International Journal on Engineering Technologies and Informatics

SKEENA PUBLISHERS
Writing for your Success

Risk Management Framework Analysis

Review Article

Volume 4 Issue 1- 2023

Author Details

*Abrar Albarraq, Amani Alkayyal, Renad Bawareth, Sarah AlMarhabi, and Asia Othman Aljahdali**

Cybersecurity Department, College of Computer Science and Engineering, University of Jeddah

*Corresponding author

Asia Othman Aljahdali, Cybersecurity Department, College of Computer Science and Engineering, University of Jeddah

Article History

Received: January 10, 2023 Accepted: : January 12, 2023 Published: January 13, 2023

Abstract

Risk management is widely regarded as one of the most effective methods for preventing the occurrence, avoiding, or limiting the impact of risks through a systematic, structured approach. Therefore, it helps organizations achieve their desired goals with the fewest losses. While technology advances on a daily basis, cyber threats grow at an exponential rate. As a result, cyber risk has become an important field to manage in order to assist organizations in achieving their goals in terms of cyber security. In this study, we present the most popular and common risk management frameworks: the International Standard Organization ISO (ISO 31000:2018), the National Institute of Standards and Technology (NIST), and the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which will help the organizations handle the cyber risk. We review their structures, principles, and processes and how they are working to analyze, assess, and manage risk. Also, how to apply the risk management framework in the context of cybercrime. Finally, we discuss the features and limitations of each of them in terms of applicability, orientations, similarities, and contrasts.

Keywords: Risk management framework; ISO 3100; 2018; NIST; COSO

Introduction

Organizations working in today's digital environment rely more and more on technology every day to control their information assets in order to achieve their primary objectives and goals. For this purpose, it is critical for businesses to develop strategies and techniques enabling them to effectively understand threats they face and manage risks, thus fostering a safer knowledge climate. Risk management is defined as a simple and progressive measure that includes a comprehensive substance on the recognizable proof, examination, and response to external or internal factors that can harm the organization's primary information assets [1]. It consists of continuous risk framing, assessment, and evaluation of risks, followed by risk control actions to accommodate impacts on a company's performance and thus follow-up actions to monitor success and define next steps, even though risk management doesn't seem to have an evident repercussion on an organization's overall performance [2]. Effective risk management systems enable companies, among other things, to collect capital, improve decision-making, promote business continuity, influence the probability of risk materialization, increase operational performance, promote accurate financial statements, generate better credibility, and regulate suits. (AIRMIC, Warning, IRM, 2010) The growing importance of information risk management today has led to a range of frameworks and methodologies offering guidance for protecting data properties. The ISO (International Standardization Organization), COSO (Committee of Sponsoring Organizations), and NIST (National Institute of Standards and Technology) frameworks are among the most widely used frameworks. system for NIST risk management.

We therefore conducted this study in order to well define and compare the Risk Management System, the Operationally Important Danger, Asset, and Vulnerability Assessment, and thus the Risk Management Discipline Security in terms of their effectiveness and how they function. Three of the most well-known risk management systems have been presented and contrasted in the corresponding parts of this paper. These structures can be used by organizations as guidance. However, the board techniques upheld by their way of life, principles, spending strategy, nature, missions, and goals can ultimately combine highlights from different systems to customize their own risk [1]. The reminder for this paper is divided into the following sections:

Section 2 explains the International Organization for Standardization (ISO) Framework with an overview, structure, principles, framework, and how ISO implements risk management. Section 3 provides a detailed overview of the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) framework structure, principles, framework, and how ISO implements risk management. Section 4 describes the NIST (National Institute of Standards and Technology) framework with an overview, structure, principles, framework, and how ISO implements risk management. Section 5 compares the following risk management frameworks: NIST, ISO, and COSO, based on their respective classifications. Finally, we summarize what has been outlined in the paper and offer our conclusions.

International Organization for Standardization (ISO) Framework: ISO 31000 Standard

The International Organization for Standardization (ISO) issued 31000 standards for risk management processes, which provide instruction on the planning, implementing, measuring, and learning features of a risk management system and guidance for a best risk management practice. The first version was issued in 2009 (ISO 31000:2009). After continued risk management practices and feedback from practitioners worldwide, ISO considered that ISO 31000:2009 needed to be developed and released as ISO 31000:2018 in 2018. ISO 31000:2018 contains more strategic instructions than ISO 31000:2009 and focuses on integrating stakeholders and considerable managers with the risk management system of the organization by developing the human factor and all procedures depending on it [3]. To achieve its objectives, it recommends that risk management be embedded in organizational policies, corporate governance, culture, objectives, and activities. Also, it focuses on the repetitive nature of risk management because reviewing processes, actions, and procedures comes from continued analysis and knowledge. In addition, the new release reflects an open systems model by simplifying the content and regularly exchanging feedback with its external environment to better suit its contents and needs. The use of direct and clear language resulted in intelligence and ease of reading. The risk management terminology has been simplified with ISO Guide 73, "Risk Management - Vocabulary," which explains risk management terminology to make the standard more understandable [4].

The ISO 31000 contains ISO 31000:2019 Risk Assessment Techniques, which explain how to assess risk with appropriate techniques; ISO Guide 73:2009 Risk Management Vocabulary (vocabulary, terminology, and terms relating to ISO 31000); and ISO 31000:2018 Risk Management Guidelines. They assist each other and issue guidelines to gain a better understanding of best practices for risk management in organizations. It is important to know that ISO 31000 only gives instructions and directions but not requirements; therefore, it can't be certified [4]. ISO defines risk as "the effect of uncertainty on objectives." Uncertainty involves state, incomplete information, chance of occurrence, and consequences of events [5]. ISO 31000:2018 consists of three main components: principles, framework, and process. These components are integrated together and help to provide effective and efficient risk management operations.

One of the basic concepts and objectives of ISO 31000 is establishing and protecting value [6]. There are eight principles that can help you understand this concept:

a. The framework and process should be suitable and compatible (proportionate principle).

b. Stakeholders must be involved in the risk management process in a timely and sufficient manner (align principle).

c. The risk management approach required must be structured and comprehensive (comprehensive principle).

d. Risk management should be integrated with all of an organization`s activities (embedded principle).

e. Risk management expects, deters, acknowledges, and responds to both internal and external changes (dynamic principle).

f. Risk management accounts for any limitations in the available information.

g. Human and cultural factors are essential and should be considered in all steps of risk management.

h. The risk management framework is continuously improved through learning and experience [7,5].

The first five principles help with how a risk management initiative should be designed and planned, which is commonly referred to as PACED, while the rest are for continuous improvement of the risk management initiative's operation and continuous improvement [7]. ISO 31000 defines a risk management framework as "a set of components that support and sustain risk management throughout an organization." The framework goes deeper by incorporating five features: integration, design, implementation, evaluation, and improvement, which are coordinated and closely related to an organization's principles, providing integrations of risk management with the organization's functions and activities, and evaluating current practices for any breaches [3]. Stakeholders and senior majors should access integration for risk management with all activities of the organization. Leadership and commitment are represented in the responsibility for making risk management compatible with the objectives, strategies, and culture of the organization, including decision-making, and implementing it successfully by establishing appropriate policies and procedures, allocating resources, and making it available with a risk management system. Also, they ought to define "risk appetite": the amount and type of risk that may or may not be considered [8]. Integration into risk management is considered a dynamic and repeated step, and it depends on understanding the structure and context of the organization [8]. The remaining components of the framework are often represented as plan-do-check-act [8].

The design concept involves understanding the organization's internal and external contexts. The external context includes all external factors such as political, legal, social, technological, cultural, economic, and financial, whether local or international, as well as external stakeholders' needs, values, expectations, and relationships. The internal context refers to the organization's vision, goals, structure, policies, governance, cultures, responsibilities, strategies, resources, and information, as well as the needs, values, expectations, and relationships of its internal stakeholders [8]. Implementation entails including objectives and deadlines, as well as evaluating, defining, and modifying the decision-making process as needed. Ensure that risk management procedures are understood and applied. To achieve efficient risk management framework evaluation, organizations must continuously measure the framework's performance and determine if it still fits with their purposes and plans or if it needs to change [8]. Since risk management is a continuous and iterative process, the ability for improvement and development is possible through continuous adapting and monitoring of the risk management framework, which therefore handles external and internal changes and leads to evolving the organization's value [7]. ISO 31000:2018 Process refers to the methodological application of policies, procedures, and communications and consulting activities for establishing context and evaluating risks through reviewing, monitoring, analyzing, treating, and recording them [3].

The process includes guidance on scope, context, and criteria; communication and consultation; monitoring and review; and recording and reporting, which all assist stakeholders in recognizing risks and making decisions. Scope, context, and criteria: risk management can be practiced to a variety of degrees, so it`s important to specify the scope and objectives that relate to it. Establishing the context of the risk management process requires understanding the external and internal context of the organization, which will allow it to manage risk according to its goals and objectives. Risk appetite should be considered in a risk management framework because it aids in risk evaluation and decision-making [8]. Risk assessment consists of the identification, analysis, and evaluation of risks to determine whether additional action is required. In risk treatment, we choose alternative risk treatment options along with creating and implementing a risk treatment plan with a timeline and responsibilities [7]. Monitoring and review include planning, gathering and analyzing information, recording results, and providing feedback to all processes of risk management to measure and enhance the effectiveness of the risk management system. Documentation and reporting of risk management procedures and results aid in the gathering of information for decision-making, with the types of reports and information varying according to stakeholder needs and goals [8].

In assessing cyber risks, both ISO 31000 and IEC 27000 (information security management systems) should be used together, as this methodology helps to evaluate the technology requirements of organizations and determine the value of their information in cyberspace, which leads to determining the level of technological protection. Despite the ability of these two standards to mitigate against cyber damage, it is necessary to take into account business continuity, and ISO 22301 for business continuity management cares about this aspect [4].

National Institute of Standards and Technology (NIST) Framework

NIST (National Institute of Standards and Technology) could be a non-regulatory agency to find, share, discuss, and improve upon open-source tools, solutions, and processes that support privacy engineering and risk management. NIST guidelines are often developed to help agencies meet specific regulatory compliance requirements [9]. The Risk Management Framework provides a structured approach to risk management, ensuring that risk is managed in line with the organization's requirements, business objectives, and risk appetite. It is designed to provide a structured, yet flexible, means for analyzing and deciding the way to alleviate the risks that arise. The Framework was derived from and builds on the gathering of the International Standards Organization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), and NIST standards [10].

The risk management framework has several characteristics. It promotes and supports the concept of risk management and continuous licensing of information systems by implementing continuous and powerful monitoring. It promotes the use of automation to provide senior leaders with the specified information to make cost-effective, risk-based organizational information systems decisions that support their core activities and business functions. It defines the duty of the security controls inside and inherited from the information systems, such as the common controls between the systems. Additionally, it links information system-level risk management processes to organizational-level risk management processes through a risk executive. The framework also incorporates information security into the enterprise architecture and system development life cycle and provides emphasis on the choice, implementation, assessment, and monitoring of security controls and, therefore, the authorization of data systems [11]. The risk management framework (RMF) process has several steps, including security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The RMF promotes the concept of risk management and continuous licensing of information systems by implementing continuous and powerful monitoring. In order to make cost-effective, risk-based decisions with regard to organizational information systems serving their core missions and business functions, senior leaders include the specified information and incorporate information security into the life cycle of enterprise architecture and system development. through the Chief Risk Officer and determines the lines of responsibility for the security controls and measures that are deployed and applied within the organizational information systems and inherited by those systems, such as common controls [11]. The RMF steps are as follows:

Step 1: categorize. The information system is processed, stored, and transmitted by the system based on an impact analysis [12].

Step 2: Select. An initial collection of information system baseline security controls based on security categorization, tailoring, and supplementing the baseline as necessary on the basis of an organizational risk assessment and local conditions [13].

Step 3: Implement. Explain how the security controls are used within the information system and its operating environment.

Step 4: Assess. Security controls use appropriate and effective assessment procedures to determine the extent to which controls have been properly implemented and operate as planned to achieve the desired result in order to meet system security requirements.

Step 5: Authorize. The information system depends on identifying the risks to which organizational assets, individuals, and other organizations are exposed and recognizing that this risk is acceptable.

Step 6: Monitor. Monitoring security controls in the information system on an ongoing basis includes assessing the effectiveness of the control, documenting changes in the system or operating environment, conducting security impact analyses of changes that occur, and reporting the security state of the system to the regulatory officials assigned. Figure 1 shows the six-step RMF process [11].

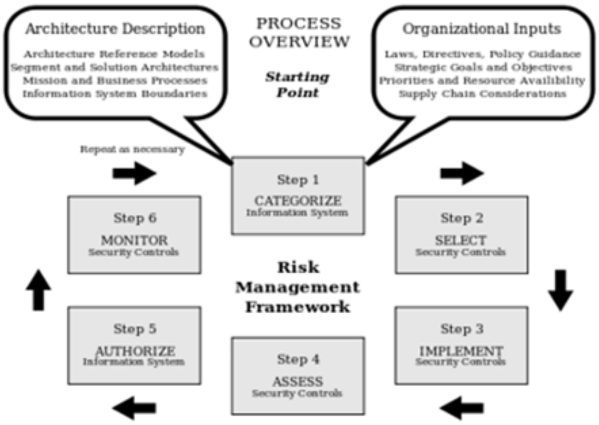


Figure 1: Risk management framework [13].

Managing security risks related to the information system is a complex and multifaceted task that involves the participation of the entire organization, from senior leaders who provide the strategic vision and priorities of the organization's high-level goals, to mid-level leaders who prepare and manage initiatives to individuals on the front lines who develop, implement, and operate systems that support the core functions of the organization. Risk management is often seen as a comprehensive activity that is completely integrated into every aspect of an organization. This illustrates a three-tiered approach to risk management that addresses risk-related concerns at three levels: the organization level, the mission and business process level, and the information system level. Figure 2 shows three levels of organization wide risk management [12].

Level 1 is concerned with risks from an organizational standpoint, and this is accomplished by developing a comprehensive, enterprise-wide risk management strategy that includes

a. The techniques and methodologies that the organization plans to use to assess system-related security risks and other risks specific to the organization.

b. procedures and processes that the organization plans to use to assess the risks that have been identified.

c. Measures used by the organization to mitigate and deal with identified risks

d. Determine the level of risk that the organization plans to risk tolerance

e. How to monitor risks on an ongoing basis despite the changes that take place in the information systems and work environments that contain them

f. Determine the kind of control the organization plans to utilize to ensure that the risk management strategy is implemented effectively and successfully.

g. The risk management approach is disseminated to organizational and contracting officials who have responsibility for planning implementation and supervision programs as part of the overall governance framework defined by the company, such as delegating managers and chief information officers, chief information security officials, system administrators, and integrated information services [11].

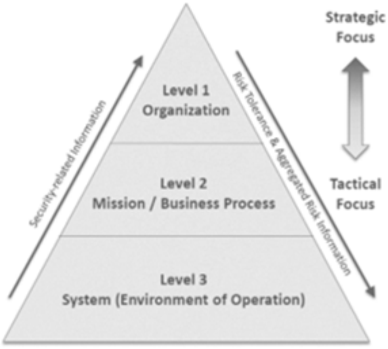

Strategic Focus
Tactical Focus
Level 1
Organization
Level 2
Mission / Business Process
Level 3
System (Environment of Operation)
Security-related Information
Risk Tolerance & Aggregated Risk Information

Figure 2: Three Levels of Organization-Wide Risk Management [16].

Level 2 deals with risk from a mission and business process perspective and is guided by the risk decisions at Level 1. Level 2 activities closely associated with enterprise architecture include:

a. Defining the organization's main missions and business processes

b. Prioritizing missions and business processes with regard to the organization's goals and objectives

c. Defining the types of information that the organization needs to conduct the specified tasks and business processes efficiently and, thus, the information flows to the organization both internally and externally

d. Developing a broad strategy to protect the organization's information and integrating information security standards and requirements into basic tasks and business operations, determining the degree of independence of the subsidiary organizations within the parent organization that the organization allows to assess, mitigate, evaluate, control, and accept risks [11].

Level 3 deals with risk from an information system perspective and is guided by the risk decisions at levels 1 and 2. It has an effect on the definitive selection and implementation at the information system level of the requisite protections and countermeasures of security controls.

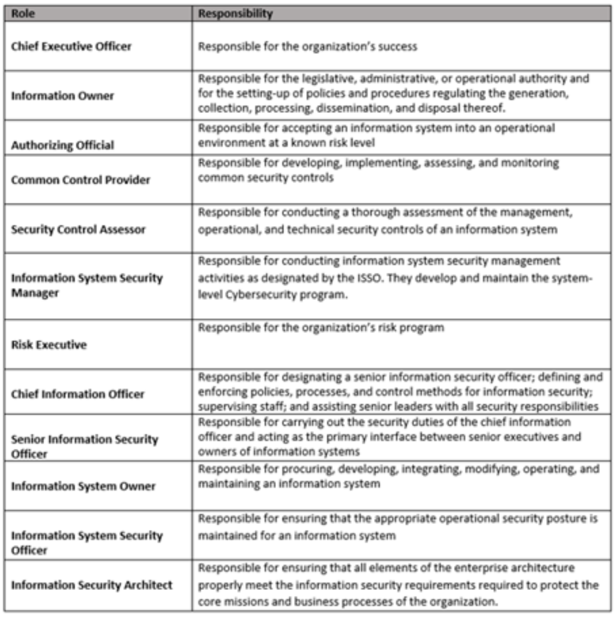
a. Provision of the security controls by the organization or an external provider [11]

b. The collection of appropriate management, organizational, and technical security controls from NIST Special Publication 800-53 meets the standards and specifications for information security. [14]

c. Outsourcing agreements such as contracts and interagency agreements, arrangements for business lines, licensing agreements, and supply chain agreements [14]

d. Security controls are usually traceable to the security standards set by the company to ensure that the criteria are fully met during the design, production, and implementation of the information system. Figure 2 shows three levels of organization-wide risk management.

The RMF identifies 13 roles and responsibilities of key participants in the organization's risk management. Figure 3 depicts the RMF's 13 roles and responsibilities. A systematic and structured language for cybersecurity risk management is provided by the Framework. The core involves practices that can be integrated into a cybersecurity program that can be customized to meet the needs of any organization. The framework is structured to complement the cybersecurity program and risk management processes of an enterprise, not replace them. The process of creating and developing system profiles provides an opportunity for organizations to identify and enhance areas in which they can improve existing processes or introduce new processes. When combined with the easy-to-understand language of the system, these profiles allow for stronger communication within the organization. Pairing Framework Profiles with an implementation plan helps an organization take full advantage of the Framework by allowing improvement initiatives between organizational stakeholders to be prioritized and shared cost-effectively, or by setting goals [15].



Role	Responsibility
Chief Executive Officer	Responsible for the organization's success
Information Owner	Responsible for the legislative, administrative, or operational authority and for the setting-up of policies and procedures regulating the generation, collection, processing, dissemination, and disposal thereof.
Authorizing Official	Responsible for accepting an information system into an operational environment at a known risk level
Common Control Provider	Responsible for developing, implementing, assessing, and monitoring common security controls
Security Control Assessor	Responsible for conducting a thorough assessment of the management, operational, and technical security controls of an information system
Information System Security Manager	Responsible for conducting information system security management activities as designated by the ISSO. They develop and maintain the system-level Cybersecurity program.
Risk Executive	Responsible for the organization's risk program
Chief Information Officer	Responsible for designating a senior information security officer; defining and enforcing policies, processes, and control methods for information security; supervising staff; and assisting senior leaders with all security responsibilities
Senior Information Security Officer	Responsible for carrying out the security duties of the chief information officer and acting as the primary interface between senior executives and owners of information systems
Information System Owner	Responsible for procuring, developing, integrating, modifying, operating, and maintaining an information system
Information System Security Officer	Responsible for ensuring that the appropriate operational security posture is maintained for an information system
Information Security Architect	Responsible for ensuring that all elements of the enterprise architecture properly meet the information security requirements required to protect the core missions and business processes of the organization.

Figure 3: Roles and responsibilities of RMF [13,17].

Committee of Sponsoring Organizations of The Treadway Commission (COSO) Framework

In 1985, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed. In 1992, they published the internal control integrated framework. The United States Congress passed the Sarbanes-Oxley Act of 2002 (SOX), after the major financial reporting failures at the beginning of the 2000s. Furthermore, SOX addresses the corporate management environment and asks U.S. government agencies to define and maintain acceptable internal control processes and financial reporting systems. The organizations are greatly unified around the COSO framework. Because a certain acceptable internal control framework is not provided for by SOX, based on the survey, 82 percent list the COSO framework as their framework for internal controls [16]. The COSO published an updated internal control framework in 2013 and declared that it would be activated on December 15, 2014, and they would be replacing the 1992 framework with that framework. Significant business and operating environment changes that had occurred in the two decades since the initial framework's release were motivated by the 2013 update. These changes benefit from increased outsourcing, regulation, globalization, and reliance on technology. The modified COSO 2013 framework lists 17 principles across its five internal control components, based on the concepts given in the original version of the framework to strengthen internal controls and evaluations [17]. Figure 1 shows the COSO cube.

Figure 4 shows While in the 1992 framework, control principles were stated, they were not directly addressed until the current publication. The principles help to formalize COSO's central criteria and offer guidelines on what constitutes good control.

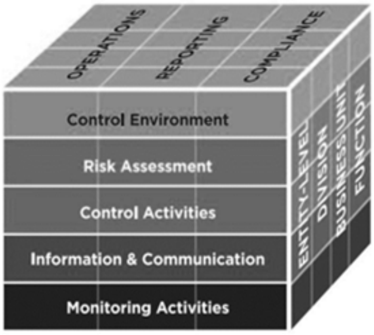


Figure 4: The COSO cube represents its five components.

The five key components of the updated COSO Framework 2013 are defined as follows: A collection of standards, structures, and procedures that provide the basis for successful internal control over the enterprise are defined in the control environment. A control environment relates to the Institute of Internal Auditors (IIA) and is the basis on which an efficient internal control structure is managed and established in an enterprise that aims to:

i. meet the strategic goals of the organization;

ii. provide external and internal stakeholders with credible financial statements;

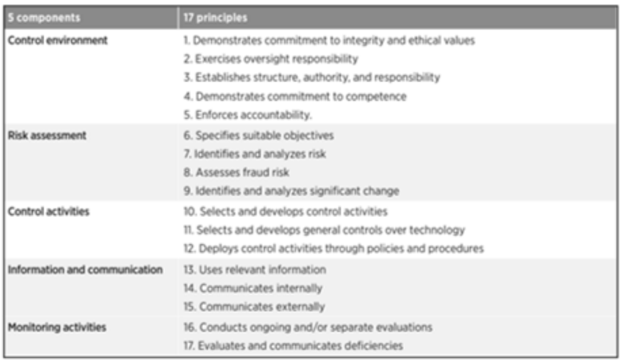
iii. conduct the business of the organization effectively and efficiently;

iv. conform with all laws and regulations; and

v. protect its assets [18].

The basis for deciding how risks can be handled is laid out in the risk assessment. The concept of "risk" refers to the possibility of a situation occurring and how much it will have an adverse impact on the achievement of organizational goals. In order to evaluate the effect of possible changes in the internal and external environment and to take steps to mitigate and manage the impact, risk assessment requires perfect management [18]. The collection of actions for control activities is typically specified in regulations, practices, and standards that help manage risk mitigation to ensure the achievement of goals. Control activities can be performed at all levels of the organization and may be detective or preventive in nature. In order to support internal control elements, information and communication are created or developed by management from both internal and external sources. In order to adapt to and facilitate the fulfillment of specifications and goals, communication based on internal and external sources is used to disseminate important information within and outside the organization as necessary. Internal information communication helps senior managers communicate to workers that the actions under control can be taken seriously. Monitoring activities are annual or regular reviews to ensure that each of the five internal control components is controlled, that the influence of the principles is still monitored in each component, that they are present, and that they are working according to their objectives [18].

The COSO 2013 updated framework is an accurate, resilient, and cost-effective framework for the development and evaluation of organizations' internal control systems. The five internal control components and their related principles should be confirmed by the organization in order to improve controls and evaluations. The following table lists the 17 internal control principles across each of their five internal control components as presented in the 2013 Framework. See Figure 2 [18]. The Environmental Scanning Committee of the American Accounting Association's Accounting Information Systems reviewed the updated COSO 2013 framework and communicated their view that, based on the improvements of the updated framework, the updated framework helps and strengthens the internal control of the organization's system. Through evaluation of the final 2013 COSO update, U.S. accounting professionals notice an increase in the strength of internal controls related to the technical part (cyber security, personal device security, backup data, and encryption data) based on the updated COSO framework [18]. In order to handle cyber threats in a protected, vigilant, and robust way, enterprises should see their cyber profile through the components of internal control. For example, see Figure 5.



5 components	17 principles
Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability.
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys control activities through policies and procedures
Information and communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Figure 5: The five internal control components and their related 17 principles [20].

Control Environment: Does the Management Committee understand the organization's cyber-risk profile and how the company manages the emerging face of cyber-risk management?

Risk Assessment: Does the company and its serious stakeholders understand how cyber risk could affect the objectives of the company based on the evaluations of activities, reporting, monitoring, compliance assessments, and information collected?

Control Activities: Does the company have technology-level management practices that help the organization handle cyber risk within the organization's appropriate level? Have these control activities been deployed by the company through structured rules and procedures?

Information and communication: Does the company define the criteria for information to handle internal cyber risk control? Does the company support the functioning of internal management through the external and internal communication protocols and channels that have been identified? How can a cyber-risk incident be handled, responded to, and shared by the company?

Monitoring Activities: How does the company choose, evolve, and execute evaluations to verify the effectiveness of operating the internal controls that address the cyber risks? How is the organization tracking its cyber risk profile? When deficiencies are discovered, how are these deficiencies prioritized and communicated for corrective action? [19]

One of the biggest challenges facing technology risk managers is the idea of risk appetite. The glossary of the COSO ERM framework describes "risk" as "the probability of events occurring and affecting the achievement of strategy and business goals" and "risk appetite" as "the form and amount of risk." The probability that events occur and affect the achievement of strategy and business goals is "the possibility that events will occur and affect the achievement of strategy and business objectives." "Risk appetite" means "the types and amount of risk that a company is willing to consider valuable on a broad level in its pursuit." Risk appetite is defined as "the types and amount of risk that a company is willing to simply accept in pursuit of something valuable."However, these same innovations can also cause substantial harm to the image of an organization and cause litigation. The quantification of the appetite for technology risk poses greater challenges for risk managers, who view technology risk as "all or nothing"—that is, either a breach happens or not—as a vital financial risk that focuses on risk-adjusted returns. Many businesses, for example, are wary of being breached, even if it means incurring exorbitant or significant costs.

To handle risk in a highly advisable business manner, companies track and evaluate their activities against industry guidelines or guidance (e.g., CoBIT, ISO, PCI Security Standards, and the Internet Security Controls Center). Such criteria, however, are not always quantifiable but provide a framework for organizations to assess their risk appetite. Alternatively, some organizations use a maturity model to benchmark or set step-level goals (e.g., Gartner or CMMI guidelines supported); risk appetite is then characterized by how well the organization, relative to others, manages its technology risk. It is important to note this challenge when contemplating the risks addressed, however, because the general practices used in one's industry are closely correlated with these considerations as well as the risk appetite of a business. The authors of the COSO ERM system understood and appreciated the effect of technology on enterprise risk; they established within the "Looking into the Future" segment of the manager overview that organizations will continue "to face a future filled with volatility, complexity, and ambiguity." They also identified four illustrative patterns that affect enterprise risk management, each meaning "to face a future filled with volatility, complexity, and ambiguity." It focuses on tackling data proliferation, leveraging informatics and automation, balancing the importance of risk management, and creating stronger organizations.

Enterprise risk management's underlying theory is that each company exists to provide value for its stakeholders. All organizations face uncertainty, so the dilemma for management is to see what proportion of uncertainty to consider simply because it wants to maximize the value of stakeholders. Uncertainty poses both risk and chance, with the potential to erode or boost value. Enterprise risk management helps management handle complexity and related risk and opportunity efficiently, improving the ability to generate value. Value is improved when managers set targets and strategies to aim for an optimum balance between return goals, development, and related risks, and to deploy capital efficiently and effectively in pursuit of the objectives of the organization. Control of business risk includes:

i. Aligning risk appetite and strategy Management considers the risk appetite of the company in determining strategic options, identifying relevant priorities, and designing risk management processes.

ii. Enhancing risk response choices Enterprise risk management offers the rigor to define and select risk mitigation, reduction, sharing, and acceptance among alternative risk responses.

iii. Reducing operational surprises and losses: companies can recognize and respond to potential incidents to minimize surprises and related costs or losses.

iv. Improving capital deployment: The acquisition of comprehensive risk knowledge enables management to evaluate total capital requirements efficiently and improve the allocation of capital.

v. Enterprise risk management helps ensure efficient reporting and compliance with legislation and regulations and helps mitigate harm to the entity's reputation and its related implications.

Discussion

The three risk management systems examined in this paper share the common goal of guiding risk monitoring organizations through a combination of massive methodologies that run through all levels of an organization. However, there are many distinctions between each of these techniques. They have a different collection of positive and negative qualities that can be combined to meet the needs of an organization. The world of validation and their primary goals are the first significant differences between them. However, within the United States, the NIST Risk Management System is mostly validated and concentrated on government organizations, Table 1 while ISO 31000 and its supporting materials are internationally accepted and can be adapted for use in the public, private, and community sectors. Within the USA, COSO is often approved and targets private organizations. The NIST system focused on the reassurance of information assets and cybersecurity. In addition, the system includes plenty of publicly accessible knowledge to help public and private institutions implement risk management strategies. It is important to note that this approach is significantly more robust in terms of the security of information systems, which is also useful for compliance with FISMA regulations. In comparison, during a wide variety of industry operations and in the absence of appropriate control considerations, ISO provides general risk management guidelines. COSO also specializes in internal controls and precise reporting as risk reduction mechanisms.

Risk management is not a simple process, as shown by prior definitions and comparisons. These structures can provide guidance to organizations, but they must carefully evaluate which ones work best for their specific cases while supporting their structure, principles, and key objectives. As shown by previous descriptions and comparisons, risk management is not a simple process. Organizations can find guidance from these frameworks but should examine them carefully. Which of them fits better, assisted by their framework, principles, and key goals, for their unique cases? It is also important to note that organizations face complex challenges, making it vital for these systems to undergo continuous changes for the purpose of adaptation. Oh. Es. It is also important to note that organizations face challenges that are complex, making it vital for these systems to undergo continuous changes. For purposes of adaptation, The fundamental mottos of frameworks are focused on the principles that include the availability, confidentiality, and fairness of the information of an entity by adopting processes responsible for setting up, implementing, running, controlling, updating, maintaining, and developing the information security management system (ISMS) of the organization on the basis of the provision of cyber security systems (ISMS). While modern frameworks such as COSO, ISO, and NIST are not rivals, they complement each other in terms of use. Like COSO, NIST offers a corporate view of risk management, while NIST provides a company with security practices for the IT environment. ISO, on the other hand, provides a framework for managing information security in IT environments, as well as physical and human dimensions and business objectives.

The COSO framework was formed with three internal objectives for an organization, which are: monitoring an organization's general internal operations effectively and efficiently; obtaining an organization's precise financial report; and supporting the company if it wants to comply with external rules. The COSO system provides a company with the means to regulate its organizational climate, which is set up by top management to oversee employee training on the value of control, punishment of employees (including supervisors) who break the law, the attention of the board of directors, and other board issues

[20,21]. The 17 principles and five components of the COSO 2013 system are: control environment, risk evaluation, information and communication, monitoring activities, and auditing. These five components are reliable, resilient, scalable, and cost-effective in evaluating and implementing the organization's internal control framework. Domain control standards such as trusted access sources, record management, organizational oversight, operational accountability, task segregation, audit and risk management, and operational controls of an enterprise against cyber security threats are represented by the COSO framework [20].

Table 1: Framework Comparisons.

Framework	The Orientation	Pertinent Publications	Concentration	Overall Strategy
NIST	Government (possible adaption for industry)	NIST Special Publication 800-30 Guide for Risk Assessment Conducting NIST Special Publication 800-37 Guide for the Application to Federal Information Systems of the Risk Management Framework: A Protection NIST Special Publication 800-39 Handling the Risk Organization, Mission, and Knowledge System of Information Security View NIST Special Publications 800-53 and 53A Recommended Federal Information Systems and Organizations Security Controls and Guide for the Implementation of Security Control	Information risk management assessment monitoring and cybersecurity	Management of information security accomplished by separating the evaluation consists of planning, communication of behavior and maintenance in various processes.
ISO	Public private and community organization	ISO 31000: 2009 Principles of Risk Control and Guidance ISO Guide 73 2009 Vocabulary of Risk Management ISO/TR 31004.2013 Instructions for ISO 31000 Implementation ISO/ EC 31010:2009 Strategies for Risk Assessment	Generic guideline for risk management in a diverse set of activates from the industry	Risk management concepts were endorsed in the system design. A context analysis, risk evaluation and treatment process consistent with feedback mechanisms
COSO	Enterprise	Integr ated System 2013 Internal Control False financial statements: 1998-2007 2004 Enterprise Risk Management- Integrated System for Company Risk Management (next version in process)	Risk management, internal controls and financial fraud deterrence	Aligns priorities, sections (with values or guidelines) and organizational structure

The architecture of the ISO (International Organization for Standardization) was established to implement the process model "Plan-Do-Check-Act" (PDCA), which is used to construct all the information security management system (ISMS) processes for an organization (Syahputri 5). The sole aim of this system is to guarantee the accessibility, confidentiality, and fairness of the data of an entity. This International Standard Company contributes trusted access, continuity, and availability of access; organizational reporting; records management; audit enforcement; and risk management, as well as an organization's operational controls. It also ends the scope of areas such as change management, organizational accountability, and the division of an organization's duties. The NIST system provides a wide field of information security and an organization's control area to deter cyber security threats. It provides the basic elements of computer security, denotes the related duties and functions, and reveals the risks. Another section of this framework explains how information security policies can be applied in program management, risk management, computer security life cycle protection planning, and the appropriate assurance steps. Another part of this covers organizational controls, including staff and user concerns, emergency preparedness, incident handling, education and training, computer operation and support protection considerations, as well as environmental and physical security considerations. Organizations that include this structure will govern areas such as records management, operations reporting, records management, organizational accountability, and division of duties.

Conclusion

After evaluating the ISO (International Standardization Organization), COSO (Committee of Sponsoring Organizations), and NIST (National Institute of Standards and Technology) frameworks for the whole matter of this topic, there were several elements and factors that affected cybersecurity. There was a definition of cybersecurity and discussion that by using cybersecurity, all the organizations saved and secured their information and data from being used by outside users, and it provided the users with a data protection system. In some parts of the project, it was discussed that the information about the effective factors and elements that framed the cybersecurity, such as security structure, computer and data security hardware, a secure operating system, a secure application, and secure encoding, was provided by the security management and helped secure all the data and information of the organization. Following the evaluation, there are ISO (International Standardization Organization), COSO (Committee of Sponsoring Organizations), and NIST (The National Institute of Standards and Technology) frameworks that are comparatively similar to improving the risk management analysis. COSO is a type of performance framework with five components as previously mentioned, ISO is a type of guidelines that instruct the effects and condition of the risk and also describe the principles. So, there was also a definition of the protocols that should be used for protecting the data and information. In this project, it is very clear that data breaches are not just the problem of one state or country but the problem of the whole world. The code of conduct and protocols should also be in place for cybersecurity. There is a need to conduct awareness programs on how to use various tools and platforms in cyberspace. Such tools and techniques assist the protocol in making data protection; without the technical way of cybersecurity, whether the topic was on protecting or hacking, the technical way had to be included. So, the overall conclusion is about using and protecting cybersecurity, which protects an organization's data and information, making the organization feel safe and secure, and also keeping their analyzing collection to cybersecurity without a doubt.

References

1. https://www.theirm.org/media/886062/ISO3100_doc.pdf
2. http://www.coso.org/aboutus.htm
3. Rampini Gabriel Henrique Silva, Harmi Takia, Fernando Tobal Berssaneti (2019) Critical Success Factors of Risk Management with the Advent of ISO 31000 2018-Descriptive and Content Analyzes. Procedia Manufacturing 39: 894-903.
4. https://www.iso.org/iso-31000-risk-management.html
5. Aven Terje (2011) On the new ISO guide on risk management terminology. Reliability engineering & System safety 96(7): 719-726.
6. Florea, Radu, Ramona Florea (2016) Internal audit and risk management. ISO 31000 and ERM approaches. Economy Transdisciplinarity Cognition 19(1): 72-77.
7. https://www.theirm.org/news/standard-deviations-a-risk-practitioner-guide-to-iso-31000
8. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
9. O'Reilly Patrick D, Kristina Rigopoulos, Larry Feldman, Gregory Witte (2020) 2019 NIST/ITL Cybersecurity Program Annual Report. NIST Special Publication 800 x: 211.
10. Kohnke, Anne, Ken Sigler, and Dan Shoemaker (2016) Strategic risk management using the NIST risk management framework. EDPACS 53.5: 1-6.
11. Joint Task Force Transformation Initiative Guide for applying the risk management framework to federal information systems: A security life cycle approach. No. NIST Special Publication (SP) 800-37 Rev 1 National Institute of Standards and Technology 2014.
12. FORCE JOINT TASK TRANSFORMATION INITIATIVE (2010) Guide for applying the risk management framework to federal information systems. NIST special publication 800: 37.
13. Force Joint Task Transformation Initiative (2013) Security and privacy controls for federal information systems and organizations. NIST Special Publication 800.53: 8-13.
14. Force Joint Task (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Final Public Draft) No NIST Special Publication (SP) 800-37 Rev. 2 (Draft). National Institute of Standards and Technology.
15. https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework
16. Addy Noel D, Nathan R Berglund (2020) Determinants of Timely Adoption of the 2013 COSO Integrated Framework. Journal of Information Systems 34(1): 1-20.
17. Ritteneg Larry E (2013) COSO 2013 a reflection of the times: the long-awaited Internal Control-Integrated Framework update aims to help organizations better design and implement controls, with an eye toward today's business challenges. Internal Auditor 70(4): 60-66.
18. (2019) Committee of Sponsoring Organizations of the Treadway Commission. COSO internal control–Integrated framework: An implementation guide for the healthcare provider industry.
19. Galligan Mary E, Kelly Rau (2015) COSO in the Cyber Age. Deloitte.
20. http://www.coso.org/documents/coso_erm_executivesummary.pdf
21. http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf