**Cybersecurity Risk Audit: A systematic literature review**

I.D. Sanchez-Garcia1, A.M. Rea-Guaman2, T. San Feliu1 and J.A. Calvo-Manzano1

1 Universidad Politécnica de Madrid, ETS Ingenieros Informáticos

Madrid, España

[isaacdaniel.sanchez@alumnos.upm.es](mailto:isaacdaniel.sanchez@alumnos.upm.es),

{tomas.sanfeliu, joseantonio.calvomanzano}@upm.es,

2 Universidad de las Fuerzas Armadas – ESPE, Departamento de Ciencias de la Computación

Sangolquí, Ecuador

[amrea1@espe.edu.ec](mailto:amrea1@espe.edu.ec)

**Abstract.** One of the stages of cybersecurity risk management is monitoring and review. This stage is part of the continuous improvement of a cybersecurity risk management system. This article aims to carry out a state-of-the-art cybersecurity risk audit where common objectives are established, and the guidelines of the cybersecurity risk audit are analyzed. The SLR was carried out considering the studies of the last ten years (2012-2022), from which 23 studies that mentioned cybersecurity risk audit objectives and guidelines were identified. The relationships among different objectives of cybersecurity risk audit were identified. In addition, the most used cybersecurity risk audit guidelines (e.g., the ISO 27000 family and the NIST CSF), and their application scopes were also identified. Additionally, it was identified that the cybersecurity risk audit approaches could be classified in the primary studies: 1) strategic, 2) technical, and 3) process. Finally, it is considered that the cybersecurity risk audit can be complemented by considering attributes of the SOX-COSO and IAASB internal control guides.

**Keywords:** Cybersecurity; Audit; Assurance; Compliance, Improve Cybersecurity, Monitoring, Systematic Literature Review.

1 Introduction

ISO 27005:2018 specifies four stages for managing cybersecurity risks. These stages are: 1) setting the context, 2) risk assessment, 3) risk treatment, and 4) risk monitoring and review. The name of these four (4) stages may change depending on the model frameworks, standards, and methodologies. In any case, the monitoring and review stage usually closes the cybersecurity risk management process.

Cybersecurity risk monitoring and review stage includes regular monitoring of risks and countermeasures defined in the risk assessment and treatment stages. In addition, timely reviews (audits) are necessary for proper monitoring to validate the effectiveness of countermeasures in addressing risks [1]. This study will focus on the problems related to cybersecurity risk audits, which are part of the cybersecurity risk monitoring and review stage.

Cybersecurity risk audit involves the periodic review of security controls to identify weaknesses where controls were not adequately designed or functioning as intended. The cybersecurity risk audit, in turn, is divided into two types, internal and external, as are other types of audits. The internal audit is characterized by the fact that it is carried out by personnel internal to the organization, evaluating the countermeasures implemented by the organization. On the other hand, the external audit is carried out by personnel from outside the organization, aiming to make the review more objective than an internal audit [2]. Cybersecurity risk audits may include IT applications, IT operations, governance, and personnel: all of which are specific areas of information systems implementation.

The study published by the European Confederation of Institutes of Internal Auditors (ECIIA) [3] highlights the importance of cybersecurity risk audits and mentions that it is the primary concern of Chief Audit Executives (CAE). Furthermore, authors such as Slapničar et al. [1] and Duncan and Whittington [4] consider cybersecurity risk audit to be a relatively young field. Cybersecurity risk audit has not yet reached an acceptable level of maturity. This lack of maturity is understandable when compared to accounting audit, which has been practiced for decades, and its level of maturity is acceptable. Authors such as Duncan and Whittington believe that much more clarity is needed on the concepts, procedures, and pieces of evidence needed to validate the correct functioning of a countermeasure.

The main issues that organizations face when conducting cybersecurity risk audits are as follows:

a) the complexities of cybersecurity risks. These complexities can be a challenge to performing cybersecurity risk audits.

b) organizations may have few internal professionals who are clear about the objectives of a cybersecurity risk audit. Many organizations require the assistance of qualified external experts to help them make strategic decisions to conduct cybersecurity risk audits [5].

The cybersecurity risk auditor faces the challenge of keeping up with a rapidly changing business and technology environment [6]. The automation of organizational processes and the increased scope of cybersecurity risks present new challenges in setting and achieving objectives in cybersecurity audits [4].

Due to the auditor's lack of clarity and precision of cybersecurity risk audit concepts and objectives [7], the auditor has limited understanding and control in the execution of cybersecurity risk audits. This lack of expertise may have created an expectation gap regarding the auditor's ability and responsibility to generate confidence. The lack of confidence creates ambiguity concerning what auditors can take responsibility for and what is expected from companies. This ambiguity is due to the lack of concept standardization and a lack of definition of cybersecurity risk audit objectives [8]. Some authors, such as Kotb et al. [6] and Turetken et al. [9], consider that there is no agreement on the definition or evaluation of the effectiveness of the cybersecurity risk audit. This lack of definition is primarily due to organizations being confused or unaware of the objectives related to cybersecurity risk audits.

On the other hand, another challenge for organizations is the difficulty in adhering to a cybersecurity risk audit standard or guideline. According to Sabillon et al. [10], there needs to be a clear guideline or consensus on what areas, sub-areas, domains, or sub-domains should be included in a cybersecurity risk audit. One example of the difficulties of current cybersecurity risk audit standards is the study published by Gauthier & Brender [11]. This study identified a need for efforts to address the development of specific audit standards related to cybersecurity. The results of this study show that auditors believe that the current audit standards for cybersecurity risk audits are too vague and need more guidance in cybersecurity risk audits. Another example is the Commonwealth of Virginia's cybersecurity program [12], where it was revealed that 84% of Virginia agencies that submitted audit findings did not follow audit standards or guidance.

The purpose of this research work is summarized in the following objectives:

a) identify the main objectives of cybersecurity risk audits, and

b) identify and analyze cybersecurity risk audit guidelines.

A Systematic Literature Review (SLR) using as a guide Kitchenham et al. [13] technique was conducted to achieve the above research objectives.

The contributions of this research work will be:

1) Establish common objectives applicable to cybersecurity risk audits.

2) Discuss the contributions and benefits of cybersecurity risk audit guidelines.

This research paper is organized as follows: Section 2 presents the background of cybersecurity risk audits; Section 3 presents the details of the systematic review process; Section 4 analyses and interprets the results of the systematic literature review; and finally, Section 5 presents the conclusions.

2 Background

Turetken et al. [9] mention that the literature has not yet converged on a set of indicators to quantify the effectiveness of internal audits. When discussing cybersecurity risk audits, the concepts of traditional audits should be taken as a reference and extended upon [9].

Currently, organizations conduct cybersecurity risk audits by measuring the effectiveness of countermeasures. Organizations use objective indicators to measure countermeasures. The internal audit evaluates the company´s internal control based on the analysis of risks within the organization, representing real support for the company's management. An internal audit aims to provide advice and objective assurance on the effectiveness of the internal management control system by giving recommendations that ensure and contribute to improving the organization’s activity. The “risk” is a component that is found in the management of an organization in terms of identifying it everywhere in the economic and financial life [14], [15].

The cybersecurity guidelines provide recommended actions or suggestions for managing cybersecurity policies. While cybersecurity guidance is not mandatory, there are no disciplinary consequences for not adopting them. Nonetheless, cybersecurity guidance is widely regarded as best practice and should be implemented. These guidelines typically employ terms such as "must" or "may" in their definitions and are usually tailored for specific environments to guide user actions [16].

Megan et al. [17] compile data from studies related to cybersecurity risk audits. As a result, Megan et al. [17] mention that organizations are making significant efforts, especially in developing countries, to enhance the execution of cybersecurity risk audits. Organizations that have already experienced cybersecurity issues due to a lack of cybersecurity risk audits have worked on improving the competence of internal audit committees and implementing practical guidelines within the organization, defining clear objectives [17].

To be practical, objectives related to cybersecurity risk audit must be viewed from an internal control view [10]. Some research studies (e.g., [18]; [19]) have analysed the role of internal audit in cybersecurity risk management and governance.

Current efforts to address cybersecurity risk audits are reflected in the current guidelines used for cybersecurity risk audits, such as ISO 27000 family [20], NIST CSF [21], and COBIT [22]. In order to implement these guidelines, it is necessary to transfer certain concepts to the field of internal control to address cybersecurity comprehensively[23].

According to Ezzamouri & Hulstijn [24], a cybersecurity risks audit with an appropriate guideline allows auditors to provide assurance on the criticality and impact of a risk. This assurance will depend on the effectiveness of the countermeasures implemented and will be captured in an audit report. Ongoing monitoring is usually the responsibility of management, as it affects the internal controls embedded in the company's technological processes.

The cybersecurity risk audit has not been able to fulfill its expected positive contribution to businesses and organizations. Challenges such as massive IT investments, rapid technological change, increased data volumes, and other issues in IT implementation have hindered the effectiveness of cybersecurity risk audits. Traditional IT audit practices are no longer sufficient to provide businesses adequate insurance [25]. Additionally, the complex nature of multidimensional cybersecurity risk audits and frequent errors in considering the necessary audit framework present obstacles to conducting effective cybersecurity risk audits [26].

Aditya et al.[25] have conducted an SLR on cybersecurity risk audits. These authors conclude that, until 2021, the existing cybersecurity risk audit guidelines are not applicable to modern organizations. The existing cybersecurity risk audit guidelines are complex, overlapping, and difficult to implement. Additionally, cybersecurity risk audit guidelines such as ISO 27002, COSO, and COBIT are too extensive to be managed and do not align with the risk-based cybersecurity risk audit approach. In other words, the traditional cybersecurity risk audit guidelines may no longer be applicable to the current business environment.

In conclusion, the SLR of Aditya et al. [25] presents the definition of audit objectives and the guidelines related to technology audits as two main issues of the last ten years. Most research and contributions to audits have not been directly linked to cybersecurity risk audits. Aditya also mentions that organizations will have more significant concerns as IT environments become increasingly complex. Greater complexity means that more practices for cybersecurity risk audit must be considered. Likewise, the audit of cybersecurity risks is a topic that has been investigated for a few years, so it has not yet been possible to define it with a high level of depth.

The objectives proposed for the SLR of this research work seek to establish a state-of-the-art on what is mentioned in the bibliography on cybersecurity risk audit. Subsequently, it seeks to identify common points to establish a common criterion and a standard definition of the audit of cybersecurity risks.

3 Systematic Literature Review

The methodology proposed by B. Kitchenham was selected to perform this Systematic Literature Review (SLR) [13]. SLR is a formal and verifiable process that the researcher performs to document the state of knowledge on a particular topic. According to B. Kitchenham, a systematic review evaluates and interprets all available research relevant to a given research question in the topic area or phenomenon of interest [27]. This SLR includes the following steps: (1) Propose a review protocol and define the research questions (Section 3.1), (2) Conduct the review (identify primary studies and evaluate these studies) (Section 3.2), (3) Extract the results (Section 3.3), and (4) Discuss and analyze the results of the systematic literature review (Section 4).

3.1 Propose a review protocol and define the research questions.

It is necessary to define a set of questions called “research questions” to achieve the main objectives of the SLR. To achieve the objectives “a)” and “b)” of this research work (presented at the end of section 1), the following research questions were created:

**Research Question 1 (RQ1):** What objectives are used in cybersecurity risk audits according to the literature?

When answering RQ1, the literature’s main objectives about cybersecurity risk audits will be identified. According to their focus (internal audit, information security, or cybersecurity), they will also be classified to identify the universe of those applicable to cybersecurity. The RQ1 was created according to objective a) identify the main objectives of cybersecurity risk audits.

**Research Question 2 (RQ2):** What are the most used guidelines in the literature on cybersecurity risk audits and their characteristics?

The objective of RQ2 is to identify guidelines, standards, frameworks, or models related to cybersecurity risk audits. It also aims to identify trends or gaps in the guidelines and standards. RQ2 was created based on objective b) identify and analyze cybersecurity risk audit guidelines.

3.1.1 PICO protocol

The PICO (population, intervention, comparison, and outcome) protocol established in B. Kitchenham's model, which has been widely used and extensively tested in the execution of systematic literature reviews, was chosen for implementation in our study.

* **Population:** Publications related to the objectives of cybersecurity risk audits. Additionally, guidelines related to cybersecurity risk audits are also considered.
* **Intervention:** Research studies mention different objectives and guidelines related to cybersecurity risk audits.
* **Comparison:** Identify and compare objectives and guidelines related to cyber security risk audits mentioned by publications.
* **Outcome:** Objectives of cybersecurity risk audits, frequency, and approach of cybersecurity risk audit guidelines.

3.1.2 Research string generation

A set of keywords has been selected to obtain the highest results. Synonyms for the keywords have been included to avoid excluding relevant studies and to build the search string efficiently. The synonyms used, as well as the keywords, are shown in Table 1.

**Table 1.** Keywords and synonyms for building the research strings.

|  |  |
| --- | --- |
| Keyword | Synonyms |
| Cybersecurity | Cyber security, Information security |
| Audit | Assurance, Guide, Law, Standard |

The search strings have been built with the keywords and synonyms from Table 1. The logical connectors “AND” and “OR” were added to join the keywords and synonyms, constructing the following generic search string: ("Audit" OR "Assurance" OR "Guide OR "Law" OR "Standard") AND ("Cybersecurity" OR "Cyber Security" OR "Information Security").

The sources were searched following the criteria defined for their selection (see section 3.2).

3.2 Conduct the review

The criteria for the selection of sources (databases) were based on: a) the experience reported by Dyba et al. [28], and Petersen et al. [29]; b) the availability of full-text studies found through the search strings; c) studies available on the web for free; and d) specialized cybersecurity magazines that are available in the library of the Universidad Politécnica de Madrid. The sources selected for this SLR are 1) ACM Digital Library, 2) IEEE Digital Library, 3) ISI Web of Science, 4) ScienceDirect, 5) Scopus, and 6) Springer Link. Google Scholar was selected only for applying the snowball technique.

The search string defined in the previous section was entered into the search engines of the sources.

3.2.1 Inclusion and exclusion criteria

Inclusion and exclusion (I&E) criteria must be defined to select the studies related to the SLR. The I&E criteria were defined according to the experience of Kitchenham et al. [13], and Petersen et al. [29]. The selection of studies has been conducted using the following I&E criteria.

Inclusion criteria:

* **Accurate digital libraries**: We assessed the quality, quantity, and reliability of published studies from seven digital libraries (chosen from the criteria for selecting the sources).
* **Content of the studies**: It was realized that the main topic of the identified studies was related to the research questions RQ1 and RQ2. For this analysis, the title, the abstract, and the keywords of the studies were validated.
* **Consistency of the study**: It was confirmed that the studies were related to the field of cybersecurity. To this end, the field and the title of the studies were identified, ensuring that they were consistent with the objectives of the SLR.
* **Full-text studies**: All studies identified in the Digital Libraries were reviewed, validating the completeness of the information. In this way, only complete studies were included.

Exclusion criteria:

* **Duplicate studies**: Duplicate studies were removed from the various Digital Libraries. This exclusion criterion aims to reduce the volume of unnecessary information.
* **Studies based only on a particular opinion**: Studies that only mention a particular opinion were excluded. This exclusion criterion aims to have studies based on validated scientific hypotheses.
* **Studies before 2012**: Due to the continuous updating of the cybersecurity field, studies before 2012 were excluded. Therefore, information from a study before 2012 would be considered irrelevant to this SLR.
* **Studies that are irrelevant to the research questions or unrelated to the topic**: Studies unrelated to any of the research question RQ1 and RQ2 were also excluded.
* **Unclear or ambiguous studies**: Studies that did not clarify their contributions or did not clarify their relationship to cybersecurity were discarded.
* **Studies that mention risk audit but not in the cybersecurity field**: Studies that mentioned audit guidelines related to areas other than cybersecurity were discarded.
* **Gray literature, or literature published by non-traditional publishers**: This type of literature was excluded.

3.2.2 Selection of primary studies

The selection of primary studies has been divided into a three-activity procedure. A dataset was created to perform these activities (see https://short.upm.es/xljfp). This dataset contains the results of the three activities.

In the first activity, we inserted the search string created in the review protocol into the database’s search engines. After the first activity, 2,032 studies were found. The results are presented in Table 2.

**Table 2** Distribution of studies by source.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Source | Initial studies (First activity) | Relevant studies (Second activity) | Primary studies Task 1 (Third activity) | Primary studies-Task 2 (Third activity) |
| ACM Digital Library (ACM) | 464 | 12 | 4 | 4 |
| IEEE Digital Library (IEEE) | 107 | 24 | 7 | 7 |
| ISI Web of Science (WOS) | 61 | 9 | 2 | 2 |
| Springer Link (SP) | 1015 | 33 | 3 | 3 |
| Science Direct (SD) | 53 | 1 | 0 | 0 |
| Scopus (SC) | 332 | 13 | 4 | 4 |
| Google Scholar (GS) | 0 | 0 | 0 | 3 |
| Total | 2032 | 92 | 20 | 23 |

Then, exclusion criteria were applied in the second activity (I & E criteria), reading the title, abstract, and keywords. We found and excluded 63 duplicate studies. After using the I & E criteria, 1,877 additional studies were excluded because they were irrelevant to answering the research questions. A total of 92 publications were considered relevant. All results are shown in the SLR process dataset (see https://short.upm.es/xljfp for more information).

In the third activity, we selected the studies based on the following:

• Task 1, reading the full text. If the study provides enough information, then it is selected and saved.

• Task 2, an additional search using the snowballing technique described by C. Wohlin [30] is applied. As a result, two additional studies were added.

After applying the third activity, we refused 72 studies and accepted three studies from internet browsers to obtain 23 accepted studies after the third activity.

3.3 Extract the results

In this section, a template was designed to gather the relevant information from each study. The template includes the following fields: (1) ID (identifier) of the study, (2) bibliography (title, author, year), (3) type of study (case study, survey, experiment, research), (4) objective of the study, (5) context in which the study is conducted (Solution proposals, Evaluation searches, Opinion articles, Experience articles, Philosophical articles), (6) type of study (improvement, deployment, or both), (7) Objectives of cybersecurity risk audits identified in each study, and (8) guidelines for cybersecurity risk audits (for more information, see https://short.upm.es/om6jj).

After reading the complete text, the relevant information was analyzed for each selected study to characterize the results (see section 4).

4 Results, Analysis, and Interpretation of the Results

The results were summarized and analyzed at the end of the systematic literature review. In summary, the studies were classified into studies related to the two objectives of the research work: (a) identify the main objectives of cybersecurity risk audits, and (b) consolidate and synthesize knowledge on cybersecurity risk audit guidelines. The analysis determined the frequency with which cybersecurity risk audit guidelines are named. The support document for the analysis of the results can be consulted at the following link https://short.upm.es/e0z1g.

**4.1 Report of the results of the systematic review**

Within this activity of the SLR, the results of the systematic literature review are presented, both the information from the primary studies, and the results related to the research questions RQ1, RQ2.

4.1.1 Information about objectives

As part of this SLR, the objectives related to cybersecurity risk audits were extracted from the primary studies. The purpose of extracting this information is to answer the research question RQ1 proposed in section 1 "Introduction". This information can also be used to build relationships among the concepts to help consolidate a state-of-the-art of the objectives of cybersecurity risk audits.

In primary research studies, when authors discuss the goals of cybersecurity risk audits, they frequently mention concepts such as evaluation, assurance, compliance, and security. Based on their background or professional context, individuals engaged in risk management might interpret these terms in various ways. These four terms are unclear and distinct for organizations and employees involved in management systems. Because of this lack of clarity, these four objectives are often used in different ways and approaches. Adapting the objectives defined by the authors and complementing them with the cybersecurity approach mentioned by Duncan et al [4] in the field of cybersecurity, the objectives of a cybersecurity risk audit can be defined as follows:

* Evaluation: “To make an official systematic examination of something in order to check its accuracy.”
* Assurance: “Promise or commitment that makes a thing certain; a formal undertaking guarantee; a positive statement intended to give confidence.”
* Compliance "The action or the fact of complying with a desire or mandate" requires a code or set of standards against which the activities and processes of the company can be compared, comply) or not comply."
* Cybersecurity improving: “Prevention of damage, protection and recovery of computers, electronic communications systems, electronic communications services, cable communications and electronic communications, including the information contained in them, to guarantee their availability, integrity, authentication, confidentiality, and non-disclosure repudiation” [20].

The authors agree that an audit is a tool whose objectives are to evaluate, ensure, comply with, and improve cybersecurity. Consequently, an audit that achieves these four objectives would constitute a cybersecurity risk audit.

An in-depth reading of primary studies was conducted to validate the objectives outlined by the literature on cybersecurity risk audits. As a result, the following relevant objectives shown in Table 3 were identified.

**Table 3.** Relevant concepts in primary studies

|  |  |  |
| --- | --- | --- |
| Study ID | Objectives | Year |
| ACM1 [4] | Assurance, Compliance, Evaluation | 2014 |
| ACM2 [31] | Evaluation, Cybersecurity improving | 2018 |
| ACM3 [32] | Assurance, Cybersecurity improving | 2013 |
| ACM4 [33] | Evaluation, Cybersecurity improving | 2019 |
| SP1 [34] | Evaluation, Cybersecurity improving | 2013 |
| SP2 [35] | Evaluation, Cybersecurity improving | 2022 |
| SP3 [36] | Compliance, Cybersecurity improving | 2018 |
| WOS1 [37] | Evaluation | 2012 |
| WOS2 [38] | Evaluation | 2019 |
| SC1 [39] | Compliance, Evaluation, Cybersecurity improving | 2021 |
| SC2 [40] | Evaluation | 2021 |
| SC3 [41] | Compliance, Evaluation | 2021 |
| SC4 [42] | Assurance, Compliance | 2018 |
|  |  |  |
| IEEE1 [43] | Evaluation | 2022 |
| IEEE2 [44] | Evaluation | 2016 |
| IEEE3 [45] | Evaluation, Cybersecurity improving | 2017 |
| IEEE4 [46] | Cybersecurity improving | 2020 |
| IEEE5 [47] | Assurance | 2014 |
| IEEE6 [48] | Compliance, Evaluation | 2014 |
| IEEE7 [49] | Assurance | 2022 |
| GS1 [10] | Evaluation | 2018 |
| GS2 [25] | Evaluation | 2018 |
| GS3 [50] | Evaluation | 2019 |
|  |  |  |

* **Evaluation**: According to the authors, this is the primary purpose of the cybersecurity risk audit. This objective satisfies the need to measure current advances in cybersecurity risk audit. Moreover, the authors directly associate this objective with the concept of audit.

The following studies have explored cybersecurity risk assessment via audits: ACM1, ACM2, ACM4, SP1, SP2, WOS1, WOS2, SC1, SC2, SC3, IEEE1, IEEE2, IEEE3, IEEE6, GS1, GS2, and GS3. In the ACM1 and SP2 studies, the audit is recognized as a fundamental component of assessments (evaluation) and assurance pillars within a management system. Similarly, the ACM2 study specifically delves into cybersecurity risk audits through the lens of mobile application audits. In contrast, the remaining studies utilize easily traceable activities that ensure straightforward assessment procedures.

The authors of ACM4 and SP1 highlighted the use of audits to assess the effectiveness of countermeasures within a management system. At the operational level of business processes, the research in WOS 1 underscores the importance of the system audit procedure. In contrast, the WOS2 study characterizes audits as obligatory examinations carried out by both internal and external organizations to uphold the confidentiality of information.

The GS1 study presents an all-encompassing cybersecurity audit methodology spanning 18 domains applicable to companies of all kinds. Over the last decade, research conducted in the GS2 study has highlighted IT audit benefits, IT audit orientation, and IT audit objectives as the most prominent subjects within the audit domain. Furthermore, as indicated by the GS3 study, proficient management and execution of robust cybersecurity audits play a pivotal role in enhancing a business's cybersecurity operations. These audits safeguard the organization's assets from potential harm and destruction by pinpointing and mitigating cyberattacks and threats.

* **Compliance**: This objective relates to internal and external standards and norms. Compliance with standards is a crucial component in evaluating and monitoring cybersecurity threats. Some authors use regulatory requirements as a benchmark to determine the minimal efficacy of a cybersecurity management system.

Similar to cybersecurity, information security aims to ensure the essential attributes of confidentiality, availability, and integrity of information (referred to as CIA). These attributes hold significance in the subsequent analysis and examination of studies such as AMCM2, SP2, SC1, and IEEE1. In the context of the ACM2 study, the CIA attributes are foundational in the development of mobile applications. Conversely, the SP2 investigation highlights the CIA as a compulsory requirement specified by Norwegian regulations for critical infrastructures. Meanwhile, the SC1 study takes a distinct approach by emphasizing the CIA as a pivotal concept for evaluating management systems based on the NIST 800-37 model. Lastly, the IEEE1 study emphasizes the confidentiality attribute within the CIA framework and categorizes data according to privacy considerations.

ACM1, SP3, SC1, SC3, SC4, and IEEE6 are studies that delve into compliance, including regulations and their significance. In ACM1, there is an emphasis on the imperative of conforming to both international and local standards. In contrast, SP3's exploration centers on the strategic edge attained by companies that align themselves with global frameworks like the NIST CSF.

The SC1 study asserts that substantiating compliance with an information system could involve presenting evidence like sample audit records or system settings tailored for audits (like configurations for error logs and activity logs within an information system). In the case of SC3, the study pinpoints internal audit as a control encompassing four sub-controls: forensic investigation, formal risk acceptance, cybersecurity compliance, and internal control testing.

According to the SC4 study, the effectiveness of an audit should not be confined solely to assessing compliance with cyber-related policies and processes.

* **Assurance**: The assurance objective aims to ensure the fulfillment of predetermined objectives while implementing a cybersecurity management system. Several mechanisms can provide this assurance, including audits, adherence to standards, alignment with frameworks, and alignment with internal policies and procedures. Moreover, assurance extends to the organization's cybersecurity program and encompasses incident response procedures, business continuity, and disaster recovery efforts. Additionally, the management and audit committee should receive a comprehensive report detailing the cybersecurity-related findings from the engagement.

The significance of the relationship with local or international standards constitutes a crucial third element. Within cybersecurity risk auditing, the authors underline the necessity for a structured framework. This necessity explains why a requirements framework often finds its foundation in local or international standards and best practices.

Among the studies, ACM1, ACM3, ACM4, SP1, SP2, WOS2, SC1, SC2, SC3, SC4, IEEE3, IEEE6, and GS1 shed light on the interplay between monitoring, review, and standards. The GS2 and GS3 studies utilize risk management norms and standards to dissect IT and information security audits. They also converge to address cyber threats through cybersecurity audits.

ACM1 enumerates organizations such as NIST, ISO, ENISA, and ITU, responsible for shaping appropriate cybersecurity rules and standards. On the contrary, studies such as ACM3, SP1, SP2, SP3, and WOS2 point to cybersecurity rules and standards such as COBIT, which are not designed exclusively for cyber security, as a guide for security risk audits.

ACM4 highlights Ecuador's need to establish a regulatory framework for cybersecurity risk audits. Regarding assessment, SC1 primarily leans on NIST 800-37, while SP2, SP3, and SP4 refer to COBIT 5 as their guiding framework. Additionally, SP3 incorporates ISO 27001 and other standards. SP4 introduces internal control within the scope of evaluating and overseeing a management system.

ACM1, ACM3, SC4, IEEE5, and IEEE7 stand out as studies delving ensuring relevance. In both ACM1 and ACM3, assurance is explored as the process of shaping and overseeing institutional objectives. These studies showcase a robust connection between evaluation, compliance, and the enhancement of cybersecurity.

As outlined in the SC4 study, numerous procedures and operations currently contribute to assuring cybersecurity and deterring attacks. These encompass risk assessment, risk treatment, risk management, security assurance, and auditing. The Information Security Assurance Model (ISAM) is grounded in information security principles and best practices aimed at governing and enhancing the security of the exam preparation process. Additionally, the IEEE7 study affirms that security standards have consistently been regarded as a practical approach for delivering cyber assurance, albeit encountering hurdles in their widespread adoption.

**Cybersecurity improvement**: This objective aims to pinpoint potential vulnerabilities within the cybersecurity management system and extract lessons from them. The authors argue that recognizing these weaknesses or areas for enhancement facilitates the implementation of corrective measures to bolster cybersecurity effectively. This objective is explored in the following studies: ACM 2, ACM 3, ACM 4, SP1, SP2, SP3, SC1, IEEE3, and IEEE4.

The following studies - ACM2, ACM3, ACM4, SP1, SP2, SP3, SC1, SC2, IEEE2, IEEE3, IEEE4, GS1, and GS3 - explicitly delve into the realm of cybersecurity within the broader context of information security. This explicit focus aims to contribute to the cybersecurity risk audit. GS1 and GS2 discuss the limitations and gaps in cybersecurity controls that hinder comprehensive cybersecurity audits or domain-specific cybersecurity audits.

Within this landscape, the SC3 study introduces a cybersecurity framework designed to guide organizations through the process of conducting cybersecurity audits. On the other hand, the SC4 study scrutinizes methodologies for cybersecurity assurance, shedding light on critical issues and weaknesses from the perspectives of internal audit and risk management.

The IEEE6 and IEEE7 studies take on the task of addressing cybersecurity factors for compliance with standards like PCI DSS 3.0 and cybersecurity regulations compliance standards. In particular, encryption surfaces are mentioned in studies as ACM2 as a solution to mitigate the risks associated with gross force and network attacks..

Technical domains connected to cybersecurity, including operating system security, are discussed in the ACM3 study. In contrast, ACM4 views cybersecurity as an integral part of the ongoing systems improvement process.

The SP1 study examines the interrelationships between conventional security measures and cybersecurity by analyzing system access policies.. Conversely, SP2 portrays cybersecurity as a critical component within Norway’s broader security framework for critical infrastructure. Simultaneously, the SP3 study underscores the importance of adhering to norms and standards to ensure the effective implementation of a cybersecurity management system.

According to the ACM2 study, automating the audit process for mobile applications makes it easier for an organization to strengthen its cybersecurity. In contrast, ACM3 and ACM4 describe the enhancement of cybersecurity due to continuous management system reviews. SP1, SP2, and SP3 indicate that cybersecurity improvement is due to adopting specific countermeasures or coupling with national or international laws, standards, and frameworks.

In additive manufacturing (AM), the SC1 paper underscores the importance of leveraging cybersecurity frameworks like the NIST Risk Management Framework (RMF) within the AM community. This serves to mitigate the potential impact of future IT cybersecurity risks on the AM industry.

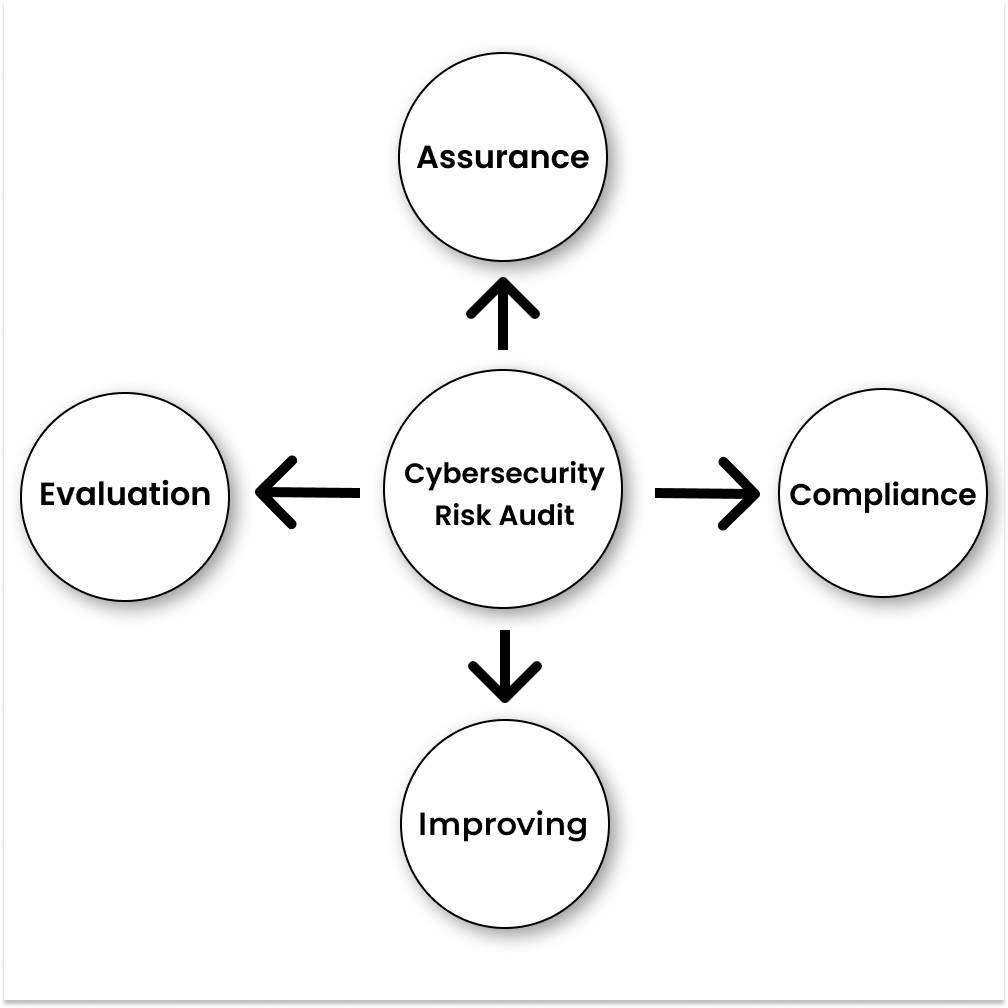
The IEEE3 study focuses on the oil and gas industry. The study shows how auditing techniques based on modern standards such as ISO are used for business risk management in the oil and gas sector.

In the financial realm, the IEEE4 study emphasizes the need for an integrated management system based on well-established ISO standards when developing an information security management system (ISMS) for a financial institution.

**Highlights of section 4.1.1**

When analyzing the primary studies, we identified that they could be classified according to the objectives the cybersecurity risk audit must meet. For The relationship between the objectives, it is worth classifying the concepts and objectives into four main objectives, taking as a reference the work of Duncan et al. [4].

This work found that the four objectives of cybersecurity risk auditing are closely related because the cybersecurity risk audit process must be improved in addition to performing an assessment, measuring compliance, and validating assurance.



**Fig. 1** Objectives of the cybersecurity risk audit.

By analyzing the four objectives of the cybersecurity risk audit, we determined that they are interrelated (see Fig. 1). For example, the objective of an audit is to conduct a review to ensure the effectiveness of a management system. In addition, according to the Oxford English Dictionary, an audit is "an official examination of the quality or standard of something," so an audit can be related to both assurance and compliance with a standard or regulation. The final objective of a cybersecurity management system audit is to improve the current state of cybersecurity.

Summarizing the results of this section, within the concepts related to cybersecurity focused on conducting risk audits, it was identified that the authors mention the objectives "Evaluation," "Assurance," "Compliance," and "Improve Cybersecurity.” These objectives are interrelated as they are the fundamental pillars of cybersecurity risk audits.

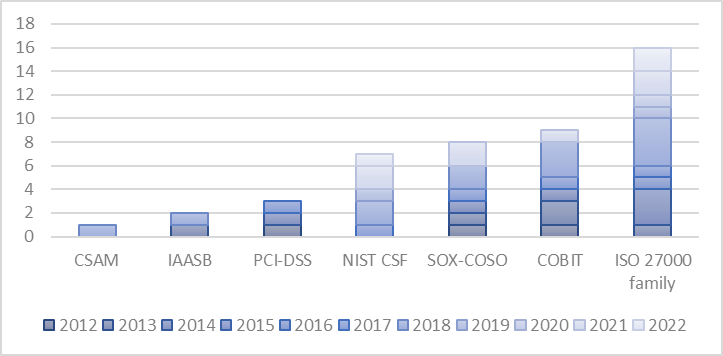
4.1.2 Information on cybersecurity risk audit guidelines and standards.

, The cybersecurity risk audit guidelines mentioned by the primary studies were inquired about (see Table 4 to answer the research question RQ2 established in section 1.

**Table 4.** Identified cybersecurity audit guidelines.

|  |  |
| --- | --- |
| Guidelines | References |
| ISO ([International Organization for Standardization](https://www.iso.org/), 27000 - 31000) | [4], [34], [35], [36], [39], [41], [42], [43], [44], [45], [46], [47], [48], [10], [25], [50] |
| COBIT (Control Objectives for Information and related Technology) | [4], [34], [36], [37], [40], [41], [42], [10], [25] |
| SOX Act - COSO (Sarbanes Oxley) | [4], [32], [34], [36], [37], [40], [10], [25] |
| NIST CSF (National Institute of Standards and Technology- Cybersecurity Framework) | [35], [36], [39], [41], [42], [10], [50] |
| IAABS (International Auditing and Assurance Standards Board) | [34], [36] |
| PCI-DSS (Payment Card Industry Data Security Standard) | [37], [48], [10] |
| CSAM (A Comprehensive Cybersecurity Audit Model) | [10] |

Fig. 2 shows the frequency of appointments of cybersecurity audit guidelines per year. According to data, the ISO 27000 family is the most extensively used from selected research studies because it encompasses various areas of industry, not just cybersecurity..



**Fig. 2** Frequency of the name of the Cybersecurity Audit Guidelines identified by year.

The principal guidelines for cybersecurity risk audit in primary studies are described below:

**“ISO 27000”:** The family of International Organization for Standardization standards is a family of information security standards. This family of cybersecurity risk audit standards is mentioned by authors like Hagen & Toftegaard [35]. ISO 27004 is a security audit-specific ISO standard. The ISO 27004 standard is a starting point for authors such as Steinbart et al. [18] when addressing cybersecurity. ISO 27004 is a technical and process-oriented standard. In addition, its goals include review, assurance, and enhancement of security. In the systematic review, 16 of 23 studies cite the 27000 family standards as important guidelines for monitoring and analyzing cybersecurity threats. The interoperability of the 27000 family with other standards or norms, such as NIST or ISO 31000, is an additional benefit.

**“SOX/COSO”:** SOX is a United States federal Act drawn on internal control principles established by the Committee of Sponsoring Organizations of the Treadway (COSO). These instructions are based on internal control rather than cybersecurity since the scope of internal control encompasses all areas of operations and management. SOX/COSO is frequently used to assess technological controls' compliance. COSO has five key principles: 1) Governance and culture, 2) Strategy and objective formulation, 3) Performance, 4) Review and monitoring, and 5) Information, communication, and reporting. Internal control and financial audit references include the SOX regulation and the COSO internal control framework, according to authors such as Duncan et al. [4] and Hoag J. [32]. The authors employ these audits and their principles to conduct cybersecurity-focused audits. In addition, the SOX Act and the COSO give criteria for establishing an organizational control environment, including top management. SOX and COSO are used for their characteristics as guidelines for the strategic level of an organization. SOX/evaluation COSO's and monitoring objectives include evaluation, assurance, and compliance.

**“NIST CSF”**: The NIST Cybersecurity Framework, released in 2018, is a cybersecurity-focused reference. It comprises CORE, TIERS, and PROFILES that assist in evaluating the organization's level of cybersecurity management and set attainable targets for the short and medium term. Five functions comprise the CORE of the framework: "Identify," "Protect," "Detect," "Respond," and "Recover." Also included are 23 categories and 108 specific subcategories. The NIST CSF is an established framework that facilitates comparison-based evaluation. As one of the first assessment frameworks specifically focused on cybersecurity, authors like Sabillon et al. [10] and Ibrahim et al. [36] use it as a starting point for technical and process evaluations. The objectives of the NIST CSF cybersecurity risk audit are to evaluate and enhance cybersecurity.

**“IAASB”:** International Audit and Assurance Standards Board is responsible for publishing International Audit Standards (ISA). The audit standards used in the European Union and other nations do not adhere to the SOX Act. The ISA standards stipulate a three-step audit procedure delineated by three distinct criteria Planning, Execution, and Reporting. Authors such as Burgemeestre et al. [34] highlight these recommendations, together with COSO and SOX, to handle technology, security, and cybersecurity evaluations beginning with internal control. The ISA standards emphasize the strategic and operational levels. The IAASB audit standards include three objectives: evaluation, assurance, and compliance.

**“COBIT 5”:** "Control Objectives for Information and Related Technology" is a best practices manual defining IT risk as an enterprise risk. In particular, the business risk associated with an enterprise's usage, ownership, operation, participation, impact, and adoption of IT. This manual of best practices is utilized by authors such as Matari et al. [41] to validate compliance with the objectives of an organization's deployed countermeasures. COBIT is a guideline designed for strategic-level information technology that aims to guarantee and assess.

**“PCI-DSS”:** The Payment Card Industry Data Security Standard can be used to monitor and review a management system. The PCI-DSS is utilized by authors such as Steinbart et al. for conducting compliance evaluations. The PCI-DSS is required for all enterprises that provide regulated financial and banking services. Due to this requirement, the PCI-DSS is frequently used as a guideline to conduct compliance reviews using a process and technical approach. PCI-DSS monitoring, and compliance aims to ensure, comply with, and enhance security.

**“CSAM”**: CSAM is a model proposed by the Universitat Oberta de Catalunya. The model is intended for conducting cybersecurity audits in any organization or country to assess security, maturity, and preparedness against cyber threats. The CSAM model is based on frameworks such as NIST CSF, MITRE, and PCI-DSS. The Cybersecurity Audit Model (CSAM) includes general information, resources, and 18 domains. Certain domains have specific sub-domains where controls are evaluated. Then the checklists verify compliance with specific sub-controls based on domain/sub-domain. The scorecard findings determine the domain rating and score, yielding the overall cybersecurity maturity grade.

Only the NIST CSF and CSAM [10] were designed for cybersecurity risk and their use within any enterprise, although their level of execution is quite tricky. Other standards, such as ISO 27004 of the ISO 27000 family, emphasize information security. In addition, PCI-DSS provides a specialized approach to information security for banking data. COBIT, on the other hand, emphasizes IT governance. Based on the COSO guidance and the International Standards on Audit (ISA) developed by the IAASB, the SOX regulation emphasizes on internal control that was not intended to address IT audit.

Many relevant audit guidelines specified in the primary studies approach countermeasures evaluation differently. Hagen and Toftegaard [35] classify audit guidelines based on their application focus. 1) The strategic level, 2) the technical level, and 3) the operational level. We could classify the guidelines based on this classification, information from the guidelines cited in the source studies, and consultation with the guidelines' original paperwork. We have established that: COBIT's IT governance strategy can be classified as belonging to the strategic layer. SOX-COSO and IAASB (ISA) emphasize internal control and corporate governance. On the other hand, the study by Hagen and Toftegaard also mentions the 27000 family and the NIST CSF as technical references. The operational layer could potentially be the subject of the ISO 27000 family, NIST CSF, PCI-DSS, COBIT, IAASB, and SOX-COSO standards.

There have been identified two distinct tendencies noticed in primary research. 1) The authors utilize audit guidelines centered on the strategy level without considering the technical component, and 2) the authors employ audit guidelines with a technical approach without considering the strategic approach. These two trends demonstrate the necessity of complementing each other equally to evaluate the cybersecurity management system objectively and practically.

Most of the guidelines’ authors needed to make modifications to analyze the specific cybersecurity countermeasures, including cybersecurity aspects within the audit plan and the findings. Therefore, there is a deficiency of guidelines tailored to the specific requirements of cybersecurity management systems. This deficit may be attributable to the complexity of establishing audit guidelines. Duncan & Whittington note that many years and efforts were required to adapt audit guidelines to information technology requirements. Consequently, more significant effort is required from all parties concerned for these to address cybersecurity requirements adequately.

**Highlights of section 4.1.2**

Summarizing the results of this section, the seven most widely used guidelines for cybersecurity risk audits were identified: 1) ISO 27000 family, 2) COBIT, 3) SOX-COSO, 4) NIST CSF, 5) PCI-DSS, 6) IAASB and 7) CSAM. Of the previously identified guidelines, only the NIST CSF and CSAM were explicitly created for cybersecurity. Additionally, according to the authors, the focus of the cybersecurity risk audit guides can be classified, whether they are focused on processes, technology, or at a strategic level.

One interesting observation is that two distinct tendencies have been identified in primary research. First, the authors utilize audit guidelines centered on the strategy level without considering the technical component, and finally, they employ audit guidelines with a technical approach without considering the strategic approach. These two trends demonstrate the necessity of complementing each other equally to evaluate the cybersecurity management system objectively and practically.

## Analyzing and interpreting the results of the systematic review

This section will analyze and interpret the results obtained by answering the research questions RQ1 and RQ2. For this, the most relevant mentioned in the primary studies on the points defined in section 4.1 will be recapitulated.

**4.2.1 Discussion of the results of RQ1.**

Relationship among evaluation, compliance, assurance, and improvement of cybersecurity: Among the 23 primary studies we examined, 17 explicitly underscore the significance of "Evaluation" as a core aspect of the audit process.

An illustrative case can be found in the ACM 2 study, which highlights the importance of auditing applications. This study introduces a model tailored for scrutinizing mobile application security. Here, the audit concept takes on a specific focus, emphasizing the objective of the application security audit: to dissect both the operation and documentation of software development, thereby validating its accurate functioning.

In contrast, the GS1 study puts forth a more comprehensive audit framework for cybersecurity. This model facilitates the assessment of cybersecurity within any organizational setting. Moreover, it holds the capability to verify specific guidelines for states or nations intending to implement a National Cybersecurity Strategy (NCS). Additionally, it can assess the effectiveness of pre-existing National Cybersecurity Strategies or Policies.

Beyond the core attributes - documentation and functionality - that necessitate scrutiny during a technology audit, it is also worth incorporating the ideas of the ACM3 study. ACM3 emphasizes the strategic perspective that audits should encompass. It delineates the necessary expertise and knowledge required for executing an IT audit with a cybersecurity focus.

In contrast to the traditional IT audit, the cybersecurity-centric IT audit must assess internal control mechanisms, which are outlined by standards like SEC, and adapt them to the realm of cybersecurity. An essential proposition made by this study is that an audit cannot occur without a benchmark for comparison. This benchmark can either be in the form of standards or norms. Consequently, this interplay gives rise to the fusion of audit and compliance - two concepts that, while distinct, are inherently interconnected. Together, they form the bedrock of monitoring and review activities.

WOS1 is a prime example of a study that establishes a connection between compliance and audit. This linkage extends to the realm of audits focused on IT and those centered on internal controls, as explored in the context of WOS1. The notion of assurance comes into play by emphasizing accounting audits as an integral component of internal control processes.

For clarity, the National Institute of Standards and Technology (NIST) defines assurance as "a measure of confidence that the security features, practices, procedures, and design of an information system conform precisely to its security policy."

The ACM1 and ACM2 studies underscore the close tie between assurance and achieving organizational objectives. Likewise, the SP3 study highlights the imperative of adhering to internal and external norms and regulations to ensure robust cybersecurity assurance. The organization's cybersecurity strategy plan serves as a guiding compass in this endeavor.

**4.2.2 Discussion of the results of RQ2.**

Based on the presented findings, it becomes evident that ISO 27000 stands out as the most frequently cited guideline. Its usage has remained remarkably consistent since 2017, except for a slight decline in 2020. While ISO 27032 is indeed linked to cybersecurity, it lacks a corresponding audit framework – a gap noted in the ISO 27000 standards mentioned above.

The GS1 paper, while introducing the CSAM cybersecurity audit paradigm, references the ISO 27000 family. Similarly, GS2 and GS3 underscore the pivotal role of IT audit in cybersecurity risk management by anchoring their discussions in ISO standards.

A cybersecurity framework proposed by SC3 for enterprise-level cybersecurity audits draws from the concepts embedded within ISO standards. Meanwhile, SC4 leverages information standards to implement internal security audit control processes.

Within the literature, publications like SC1, IEEE1, IEEE2, IEEE3, IEEE4, and IEEE6 utilize information security audit standards to develop audit methodologies, including management models and process standardization in alignment with industry best practices.

Further delving into specifics, the IEEE5 study meticulously outlines ISO standards tailored to mitigate risks determined by individual organizations.

COBIT serves as a foundational paradigm for auditing the management and governance of information and technology systems. Positioned as a strategic guideline tailored for information technologies, COBIT aims to ensure assurance and evaluation.

Within the GS1 study, the framework of COBIT finds its foothold as a reference for information technology control objectives, forming the underpinning of the CSAM cybersecurity audit model. Likewise, in the GS2 study, COBIT is harnessed to systematically evaluate IT audits and draw comparisons against other IT audit recommendations.

The SC2 study, on the other hand, suggests the presentation of a streamlined IT risk management maturity audit system rooted in the "COBIT 5 for Risk" framework. In the context of the SC3 study, a cybersecurity framework geared towards enterprise-level cybersecurity audit processes takes shape. The selection of COBIT as a reference in SC3 is justified by its holistic coverage of information and technology governance and management.

Stepping into SC4, the study leverages COBIT standards to cultivate information security internal audit control processes. This approach enables management to address control necessities, technological complexities, and business risks concurrently.

Across various other studies, such as ACM1, SP1, SP3, and WOS1, COBIT is mentioned as a cited resource. These studies use COBIT to shape concepts and amalgamate the objectives of information security or cybersecurity-focused audits.

The Sabarnes-Oxley Act serves as a reference for audit management due to its intent and breadth of coverage. As previously discussed, the computer audit uses accounting audit concepts as a guideline for its application and management to encompass the field of cybersecurity.

Due to technological advancements in recent years, the ACM3 study discusses the applicability of the SOX Act and COSO in technological audits. Other authors, including SP3 and WOS1, note that the COSO and SOX personnel and process dimension of must be adapted to the technology context. The SC2 and GS1 investigations highlight the importance of implementing SOX and COSO to ensure local and international legislation compliance.

In study SP1, the IAASB's worldwide audit standards are used to expand upon the principles of evaluating design and operational effectiveness of countermeasures. The SP3 study, on the other hand, emphasizes the necessity to align with IAASB norms to achieve the minimum criteria of local and international standards.

The studies GS1, WOS1, and IEEE6 present the Cybersecurity Audit Model (CSAM). SAM specifies that assigning the audit's scope is more straightforward if the target organization has implemented a specific cybersecurity framework or standard, such as PCI DSS. According to the WOS1 and IEEE6 studies, compliance with the PCI-DSS standard is necessary for all businesses that handle banking or credit card data, and it is highlighted that this data security standard of the payment card industry must be addressed in its early stages.

The Cyber Security Audit Model (CSAM) is a new exhaustive model that encloses the optimal assurance assessment of cybersecurity in any organization. The CSAM can be implemented to conduct internal or external cybersecurity audits. This model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls.

NIST CSF can implement the business cybersecurity framework in these five phases: identification, protection, detection, response, and recovery.

5 Conclusions

This paper has argued that an inadequate cybersecurity risk audit can make achieving the objectives established within a management system difficult.

This study has shown that the authors of the primary studies refer to the cybersecurity audit without addressing the associated concepts or minimum objectives. Furthermore, cybersecurity auditing is still in its infancy and has a way to go before reaching maturity. Since IT audits and, to a greater extent, cybersecurity lacks the strict supervision of accounting audits, the question of their effectiveness arises.

This study has found that, compliance, assurance, and auditing are generally different from cybersecurity. Due to the cost of hiring specialists, audit guideline implementers seek to control the problem by limiting compliance to a box-checking exercise, as the standards invariably lag the actual scenario.

As established in the introduction, the defined objectives that make up the cybersecurity risk audit were identified and characterized: "Evaluate," "Assurance," "Compliance," and "Cybersecurity Improvement." The objective of the evaluation is mentioned in 17 of the 23 audit studies.

The evidence from this study suggests that, as a result of the relationship identified between the objectives of the cybersecurity risk audit, it is considered that a new line of research could be developed to establish the feasibility of developing an audit guide covering the "Evaluate," "Assure," "Compliance," and "Improve Cyberspace Security" objectives."

Responding to the second proposed research objective, the ISO 27000 family is the one that is named most frequently, according to the frequency with which audit guidelines are named. It also has the ISO 27004 audit guide, which considers generic steps for its implementation. These generic steps leave it up to the implementer to decide how to review the controls. Furthermore, ISO 27004 lacks guidance specifying the relevant evidence that should be collected for proper cybersecurity risk audit traceability.

There are currently few audit guidelines that are specifically focused on cybersecurity requirements. The NIST CSF and CSAM models have been the only ones identified as guidelines for auditing the maturity and effectiveness of cybersecurity risk mitigation mechanisms.

The most important limitation lies in the fact that the difficulty of homologation with standards, legislation, or guidelines used for processes other than cybersecurity may explain the absence of easily applicable and adaptable guidelines for the audit of cybersecurity risk.

Another possible point to consider in future research lines is the creation of a guideline for the audit of cybersecurity risks. The guideline should be designed taking into account the three levels of audit of equal importance: strategic, technical and process.

Further research is needed to understand disparities in the techniques and characteristics of the current audit guidelines. It is suggested that the most frequently mentioned guidelines be included in a subsequent study. The objective of this study is to determine the minimum of task and activities necessary for conducting cybersecurity audits.

References

[1] S. Slapničar, T. Vuko, M. Čular, and M. Drašček, “Effectiveness of cybersecurity audit,” *International Journal of Accounting Information Systems*, vol. 44, p. 100548, Mar. 2022, doi: 10.1016/j.accinf.2021.100548.

[2] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, *Enterprise Cybersecurity Study Guide*. Apress, 2018. doi: 10.1007/978-1-4842-3258-3.

[3] European Confederation of Institutes of Internal Auditors, “‘Risk in focus 2021. Hot topics for internal auditors,’” *available at: https://www.eciia.eu/wp-content/uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.pdf*, 2020.

[4] B. Duncan and M. Whittington, “Compliance with standards, assurance and audit: Does this equal security?,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2014, pp. 77–84. doi: 10.1145/2659651.2659711.

[5] M. E. Galligan and K. Rau, “COSO in the cyber age,” 2015.

[6] A. Kotb, H. Elbardan, and H. Halabi, “Mapping of internal audit research: a post-Enron structured literature review,” *Accounting, Auditing & Accountability Journal*, vol. 33, no. 8, pp. 1969–1996, Aug. 2020, doi: 10.1108/AAAJ-07-2018-3581.

[7] Deloitte, “The future of cyber survey 2019,” 2019. Accessed: Sep. 02, 2022. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf

[8] S. Bergquist, S. Elofsson, and C. Lindholm, “The collaboration between auditors and IT-auditors-The effects on the audit profession.”

[9] O. Turetken, S. Jethefer, and B. Ozkan, “Internal audit effectiveness: operationalization and influencing factors,” *Managerial Auditing Journal*, vol. 35, no. 2, pp. 238–271, Dec. 2019, doi: 10.1108/MAJ-08-2018-1980.

[10] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, “A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM),” in *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, Institute of Electrical and Electronics Engineers Inc., Mar. 2018, pp. 253–259. doi: 10.1109/INCISCOS.2017.20.

[11] M. P. Gauthier and N. Brender, “How do the current auditing standards fit the emergent use of blockchain?,” *Managerial Auditing Journal*, vol. 36, no. 3, pp. 365–385, Jul. 2021, doi: 10.1108/MAJ-12-2019-2513.

[12] Virginia Office of the State Inspector General OSIG, “2021 COMMONWEALTH OF VIRGINIA INFORMATION SECURITY REPORT Commonwealth Security and Risk Management Connecting-Protecting-Innovating,” 2021.

[13] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Information and Software Technology*, vol. 51, no. 1. Elsevier B.V., pp. 7–15, 2009. doi: 10.1016/j.infsof.2008.09.009.

[14] G. IGNAT, L. ȘARGU, T. BIVOL, A. BIVOL-NIGEL, and N. ȘARGU, “Studies on the Importance of Internal Audit in Detection of Risks,” in *Proceedings of the International Conference Digital Age: Traditions, Modernity and Innovations (ICDATMI 2020)*, Paris, France: Atlantis Press, 2020. doi: 10.2991/assehr.k.201212.030.

[15] A. Eulerich and M. Eulerich, “What is the value of internal auditing? – A literature review on qualitative and quantitative perspectives,” *Maandblad Voor Accountancy en Bedrijfseconomie*, vol. 94, no. 3/4, pp. 83–92, Apr. 2020, doi: 10.5117/mab.94.50375.

[16] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, “Review and insight on the behavioral aspects of cybersecurity,” *Cybersecurity*, vol. 3, no. 1, p. 10, 2020, doi: 10.1186/s42400-020-00050-w.

[17] M. Gale, I. Bongiovanni, and S. Slapnicar, “Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead,” *Comput Secur*, vol. 121, p. 102840, Oct. 2022, doi: 10.1016/j.cose.2022.102840.

[18] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, “SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs,” *Journal of Information Systems*, vol. 30, no. 1, pp. 71–92, Mar. 2016, doi: 10.2308/isys-51257.

[19] T. Stafford, G. Deitz, and Y. Li, “The role of internal audit and user training in information security policy compliance,” *Managerial Auditing Journal*, vol. 33, no. 4, pp. 410–424, Jun. 2018, doi: 10.1108/MAJ-07-2017-1596.

[20] International Organization for Standardization, “ISO/IEC 27005-2018.” 2018.

[21] National Institute of Standards and Technology, “NIST Cybersecurity framework,” *Proceedings of the Annual ISA Analysis Division Symposium*, vol. 535, pp. 9–25, 2018.

[22] Information Systems Audit and Control Association, *COBIT 2019*. 2018. Accessed: May 09, 2022. [Online]. Available: www.isaca.org/COBIT

[23] Md. S. Islam, N. Farah, and T. F. Stafford, “Factors associated with security/cybersecurity audit by internal audit function,” *Managerial Auditing Journal*, vol. 33, no. 4, pp. 377–409, Jun. 2018, doi: 10.1108/MAJ-07-2017-1595.

[24] N. Ezzamouri and J. Hulstijn, “Continuous monitoring and auditing in municipalities,” in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, New York, NY, USA: ACM, May 2018, pp. 1–10. doi: 10.1145/3209281.3209301.

[25] B. R. Aditya, R. Ferdiana, and P. I. Santosa, “Toward Modern IT Audit– Current Issues And Literature Review,” *2018 4th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia*, 2018.

[26] U. VIJAYAKUMAR and D. ILANGOVAN, “A Quantitative Approach to Information Systems Audit in Small and Medium Enterprises,” *Informatica Economica*, vol. 19, no. 3/2015, pp. 89–95, Sep. 2015, doi: 10.12948/issn14531305/19.3.2015.08.

[27] A. Fernandez *et al.*, “Flooding and mental health: A systematic mapping review,” *PLoS ONE*, vol. 10, no. 4. Public Library of Science, Apr. 10, 2015. doi: 10.1371/journal.pone.0119929.

[28] T. Dyba, T. Dingsoyr, and G. K. Hanssen, “Applying Systematic Reviews to Diverse Study Types: An Experience Report,” in *First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007)*, IEEE, Sep. 2007, pp. 225–234. doi: 10.1109/ESEM.2007.59.

[29] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic Mapping Studies in Software Engineering,” *12Th International Conference on Evaluation and Assessment in Software Engineering*, vol. 17, p. 10, 2008, doi: 10.1142/S0218194007003112.

[30] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, 2014. doi: 10.1145/2601248.2601268.

[31] X. Feng and M. Conrad, “Security audit in mobile apps security design,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Oct. 2018. doi: 10.1145/3207677.3277925.

[32] J. Hoag, “Evolution of a Cybersecurity curriculum,” in *Proceedings of the 2013 on InfoSecCD ’13 Information Security Curriculum Development Conference - InfoSecCD ’13*, New York, New York, USA: ACM Press, 2013, pp. 94–99. doi: 10.1145/2528908.2528925.

[33] S. M. T. Toapanta, N. A. Peralta, and L. E. M. Gallegos, “Definition of parameters to perform audit in cybersecurity for public one organization of ecuador,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2019, pp. 91–96. doi: 10.1145/3375900.3375913.

[34] B. Burgemeestre, J. Hulstijn, and Y. H. Tan, “Value-based argumentation for designing and auditing security measures,” *Ethics Inf Technol*, vol. 15, no. 3, pp. 153–171, Sep. 2013, doi: 10.1007/s10676-013-9325-2.

[35] J. Hagen and O. Toftegaard, “Cyber Security Requirements in the Norwegian Energy Sector,” in *IFIP Advances in Information and Communication Technology*, Springer Science and Business Media Deutschland GmbH, 2022, pp. 3–21. doi: 10.1007/978-3-030-93511-5\_1.

[36] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, “A security review of local government using NIST CSF: a case study,” *Journal of Supercomputing*, vol. 74, no. 10, pp. 5171–5186, Oct. 2018, doi: 10.1007/s11227-018-2479-2.

[37] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, “The relationship between internal audit and information security: An exploratory investigation,” *International Journal of Accounting Information Systems*, vol. 13, no. 3, pp. 228–243, Sep. 2012, doi: 10.1016/j.accinf.2012.06.007.

[38] L. Zhou, R. Thieret, V. Watzlaf, D. Dealmeida, and B. Parmanto, “A telehealth privacy and security self-assessment questionnaire for telehealth providers: Development and validation,” *Int J Telerehabil*, vol. 11, no. 1, pp. 3–14, Mar. 2019, doi: 10.5195/ijt.2019.6276.

[39] M. J. Cotteleer *et al.*, “Cybersecurity Requirements for AM Systems,” in *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*, New York, NY, USA: ACM, Nov. 2021, pp. 49–60. doi: 10.1145/3462223.3485624.

[40] H. Berrada, J. Boutahar, S. El, and G. El Houssaïni, “Simplified IT Risk Management Maturity Audit System based on ‘COBIT 5 for Risk,’” 2021. [Online]. Available: www.ijacsa.thesai.org

[41] O. M. M. Al-Matari, I. M. A. Helal, S. A. Mazen, and S. Elhennawy, “Integrated framework for cybersecurity auditing,” *Information Security Journal*, vol. 30, no. 4, pp. 189–204, 2021, doi: 10.1080/19393555.2020.1834649.

[42] S. Bozkus Kahyaoglu and K. Caliyurt, “Cyber security assurance process from the internal audit perspective,” *Managerial Auditing Journal*, vol. 33, no. 4, pp. 360–376, Jun. 2018, doi: 10.1108/MAJ-02-2018-1804.

[43] M. A. Melshiyan and A. V. Dushkin, “Information Security Audit Using Open Source Intelligence Methods,” in *Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 379–382. doi: 10.1109/ElConRus54750.2022.9755530.

[44] I. I. Livshitz, K. A. Nikiforova, P. A. Lontsikh, and S. N. Karasev, *The New Aspects for the Instantaneous Information Security Audit*. 2016.

[45] I. I. Livshitz, P. A. Lontsikh, N. P. Lontsikh, E. P. Kunakov, and D. E. Y. Elena Yu, *Implementation and Auditing of Risk Management for the Oil and Gas Company*. 2017.

[46] I. I. Livshitz, P. A. Lontsikh, N. P. Lontsikh, E. Y. Golovina, and O. M. Safonova, “The effects of cyber-security risks on added value of consulting services for IT-security management systems in holding companies,” in *Proceedings of the 2020 IEEE International Conference “Quality Management, Transport and Information Security, Information Technologies”, IT and QM and IS 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 119–122. doi: 10.1109/ITQMIS51053.2020.9322883.

[47] M. Mogale, M. Gerber, M. Carroll, and R. Von Solms, *Information Security Assurance Model (ISAM) for an Examination Paper Preparation Process*. 2014.

[48] S. Muhammad R and M. Febriana, “Moving Towards PCI DSS 3.0 Compliance: A Case Study of Credit Card Data Security Audit inan Online Payment Company,” *ICACSIS*, 2014.

[49] N. Sun, C.-T. Li, H. Chan, M. Z. Islam, M. R. Islam, and W. Armstrong, “How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond,” *IEEE Access*, vol. 10, pp. 71749–71763, 2022, doi: 10.1109/ACCESS.2022.3187211.

[50] K. Nisyak, S. Hajar, and Z. Anazida, *Review of Cybersecurity Audit Management and Execution Approaches*. 2019.