil and gas industry: Implementation of ISO 31.000. *Safety Science*, *55*, 82-91.

Bromiley, P., McShane, M., Nair, A., and Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning*, *48*(4), 265–276. doi: 10.1016/j.lrp.2014.07.005

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. (2008). Performance measurement guide for information security. *NIST Special Publication*, *800*(55), 1-64.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management - Integrating with strategy and performance.* Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO (2013). *Internal control - integrated framework. Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved from https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

COSO (2017). *Enterprise Risk Management: Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO (n.d.). *About COSO*. Retrieved from https://www.coso.org/Pages/aboutus.aspx

De Haes, S., and Van Grembergen, W. (2008). An exploratory study into the design of an IT governance minimum baseline through delphi research. *Communications of the Association for Information Systems, 22*(1), 443–458.

Deloitte (2018). *COSO ERM framework: Helping organizations to align their risk management approach with strategic objectives*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_RA_COSOERMFramework_150518.pdf

Department of Defense (2014). *Risk management framework (RMF) for DoD information technology (IT).* DoD Instruction 8510.01. Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

EFE, A. (2016). Devlet Denetleme kurulu raporunda belirtilen kalkınma ajansları sorunları üzerinden COSO ve COBIT standartlarına göre kök neden analizleriyle çözümleme. *Journal of Knowledge Economy & Knowledge Management, 11*(1).

EFE, A. (2018). An Analysıs of COBIT-5 process capability level for regional development agencies at public sector. *Erzincan Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(1), 321-335. Retrieved from https://dergipark.org.tr/en/pub/erzisosbil/issue/37685/435976

EFE, A. (2021). COSO bilgi ve iletişim bileşeninin kalkınma ajansları üzerinden analizi. *Denetişim*, (22), 69-88.

Elmoghazy, A. H., Aldebasi, B., Alkhaldi, W. M., and Alotaibi, A. F. (2019). The impact of ISO 31.000 on patient safety: A case study of a Saudi Arabian hospital. *Journal of Healthcare Risk Management, 38*(1), 15-24.

Guldentops, E. (2004). Governing and managing IT risks. *Information Systems Control Journal, 3*, 21-27.

Guldentops, E. (2004). Governing IT: the need for measures. *Information Systems Control Journal, 2*, 1–4.

HHS (2017). *Risk management framework for EHR systems: A case study. U.S.* Department of Health and Human Services. Retrieved from https://www.hhs.gov/sites/default/files/2017HealthITACRMFCaseStudy.pdf

Institute of Internal Auditors. (2021). *International Professional Practices Framework (IPPF).* Retrieved from https://na.theiia.org/standards-guidance/ippf/Pages/Standards-and-Guidance.aspx

International Aerospace Quality Group. (2016). *The AS9100 family of standards for aerospace quality management.* Retrieved from https://www.sae.org/iaqg/organization/as9100family

ISACA (2009). *Risk IT framework for management of IT-related business risks*. Retrieved from https://www.isaca.org/resources/bookstore/pages/product-details.aspx?sku=ISARITFV

ISACA (2019). *COBIT 2019 Framework: Introduction and Methodology.* Rolling Meadows, IL: ISACA.

ISO (2018). ISO 31000:2018 *Risk management — Guidelines.* International Organization for Standardization. https://www.iso.org/standard/65694.html

ISO (2018). *ISO 31000:2018 Risk management - Guidelines*. Retrieved from https://www.iso.org/standard/65694.html

Joint Task Force Transformation Initiative (2018). *Risk management framework for information systems and organizations: A System Life Cycle Approach.* National Institute of Standards and Technology Special Publication 800-37 Revision 2.

Kaplan, R. S., and Mikes, A. (2012). Managing risks: a new framework. *Harvard Business Review*, 90(6), 48–60.

Leitch, M. (2010). ISO 31000:2009—The new international standard on risk management. *Risk Analysis*, *30*(6), 887–892.

Mikes, A., and Kaplan, R. S. (2015). When one size doesn't fit all: evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance*, 27(1), 37–40.

Murali, R., Balakrishnan, K., and Vignesh, R. (2020). Implementation of ISO 31.000 for risk management in construction projects: A case study in India. *Journal of Construction in Developing Countries*, *25*(1), 45-66.

National Institute of Standards and Technology. (2018). *NIST special publication 800-37, Revision 2: Risk management framework for information systems and organizations*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST (2004). *Standards for security categorization of federal information and information systems*. Federal Information Processing Standards Publication 199. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

NIST (2009). *Standards for security categorization of federal information and information systems* (FIPS PUB 199). Retrieved from https://csrc.nist.gov/publications/detail/fips/199/archive/2004-02-01

NIST (2013). *Security and privacy controls for federal information systems and organizations* (Special Publication 800-53, Rev. 4). Retrieved from https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-53r4.pdf

NIST (2018). *Risk management framework for information systems and organizations: a system life cycle approach for security and privacy*. NIST Special Publication 800-37, Revision 2. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST (2020). *Security and privacy controls for information systems and organizations.* NIST Special Publication 800-53, Revision 5. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Nocco, B. W., and Stulz, R. M. (2006). Enterprise risk management: theory and practice. *Journal of Applied Corporate Finance*, *18*(4), 8–20.

Protiviti. (2019). *Implementing COSO's enterprise risk management framework in healthcare organizations*. Retrieved from https://www.protiviti.com/US-en/insights/implementing-cosos-enterprise-risk-management-framework-healthcare-organizations

Purdy, G. (2010). ISO 31000:2009—setting a new standard for risk management. *Risk Analysis*, *30*(6), 881–886.

PwC (2020). *Aligning COSO ERM with supply chain risk management*. Retrieved from https://www.pwc.com/us/en/services/consulting/library/aligning-coso-erm-with-supply-chain-risk-management.html

Ramachandran, S. (2012). Corporate risk management: process, techniques and insights. International Journal of Physical Distribution & Logistics Management, *43*(5/6), 480–484.

Ridley, G., Bayne, K., Outlay, C., and Ward, T. (1998). Evaluating the effectiveness of it governance. *Journal of Information Technology*, 13(4), 303–319.

Ross, R., McEvilley, M., and Oren, J. (2018). *Risk management framework for information systems and organizations: a system life cycle approach*. NIST Special Publication 800-37.

Smit, P. J. (2012). ISO 31000:2009 ERM standard in clinical medicine manufacturing. *International Journal of Health Care Quality Assurance*, 25(2), 126–140.

Spira, L. F., & Page, M. (2003). Risk Management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640–661.

Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution*. Quality Press.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). *Risk management guide for information technology systems*. NIST Special Publication, 800-30.

Van Grembergen, W., and De Haes, S. (2009). *Enterprise governance of information technology: achieving alignment and value, featuring COBIT 5*. Springer Science & Business Media.

Weill, P., and Ross, J. W. (2004*). IT governance: How top performers manage IT decision rights for superior results.* Boston, MA: Harvard Business School Press.

GENİŞLETİLMİŞ ÖZET

Giriş

Risk yönetimi çerçeveleri, organizasyonların etkin yönetimi ve işleyişi için riskleri belirleme, değerlendirme ve azaltmada önemli bir rol oynamaktadır. Bu çalışma, COSO-ERM, NIST RMF, ISO 31.000 ve COBIT olmak üzere dört yaygın risk yönetimi çerçevesinin karşılaştırmalı bir incelemesini sunmaktadır. Analiz, temel prensipler, yapı, risk değerlendirme yöntemleri ve farklı sektörlerdeki uygulanabilirlikleri üzerinden yapılmıştır.

Arka Plan

ISO 31000 ve COBIT çerçeveleri, organizasyonlardaki riskleri yönetme ve BT yönetişiminde önemlidir. Bu makale, bu çerçevelerin uygulanması, eğitim ve öğretim, uyarlama ve özelleştirme, izleme ve sürekli geliştirme ihtiyaçları gibi konulara odaklanarak uygulama zorlukları ve sınırlamalarını ele almaktadır.

Araştırma Problemi

Organizasyonlar, ISO 31000 ve COBIT çerçevelerini uygularken çeşitli zorluklar ve sınırlamalarla karşılaşmaktadır.

Çalışma, aşağıdaki varsayımlar üzerine kurulmuştur:

1. Seçilen risk yönetimi çerçeveleri (COSO-ERM, NIST RMF, ISO 31.000 ve COBIT), organizasyonların karşılaştıkları temel risklerin yönetimi ve BT yönetişimi için temsilci ve geçerli çözümler sunmaktadır.

2. Çalışmada belirtilen zorluklar ve sınırlamalar, ISO 31000 ve COBIT çerçevelerini uygulayan organizasyonlar için genel olarak geçerlidir. Belirli organizasyonlar veya endüstriler için daha spesifik zorluklar ve sınırlamalar bulunabilir.

3. Çalışmada sunulan öneriler, ISO 31000 ve COBIT çerçevelerini uygulayan organizasyonların genel başarılarını artırmaya yardımcı olabilir. Bununla birlikte, belirli organizasyonlar için daha spesifik stratejiler ve eylemler gerekebilir.

4. Gelecekteki araştırmaların, bu çalışmanın bulgularını ve önerilerini doğrulayabileceği ve genişletebileceği varsayılmaktadır. Bu nedenle, çalışmanın sonuçları ve önerileri, mevcut bilgi ve anlayışa dayalı olarak kabul edilmelidir.

Bu varsayımlar ışığında, çalışmanın sonuçları ve önerileri organizasyonların ISO 31000 ve COBIT çerçevelerini uygularken karşılaştıkları zorlukları ve sınırlamaları anlamalarına yardımcı olabilir. Bununla birlikte, organizasyonların kendi özgün durumlarını dikkate alarak, daha spesifik ve uygun çözümler bulmaları gerekebilir.

Araştırma Soruları

1. Bu çerçeveleri uygularken karşılaşılan zorluklar ve sınırlamalar nelerdir?
2. ISO 31000 ve COBIT çerçevelerinin başarılı bir şekilde uygulanması için hangi adımlar atılmalıdır?

Amaç

Çalışmanın amacı, ISO 31000 ve COBIT çerçevelerinin uygulanmasındaki zorlukları ve sınırlamaları ortaya çıkarmak ve bu çerçevelerin başarılı bir şekilde uygulanması için öneriler sunmaktır.

Yöntem

Çalışma, literatür incelemesi ve dört risk yönetimi çerçevesinin karşılaştırmalı analizine dayanmaktadır.

Bulgular

ISO 31000 ve COBIT çerçevelerini uygularken karşılaşılan zorluklar ve sınırlamalar; üst yönetimin yetersiz taahhüdü, risk yönetimi süreci ve BT yönetişimi hakkında bilgi eksikliği, uyarlama ve özelleştirme ihtiyacı ve izleme ve sürekli iyileştirme gerekliliklerdir.

Sonuçlar

ISO 31000 ve COBIT çerçevelerini uygularken karşılaşılan zorluklar ve sınırlamalar; üst yönetimin yetersiz taahhüdü, risk yönetimi süreci ve BT yönetişimi hakkında bilgi eksikliği, uyarlama ve özelleştirme ihtiyacı ve izleme ve sürekli iyileştirme gerekliliklerdir.

Organizasyonların ISO 31000 ve COBIT çerçevelerini başarılı bir şekilde uygulaması için, çalışmada belirtilen zorlukların ve sınırlamaların üstesinden gelinmelidir. Öneriler şunları içermektedir:

1. Üst yönetim, taahhüt göstermeli ve bu çerçevelerin uygulanması için gerekli kaynakları sağlamalıdır.

2. Organizasyonlar, çalışanlarının çerçeveleri ve bileşenlerini anlamalarını sağlamak için yeterli eğitim ve öğretim sunmalıdır.

3. Organizasyonlar, çerçeveleri kendi özel ihtiyaçlarına ve gereksinimlerine uyacak şekilde özelleştirmelidir.

4. Organizasyonlar, çerçevelerin etkinliği ve verimliliğini sağlamak için güçlü bir izleme ve değerlendirme sistemi kurmalıdır.

Gelecekteki araştırmalar, belirtilen zorlukları ve sınırlamaları daha ayrıntılı olarak inceleyebilir, belirli sektörler veya organizasyonel bağlamlara odaklanabilir. Ayrıca, gelecekteki araştırmalar bu çerçevelerin risk yönetimi ve BT yönetişimindeki etkinliğini ve organizasyonel performans üzerindeki etkisini inceleyebilir. Son olarak, yapılacak yeni araştırmalar bu çerçevelerin Denge Scorecard veya Six Sigma gibi diğer yönetim çerçeveleri ile entegrasyon potansiyelini keşfedebilir.