electronics

MDPI

Article

Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada

Regner Sabillon [1], Juan Ramon Bermejo Higuera [1,*], Jeimy Cano [2], Javier Bermejo Higuera [1] and Juan Antonio Sicilia Montalvo [1]

[1] Escuela Superior de Ingeniería y Tecnología, Universidad Internacional de La Rioja (UNIR), 26006 Logroño, La Rioja, Spain; regners@athabascau.ca (R.S.); javier.bermejo@unir.net (J.B.H.); juanantonio.sicilia@unir.net (J.A.S.M.)

[2] Law Faculty, Universidad de los Andes, Bogotá 111711, Colombia; jcano@uniandes.edu.co

* Correspondence: juanramon.bermejo@unir.net

Abstract: This study validates a comprehensive cybersecurity audit model through empirical analysis in three higher education institutions in Canada. The research aims to enhance cybersecurity resilience by assessing the effectiveness of cybersecurity controls across diverse educational environments. Given the increasing frequency and sophistication of cyberattacks targeting educational institutions, this research is essential to ensure the protection of sensitive academic and personal data. Data were collected through detailed audits involving system vulnerabilities, compliance with security policies, and incident response management at each institution. The findings underscore the importance of tailored cybersecurity strategies and continuous auditing to mitigate cyber risks in the Canadian higher education sector. This study contributes to the field by validating a versatile audit tool that can be adapted to various institutional contexts, promoting enhanced cybersecurity practices and evaluating the effectiveness of cybersecurity safeguards across the higher education sector in Canada. The results of the audit model validations provide the cybersecurity maturity rating of each institution. Further research is recommended to refine the model and explore its application in other industries and sectors.

Keywords: cybersecurity control; cybersecurity domain; cybersecurity audit; cyber readiness; cybersecurity audit model; cybersecurity

Citation: Sabillon, R.; Higuera, J.R.B.; Cano, J.; Higuera, J.B.; Montalvo, J.A.S. Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada. *Electronics* **2024**, *13*, 3257. https://doi.org/10.3390/electronics13163257

Academic Editor: Aryya Gangopadhyay

Received: 30 June 2024
Revised: 9 August 2024
Accepted: 14 August 2024
Published: 16 August 2024

1. Introduction

Organizations are striving to safeguard their digital assets and implement cybersecurity protocols and initiatives. However, despite ongoing efforts, it remains inevitable to entirely prevent cybersecurity breaches and cyberattacks. According to *Crowdstrike* [1], the top 10 industries affected by intrusion campaigns in 2022 were technology, financial services, healthcare, telecommunications, retail, manufacturing, academic, services, government, and pharmaceutical, where cybercrime adversary activities mostly come from Russia, Vietnam, North Korea, South Korea, Iran, Pakistan, Georgia, Colombia, China, India, and Turkey and in a lesser scale from some hacktivism groups (Crowdstrike, 2023). INTERPOL [2] reports that cybercriminals are increasing their cyberattacks by taking advantage of the current instability of the global socioeconomical situation and, based on data collected from its 195 country members, identifies ransomware, phishing, online scams, computer intrusion, and online child sexual exploitation as global cybercrime activities resulting in high or very high threats (Interpol, 2023).

In the contemporary landscape, internal audits need to evolve to address, strategize for, and assess significant cyber risks linked with cybersecurity. Smaller companies often face a more significant financial blow from cyberattacks compared to big companies. The

majority of the companies involved in this survey are considered "cyber novices" regarding their preparedness for cyber threats. The analysis reveals that simply allocating funds or having large cybersecurity budgets does not automatically advance companies to the "Cyber Experts" category. Cyber readiness tends to be more effectively managed in big companies due to the array of resources at their disposal. However, a substantial financial investment alone is not the solution. Instead, implementing strategies such as upper management involvement, cybersecurity awareness training, systematic monitoring, and documentation is crucial. According to a research study conducted by IBM Security [3], the global average total cost of a data breach increased to USD 4.45 million, showing a 15.3% increase since 2020. The 2023 cost of a data breach varies by countries and geographic regions, for example, in the USA, the cost was USD 9.48 million, USD 8.07 million in the Middle East, USD 5.13 million in Canada, USD 4.67 million in Germany, USD 4.52 million in Japan, USD 4.21 million in the UK, USD 4.08 million in France, USD 3.86 million in Italy, USD 3.69 in Latin America, and USD 3.05 million in Southeast Asian Nations (ASEAN).

Meulen et al. [4] emphasize the importance of stakeholders grasping the threat landscape to anticipate future cyberattacks and implement defensive measures. They noted the absence of specific standards for classifying cyberthreats, highlighting the ambiguity in defining threat assessments. The identified main threat actors include states, cybercriminals, and hacktivists, while acknowledged cyber threats include access breaches, data disclosure, manipulation, destruction, and service denial. Balbix [5] reports numerous challenges in adopting a robust enterprise cybersecurity posture: 64% of assessed organizations lack confidence in their security stance, 60% struggle with detecting fewer than 75% of network devices, and 80% allow for excessive access privileges. Moreover, cybersecurity leaders often fail to effectively communicate the organization's cybersecurity posture to upper management (Balbix, 2019) [6]. Despite sufficient cybersecurity measures, employees remain the weakest link in cybersecurity. Nonetheless, as organizations could face cyberattacks at any time, those prepared stand better equipped to mitigate impacts and contain consequences.

According to Pendergast [7], employees from any company are directly implicated in financial losses stemming from data breaches and cybersecurity incidents. However, various threat agents, both internal and external, can be responsible for cyberthreats and cyberattacks. Information Technology (IT) audits are undergoing redefinition to incorporate cybersecurity; however, there is no clear consensus or established guidelines on which specific areas, sub-areas, domains, or sub-domains should be covered in a cybersecurity audit. While audit planning now integrates cybersecurity into IT project development and design, it often falls short in addressing project requirements. PricewaterhouseCoopers [8] reports a surge in the exploitation of vulnerabilities in Virtual Private Networks (VPNs), enterprise remote access, and virtualization applications (PricewaterhouseCoopers, 2021). KPMG underscores the importance of considering key cyber risks in cybersecurity internal auditing, including emerging threats, technological advancements, business transformations, regulatory updates, and third-party risks. They emphasize several areas for auditing cybersecurity, including alignment with business goals and strategies, adherence to cybersecurity frameworks, identification of emerging cyberthreats, and talent identification. While the cyberthreat landscape continues to evolve, the current threats do not replace the old ones; instead, cybercriminals are developing and deploying new families of malware. These cyberattacks involve more active groups targeting organizations using customized intrusion tools alongside open source tools commonly deployed in similar hacking phases.

Autonomous Cyber Defense explores the application of artificial intelligence (AI), specifically reinforcement learning (RL), to autonomously detect, prevent, and respond to cyber threats. The goal is for these AI agents to perform tasks that human defenders perform, such as protecting networks and detecting malicious activity, but at the speed of digital attacks. This research also addresses the significant challenges in achieving fully autonomous cyber defense, including ensuring adaptability to new threats, generating logs for review (auditability), allowing human operators to intervene (directability), providing sufficient data for situational awareness (observability), securing the systems

against tampering, and ensuring that these systems can be deployed in various real-world environments (transferability). Furthermore, it highlights the importance of balancing the development of defensive and offensive agents to create robust defenses and emphasizes the need for policy support, sustained funding, joining efforts in data sharing, and talent development to advance the field of autonomous cyber defense [9].

The autonomous generation of attacks and defenses in cybersecurity involves the use of artificial intelligence (AI) to automate both offensive and defensive measures. This emerging field seeks to leverage AI to detect threats, harden systems, and respond to cyber incidents without human intervention. Reinforcement learning (RL) is a leading approach in developing these autonomous agents, allowing them to learn and adapt to various cyber threats by simulating environments wherein they can practice defense strategies. These agents aim to operate at the speed and scale required to match the pace of digital attacks, providing a significant advantage over traditional, human-led cyber defense methods. Despite the promising advancements, several challenges persist before autonomous cyber defense systems can be operationally deployed. These include ensuring adaptability to evolving threats, maintaining auditability and security of the agents, and enabling transferability across different environments. Autonomous systems must also be capable of making independent decisions while adhering to predefined legal and ethical standards. To address these challenges, ongoing research focuses on scaling up simulations, providing infrastructure for training and testing, and fostering data sharing among stakeholders. The utmost goal is to create dependable and effective autonomous agents that can protect networks and systems more efficiently than current human-centric approaches [10].

The autonomous generation of attacks and defenses in cybersecurity involves the use of artificial intelligence (AI) to automate both offensive and defensive measures. This emerging field seeks to leverage AI to detect threats, harden systems, and respond to cyber incidents without human intervention. Reinforcement learning (RL) is a leading approach in developing these autonomous agents, allowing them to learn and adapt to various cyber threats by simulating environments wherein they can practice defense strategies. These agents aim to operate at the speed and scale required to match the pace of digital attacks, providing a significant advantage over traditional, human-led cyber defense methods. Despite the promising advancements, several challenges persist before autonomous cyber defense systems can be operationally deployed. These include ensuring adaptability to evolving threats, maintaining auditability and security of the agents, and enabling transferability across different environments. Autonomous systems must also be capable of making independent decisions while adhering to predefined legal and ethical standards. To address these challenges, ongoing research focuses on scaling up simulations, providing infrastructure for training and testing, and fostering data sharing among stakeholders. The utmost goal is to create dependable and effective autonomous agents that can protect networks and systems more efficiently than current human-centric approaches [11].

Pleshakova et al. [12] delve into the evolving landscape of cybersecurity in the context of advancements in artificial intelligence (AI), particularly large language models (LLMs). These models are capable of performing complex tasks, including cryptographic functions, without explicit programming. The research points out the potential of LLMs to revolutionize cybersecurity by enabling automated threat detection and response, as well as the development of new cryptographic methods that can protect information from other neural networks. Nevertheless, the integration of LLMs also introduces new challenges, such as the risks associated with AI-based cybersecurity systems being compromised by malicious actors. The authors emphasize the increasing sophistication of cyber threats, including social engineering and fraud, which have become more targeted and complex. They review the need for advanced AI-based systems to address these challenges, proposing the use of generative adversarial networks (GANs) and decentralized LLMs for automated adversarial attacks and defenses. This paper also analyzes future trends in cybersecurity, such as intent-based networking and AI-enhanced zero-touch network security for 5G and 6G networks. The authors conclude that, while AI offers remarkable opportunities for

enhancing cybersecurity, it also requires thoughtful consideration of the associated risks and the development of robust, trustworthy systems.

Our validated model (CSAM 2.0) [13] seeks to address the shortcomings of existing cybersecurity controls in performing thorough cybersecurity audits or domain-specific assessments. There is an urgent requirement for a comprehensive cybersecurity audit model to enhance the effectiveness of information security functions. Likewise, there is a need for a model that provides cybersecurity awareness training tailored to specific company roles, moving beyond conventional awareness programs. This article details the results of empirical studies that assess the implementation and validation of our CSAM audit model [14] via extensive cybersecurity audits in real-world institutions. This study is driven by the lack of universal guidelines for executing comprehensive cybersecurity audits.

Our multi-case research was conducted to answer the following question:

How might we assess and quantify the level of resilience and preparedness against cyberthreats within an organization or a nation-state, considering factors such as cybersecurity posture, response capabilities, and risk management strategies?

This paper follows this structure: In Sections 2 and 3, we delve into the literature pertinent to our research topics. Section 4 elucidates the structure of our cybersecurity model, the CyberSecurity Audit Model (CSAM 2.0). In Section 5, we outline the research methods employed in our case study. Section 6 examines the key findings from three distinct scenarios, with a focus on summarizing the experimental results in three Canadian higher education institutions (CHEIs) that produced the cybersecurity maturity ratings. Section 7 encompasses the research discussion. Lastly, Section 8 offers the conclusions and future work drawn from our study.

2. Background

This paper focuses on creating a framework for establishing, developing, planning, executing, and sustaining a cybersecurity audit (CSA) methodology or program. The validation of this model occurred in three distinct Canadian higher education institutions, each facing different scenarios and timelines. The implementations in all settings formed part of multi-case studies, alongside the Cybersecurity Awareness TRAining Model (CATRAM 2.0) [15], a complementary model for providing cybersecurity training tailored to specific roles and responsibilities. While existing frameworks and methodologies offer various approaches to adopting cybersecurity controls across domains, many lack clear objectives and guidance on conducting comprehensive or partial cybersecurity audits. For example, the NIST Cybersecurity Framework (NIST CSF 2.0) [16] overlooks areas such as cybersecurity strategy, compliance with frameworks, and implementing controls for its six core functions. In contrast, CyberSecurity Audit Model (CSAM 2.0) [17] was uniquely crafted to conduct partial or comprehensive cybersecurity audits within specific, selected, or all cyber domains of the target organization. Moreover, CSAM 2.0 is designed for straightforward implementations and is adaptable for organizations such the target institutions in this research study.

In this research, CSAM 2.0 was confirmed as the underlying model for the selected institutions, which previously lacked cybersecurity audit policies. CSAM 2.0 was introduced to establish cybersecurity assessments for their domains and safeguards.

Presently, CSAM 2.0 is continually employed to craft forthcoming cybersecurity audit initiatives for the chosen establishments. The identities of these organizations cannot be revealed due to concerns regarding security, privacy, and the existence of non-disclosure agreements (NDAs).

This research study significantly advances global scientific knowledge by empirically validating CyberSecurity Audit Model (CSAM 2.0), a comprehensive and adaptable framework for conducting cybersecurity audits. Unlike existing cybersecurity frameworks, CSAM 2.0 integrates multiple cybersecurity domains, providing detailed guidance on evaluating and enhancing cybersecurity controls tailored to various organizational environments. By validating this model in three distinct Canadian higher education institutions, this

study demonstrates the model's versatility and effectiveness in improving cybersecurity resilience. The findings highlight the critical relevance of tailored cybersecurity strategies and continuous cyber auditing, offering a robust tool for organizations worldwide to consistently assess and strengthen their cybersecurity postures.

Moreover, this research contributes to the global discourse on cybersecurity by addressing the imperative need for adaptable and practical audit frameworks capable of evolving with the rapidly changing cyber threat landscape. By focusing on specific domains, CSAM 2.0 provides a comprehensive approach that existing auditing frameworks often lack. This paper not only fills a significant gap in the literature by offering a validated model for comprehensive cybersecurity audits but also sets a precedent for future research in diverse sectors and geographical regions. The insights gained from this study underscore the universal applicability of CSAM 2.0, paving the way for its adoption and refinement in various industries and promoting a global shift toward proactive cybersecurity risk management.

3. Literature Review

Cybersecurity, IT security, and privacy are identified as the primary overarching challenges for IT audit teams and its members. It is imperative for organizations to continuously review their IT audit projects to effectively tackle cyberthreats and arising technologies.

The Canadian federal government has developed the Cyber Security Audit Program (Government of Canada, 2021) [18], which comprises four free tools. Originally designed for Canadian federal agencies, this program is now accessible to any Canadian organization seeking to conduct cybersecurity audits based on its framework. These tools are outlined briefly as follows:

1. Placemat (Government of Canada, 2021) [19]: This document outlines the Top 10 IT Security Actions alongside 12 best practices for conducting cybersecurity audits across various domains.
2. Audit Guide (Government of Canada, 2021) [20]: It offers guidelines for planning and executing audits, focusing on cybersecurity governance, policy, compliance, risk management, and protective measures within organizations.
3. Preliminary Survey Tool (PST) (Government of Canada, 2021) [21]: This tool assesses the overall cybersecurity posture of the target organization.
4. Audit Program (Government of Canada, 2021) [22]: This document furnishes criteria, sub-criteria, and audit tests to facilitate cybersecurity audits.

Deloitte underscores the implication of intrinsic examinations in validating the efficacy of cybersecurity controls, with cyber risk management delineated according to distinct positions and liabilities:

1. The initial front of protection comprises business and IT functions.
2. The second line of protection involves information and technology risk management.
3. The final line of protection encompasses internal audits.

Deloitte's cybersecurity framework [23] emphasizes that, while certain cybersecurity domains can be assessed using existing IT channels, many cyber capabilities exceed the scope of internal audits. This framework covers a wide range of areas, such as risk and compliance management, development lifecycle, security program, third-party management, information and asset management, access management, threat and vulnerability management, data management and protection, risk analytics, crisis management and resilience, security operations, and security awareness and training (Deloitte, 2020) [24].

Furthermore, Deloitte's framework is in line with industry standards developed by governing institutions such as the National Institute of Standards and Technology (NIST), Information Technology Infrastructure Library (ITIL), Committee of Sponsoring Organizations of the Treadway Commission (COSO), and International Organization for Standardization (ISO).

The Institute of Internal Auditors (IIA) [25] has revised the Three Lines of Defense model to the Three Lines Model, incorporating principles, key roles, and relationships among primary participants. The three lines consist of the Governing Body, Management, and Internal Audit, with Management and Internal Audit reporting to the Governing Body. Each stakeholder has distinct roles and responsibilities including accountability, reporting, delegation, direction, resources, oversight, alignment, communication, coordination, and collaboration (The Institute of Internal Auditors, 2020). Given the evolving nature of cyber risks, businesses must embed cyber resilience and flexibility into their operations, implementing cyber-by-design principles across initiatives and continually reassessing cyber risks. While security education and awareness are crucial, cyber practices and behaviors should be ingrained in organizational culture to foster reliability and trust in hyper-connected environments.

A cybersecurity study by Deloitte and NASCIO [26] emphasizes key cybersecurity initiatives, including training and awareness programs, metric programs for measuring and reporting cybersecurity status, cyber risk assessment, and cyber strategy (Deloitte, 2018). The 2020 edition [23] underscores critical cybersecurity adaptations in response to COVID-19, such as securing teleconferencing and video solutions, implementing multifactor authentication mechanisms, conducting awareness training to combat pandemic-related phishing and disinformation campaigns, maintaining up-to-date business continuity operation plans, and offering continuous guidance to address COVID-19 scams (Deloitte, 2020). Additionally, increased collaboration between federal and local governments and higher education institutions has led to the transition to a centralized model to enhance cyber operations, resources, and staffing.

However, challenges persist in assessing cybersecurity alertness, including the lack of guidelines for conducting cybersecurity examinations. Addressing cyberattacks requires a focused approach to cybersecurity audit processes, ensuring the encryption of critical information, and maintaining proper patch management. Furthermore, there is a lack of metrics to gauge the quality and outcomes of cybersecurity audits, with the cybersecurity audit domain evolving rapidly. To conduct meaningful cybersecurity audits, auditors ought to encompass all crucial areas of the organization and audit reporting should not merely highlight security weaknesses but also propose appropriate solutions. While recommendations are not always mandatory in final audit reports, they are advisable to include remedial, preventative, or straightaway actions for subsequent audits. The goal of cybersecurity audits should be to provide genuine assessments of security safeguards, standards, processes, and guidelines to senior management. Cybersecurity auditors must possess the technical skills and expertise to conduct advanced testing and assess the effectiveness of cybersecurity controls, going beyond simple interviews and documentation verification.

In the realm of cyber readiness studies, Hathaway et al. [27] developed a comprehensive methodology that has been implemented in 125 countries and is available in six languages: Arabic, Chinese, English, French, Russian, and Spanish. The authors also created specific Cyber Readiness Index (CRI) profiles for countries such as France, Germany, India, Italy, Japan, The Netherlands, Morocco, Slovakia, Saudi Arabia, the UK, and the United States of America. Originally released in November 2013, the Cyber Readiness Index 1.0 was updated with the Cyber Readiness Index 2.0 in November 2015. This methodology underscores that "No country is cyber ready" and evaluates a nation's readiness to manage cyber risks, identifying critical cyber-related areas and recommending measures to safeguard their economy and connectivity through cybersecurity initiatives (Hathaway et al., 2015).

ENISA [28] has reported an increase in specific types of cyberattacks such as web-based attacks, spam, identity theft, insider threats, information leakage, ransomware, and cyber espionage (ENISA, 2020). ENISA also identified two key factors during the global pandemic:

1. The sudden transformation in global society, particularly in how we work, study, and interact socially using technology.
2. The enhanced cyber capabilities of advanced threat actors, which significantly amplified the impact of COVID-19 in cyberspace.

Regarding financial audits, financial auditors have assessed IT controls for several years, starting with SAS 3 in 1974, SAS 44 in 1982, SAS 70 in 1992, WebTrust in 1997, SysTrust in 1999, the Trust Services Principles & Criteria in 2003, SSAE 16 in 2010, SOC 1 in 2011, SSAE 18 in 2016, and using the Cybersecurity Risk Management Reporting Framework and Examination criteria [29]. The Center for Audit Quality [30] endorses these cyber schemes as foundational for implementing and assessing corporate cybersecurity risk management programs. In 2021, the CAQ explored the implications of artificial intelligence (AI) and machine learning in enhancing defense mechanisms against cyber threats to mitigate cybersecurity risks.

Additionally, the American Institute of Certified Public Accountants (AICPA) [31] has developed its own cybersecurity framework known as the Cybersecurity Reporting Framework. This framework is an entity-level cybersecurity risk management framework that emphasizes upper management's descriptions and assertions.

Wertheim [32] suggests a plan of action emphasizing that cybersecurity issues are integral to business operations. This involves a thorough understanding of cyber risk management, recognizing the audit function's role in assessing cybersecurity controls, evaluating the effectiveness of current cyber controls, and recommending new ones if necessary. It also includes monitoring systems and technologies, managing patches properly, continuously auditing incident response plans (IRPs), and signing agreements with outsourcing providers when needed. Ultimately, organizations that effectively protect their cyber assets are better equipped to handle cyber incidents, with the primary goal being to minimize the impact of any cyberattacks on their critical business operations.

In summary, current global trends indicate that numerous regulatory associations and organizations are developing their own cybersecurity frameworks and policies to enhance overall cybersecurity posture. Many companies are also adopting and adapting existing cybersecurity frameworks to implement cyber controls. Conducting cybersecurity audits is essential for continually evaluating the effectiveness of security controls and detecting missing controls early to safeguard an organization's assets.

Cybersecurity Asset Management (CSAM) facilitates this by easily evaluating an organization's cybersecurity posture. We have identified specific frameworks for conducting cybersecurity audits like NIST SP 800-53 Rev. 5 [33], SOC 2 [34], SOC for Cybersecurity [35], PCI DSS v4.0 [36], NIST Cybersecurity Framework (CSF) 2.0 [16], CIS Controls v8 [37] and ISO/IEC 27001:2022 [38] that are discussed below.

3.1. NIST Special Publication 800-53 Revision 5

NIST SP 800-53 Rev. 5 [33] provides a comprehensive framework for implementing security and privacy controls, with a specific focus on audit and accountability. By following the guidelines and controls outlined in the Audit and Accountability (AU) family, organizations can ensure that they have robust mechanisms for conducting audits, which are crucial for maintaining security and privacy compliance. Implementing these controls as part of the broader Risk Management Framework (RMF) ensures that audit processes are integrated into the overall risk management strategy of the organization.

Phases for conducting AU audits:

- Preparation: Define the realm, goals, and benchmark for the audit. Ensure that policies and procedures for auditing are in place (AU-1).
- Execution: Collect and analyze audit data (AU-6), ensuring that audit records are generated (AU-12) and stored securely (AU-4).
- Review and Reporting: Regularly review audit logs and records to identify and respond to unusual or unauthorized activities (AU-6, AU-7).

- Protection: Implement measures to safeguard audit information from unauthorized access, alteration, or removal (AU-9).
- Retention and Management: Maintain review records for an appropriate period as defined by organizational policies (AU-11).

3.2. SOC 2

The Association of International Certified Professional Accountants (AICPA) Service Organization Control Type 2 (SOC 2) [34] provides a system for overseeing and securing customer data in cloud environments, founded on five trust service principles. Conducting a SOC 2 audit involves defining the scope, conducting a readiness assessment, collecting evidence, testing controls, and preparing a report. The audit ensures that the organization's controls are well-designed and functioning effectively to protect data, thereby building trust with customers and stakeholders. The result is a comprehensive report that provides assurance on the organization's ability to manage and secure customer data according to the trust service criteria.

Relevant aspects for conducting SOC 2 audits:

1. SOC 2 Types:
   - Type I: Evaluates the appropriateness of the design of controls at a given moment in time.
   - Type II: Evaluates the suitability of the design and operational effectiveness of controls over a specified period, typically ranging from six months to a year.
2. SOC 2 Audit Process:
   - Scoping: Define the scope of the audit aligned with the trust service criteria pertinent to the organization.
   - Readiness Assessment: Conduct a preliminary assessment to identify gaps in controls and implement necessary changes.
   - Evidence Collection: Gather evidence that demonstrates the adequacy and operational effectiveness of the controls. This includes policies, procedures, and logs.
   - Testing: The auditor tests the controls to evaluate their design and operational effectiveness. For Type II audits, this includes testing over the specified period.
   - Reporting: The auditor prepares a SOC 2 report detailing the findings, including any deviations or exceptions.
3. Key Controls for SOC 2 Audits:
   - Logical and Physical Access Controls: Securing systems and data to restrict access solely to authorized users.
   - System Operations Controls: Monitoring and maintaining system performance and integrity.
   - Change Management Controls: Managing changes to the system to ensure they are authorized and do not negatively impact security or performance.
   - Risk Management Controls: Identifying and reducing risks to handle the security and privacy of data.
4. Reports:
   - Overview of the organization and its services.
   - Description of the system: Includes details of the infrastructure, software, people, processes, and data involved.
   - Control objectives and controls: Listing the controls implemented to achieve the Trusted Service Criteria (TSC).
   - Auditor's opinion: An independent assessment of whether the controls meet the TSC.
   - Test results: Detailed results of the auditor's assessment of the controls.
   - Management's assertion: The organization's statement confirming that the controls are appropriately designed and functioning effectively.

3.3. SOC for Cybersecurity

The Association of International Certified Professional Accountants (AICPA) Service Organization Control for Cybersecurity [35] is a framework designed to help organizations assess and report on their cybersecurity risk management programs. Conducting a cybersecurity audit using SOC for Cybersecurity involves several key steps:

1. Understanding the framework: Familiarize yourself with the AICPA SOC for Cybersecurity framework, including its principles and criteria. These criteria are organized into five categories: Governance, Risk Assessment, Risk Management, Information Communication, and Monitoring Activities.
2. Scoping the Audit: Specify the extent of the audit, identifying the systems, processes, and controls to be evaluated. Distinguish the assets, systems, and processes that are part of the audit's scope.
3. Planning the Audit: Develop a plan detailing the objectives, scope, methodology, and schedule for conducting the audit. Identify the key stakeholders and resources needed for the audit.
4. Assessing Controls: Assess the efficiency of the organization's cybersecurity measures in accordance with the specified criteria outlined in the SOC for Cybersecurity framework. This may involve reviewing policies, procedures, technical configurations, and other relevant documentation.
5. Testing Controls: Perform testing to validate the effectiveness of the cybersecurity controls. This may include walkthroughs, interviews, observations, and technical testing such as vulnerability assessments and penetration testing.
6. Identifying Gaps and Deficiencies: Identify any gaps or deficiencies in the organization's cybersecurity program compared to the SOC for Cybersecurity criteria. Document these findings and assess their significance and potential impact on cybersecurity risk.
7. Reporting: Prepare a report summarizing the results of the cybersecurity audit. The report should include an overview of the organization's cybersecurity program, an assessment of the effectiveness of the cybersecurity controls, any identified gaps or deficiencies, and recommendations for improvement.
8. Communicating Findings: Present the audit findings to key stakeholders, including management and those responsible for cybersecurity oversight. Discuss the implications of the findings and recommendations for addressing any identified issues.
9. Follow-Up and Monitoring: Monitor the organization's progress in addressing any identified gaps or deficiencies. Follow up with management to ensure that appropriate corrective actions are taken to improve the cybersecurity program.
10. Continuous Improvement: Encourage a culture of continuous improvement in cybersecurity risk management. Provide ongoing guidance and support to help the organization strengthen its cybersecurity program over time.

By following these steps, organizations can effectively conduct cybersecurity audits using the AICPA SOC for Cybersecurity framework to assess and enhance their cybersecurity risk management programs.

3.4. PCI DSS v4.0

Payment Card Industry Data Security Standard (PCI DSS) v4.0 [36] is designed to enhance the security of payment card transactions by setting rigorous standards for protecting cardholder data. Conducting a PCI DSS 4.0 audit involves defining the scope, collecting evidence, testing controls, and preparing detailed reports to demonstrate compliance. The updated version emphasizes flexibility, continuous compliance, and stronger security measures, ensuring that organizations can effectively protect cardholder data in an evolving threat landscape.

Process for conducting PCI DSS v 4.0 compliance audits:

- Scoping: Define the scope of the assessment to identify all systems and procedures related to the storage, processing, or transmission of cardholder data.
- Pre-Assessment: Conduct a readiness assessment to identify gaps and implement necessary remediation steps.
- Evidence Collection: Gather documentation, logs, configurations, and other evidence demonstrating compliance with each of the 12 requirements.
- Testing and Validation: Assess the effectiveness of controls through testing procedures such as vulnerability scans, penetration testing, configuration reviews, and process inspections.
- Report on Compliance (ROC): Prepare a detailed report outlining compliance status, including evidence of control implementation and any observed deficiencies.
- Attestation of Compliance (AOC): A formal declaration of compliance status submitted to relevant stakeholders and payment brand.

3.5. NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology (NIST) CSF 2.0 [16] is intended to assist organizations in managing and reducing cybersecurity risks through a structured and flexible approach. Conducting audits based on NIST CSF 2.0 involves assessing the organization's implementation of the framework's core functions, ensuring alignment with business needs, and continuously improving cybersecurity practices. By following the framework, organizations can enhance their cybersecurity posture, better manage risks, and ensure robust protection of critical assets and data.

Process to conduct audits based on NIST CSF 2.0:

1. Audit Preparation:
    - Scope: Identify the scope, encompassing systems, processes, and departments to be reviewed.
    - Establish Baseline: Develop a baseline understanding of current cybersecurity posture by mapping existing practices to the NIST CSF.
2. Govern Phase:
    - Oversight: Verify oversight for cybersecurity risk management at the executive and board levels.
    - Policies: Assess cybersecurity policies and methodologies.
    - Roles: Ensure cybersecurity roles and responsibilities across the organization.
    - Strategy and Investment: Confirm a cybersecurity strategy is aligned with organizational goals and appropriate resources have been allocated.
    - Performance Measurement: Verify metrics and reporting mechanisms to track cybersecurity performance and improvement.
3. Identify Phase:
    - Asset Management: Verify that all assets (hardware, software, data) are inventoried and managed.
    - Business Environment: Ensure that the organization's position within the supply chain, critical infrastructure, and key stakeholders are identified and understood.
    - Governance: Review policies, procedures, and processes to ensure they are documented and aligned with the organization's objectives.
    - Risk Assessment: Evaluate the processes for identifying, analyzing, and prioritizing risks.
    - Risk Management Strategy: Confirm that a strategy for managing risk is established and communicated.

4. Protect Phase:
    - Access Control: Assess the mechanisms for managing access to systems and data.
    - Data Security: Verify that data are protected through encryption, masking, and other techniques.
    - Information Protection Processes and Procedures: Review the implementation of policies and procedures to protect information systems.
    - Maintenance: Ensure that systems are maintained and updated regularly.
    - Protective Technology: Check the deployment and effectiveness of security technologies (e.g., firewalls, antivirus software).
5. Detect Phase:
    - Anomalies and Events: Confirm that systems are in place to detect and report security anomalies and events.
    - Security Continuous Monitoring: Assess the continuous monitoring capabilities for identifying cybersecurity threats.
    - Detection Processes: Review processes for ensuring timely and accurate detection of cybersecurity events.
6. Respond Phase:
    - Response Planning: Verify that response plans are in place and tested regularly.
    - Communications: Ensure that communication strategies are established for internal and external stakeholders during incidents.
    - Analysis: Evaluate the processes for analyzing and mitigating cybersecurity incidents.
    - Mitigation: Assess the steps taken to contain and mitigate incidents.
    - Improvements: Check whether lessons learned from incidents are incorporated into response plans.
7. Recover Phase:
    - Recovery Planning: Confirm that recovery plans are developed and tested.
    - Improvements: Ensure that the recovery process incorporates lessons learned and improves over time.
    - Communications: Assess communication plans for informing stakeholders about recovery efforts and status.

3.6. CIS Controls v8

Conducting cybersecurity audits using the CIS (Center for Internet Security) Controls version 8 [37] involves leveraging a ranked list of recommended practices to shield organizations from prevalent cyber threats. CIS Controls v8 is intended to be adaptable and suitable for organizations of different sizes and across different industries. CIS Controls v8 is organized into 18 controls, grouped into three categories: Basic, Foundational, and Organizational. Each control consists of specific safeguards designed to mitigate security risks.

The following overview is provided on how to conduct a cybersecurity audit using CIS Controls v8:

1. Preparation and Planning:
    - Scope: Specify the audit scope, detailing which systems, processes, and departments will undergo review.
    - Gather Documentation: Collect existing policies, procedures, asset inventories, and any previous audit reports.
2. Gap Analysis:
    - Self-Assessment: Conduct a self-assessment to identify gaps between current security practices and the CIS Controls v8 requirements.
    - Map Existing Controls: Map your existing controls to the corresponding CIS Controls to understand coverage and identify gaps.

3. Implementation Review:

Basic Controls:

- Inventory and Control of Enterprise Assets: Ensure that a thorough and precise inventory is maintained of all hardware devices and software on the network.
- Data Protection: Verify that data classification, encryption, and access controls are in place to protect sensitive information.
- Secure Configuration: Assess the configuration settings of systems and software to ensure they are secure and compliant with best practices.
- Foundational Controls.
- Vulnerability Management: Review the processes for identifying, assessing, and remediating vulnerabilities.
- Malware Defenses: Check the implementation and effectiveness of antivirus and anti-malware solutions.
- Incident Response: Review the incident response plan and verify that it undergoes regular testing and updates.
- Organizational Controls.
- Penetration Testing: Ensure regular penetration test engagements are conducted to discover and rectify security vulnerabilities.
- Security Training: Review the training programs to ensure employees are aware of security policies and practices.

4. Testing and Validation:
   - Technical Testing: Perform technical tests such as vulnerability scans, configuration reviews, and penetration tests to validate the effectiveness of controls.
   - Log Review: Analyze audit logs to detect any anomalies or unauthorized access attempts.
5. Documentation and Reporting:
   - Document Findings: Record all findings, including areas of compliance and non-compliance, along with evidence supporting each finding.
   - Audit Report: Prepare a detailed audit report that summarizes the findings, provides recommendations for remediation, and highlights areas for improvement.
6. Remediation and Follow-Up:
   - Remediation Plan: Develop a plan to tackle identified gaps and weaknesses, assigning responsibilities and setting timelines for each action item.
   - Implement Changes: Implement the recommended changes to improve the cybersecurity posture.
   - Re-assessment: Conduct follow-up audits or assessments to ensure the remediation actions have been effectively implemented.

3.7. ISO/IEC 27001:2022

The International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001:2022 [38] is an internationally recognized standard for managing information security. It offers a structured method for safeguarding sensitive company information, encompassing people, processes, and IT systems to ensure its security. Conducting a security audit using ISO/IEC 27001:2022 involves several key steps to ensure that an organization's information security management system (ISMS) adheres to the standard. The following is an overview on how to conduct a cybersecurity audit using ISO/IEC 27001:2022:

1. Planning:
   - Scope: Clearly define the scope of the evaluation, which encompasses the areas, processes, and departments to be audited.
   - Obtain Documentation: Collect all necessary documentation, including ISMS policies, risk assessments, control implementations, and previous audit reports.

2. Audit Planning:
    - Plan: Create a comprehensive audit plan detailing the objectives, scope, criteria, methods, and schedule of the audit.
    - Audit Team: Select a qualified audit team with the necessary knowledge and expertise in ISO/IEC 27001:2022and information security practices.
3. Pre-Audit Activities:
    - Document Review: Review the ISMS documentation to ensure it meets the requirements of ISO/IEC 27001:2022. This includes policies, procedures, risk assessments, and control implementations.
    - Audit Checklist: Develop an audit checklist based on the requirements of ISO/IEC 27001:2022 to guide the audit process.
4. On-Site Audit:
    - Opening Meeting: Hold an initial meeting with key stakeholders to clarify the audit objectives, scope, and methodology.
    - Interviews: Interview personnel to assess their understanding and implementation of the ISMS policies and procedures.
    - Observation: Observe processes and practices to verify compliance with ISMS requirements.
    - Evidence Collection: Collect evidence through documentation review, interviews, and observations to evaluate the efficiency of the ISMS and the implementation of controls.
5. Control Testing:
    - Risk Assessment and Treatment: Verify that the organization has conducted a thorough risk assessment and implemented appropriate risk treatment plans.
    - Implementation of Controls: Check the implementation of controls from Annex A of ISO/IEC 27001:2022, ensuring they address the identified risks.
    - Effectiveness: Assess the efficacy of the controls through sampling, testing, and analysis.
6. Audit Findings and Reporting:
    - Document Findings: Record all audit findings, including areas of compliance, non-compliance, and opportunities for improvement.
    - Non-Conformities: Identify any non-conformities and classify them as major or minor based on their impact on the ISMS.
    - Audit Report: Compile a comprehensive audit report that outlines findings, including strengths, weaknesses, non-conformities, and recommendations for enhancement.
7. Closing Meeting:
    - Present Findings: Conduct a closing meeting with key stakeholders to present the audit findings and discuss any non-conformities and recommendations.
    - Agree on Actions: Agree on the actions to be taken to address non-conformities and improve the ISMS.
8. Post-Audit Activities:
    - Corrective Actions: Develop and implement corrective actions to address the identified non-conformities.
    - Follow-Up Audit: Perform subsequent audits to verify the implementation and effectiveness of corrective actions.
    - Continual Improvement: Use the audit findings to drive continual improvement of the ISMS, ensuring ongoing compliance with ISO/IEC 27001:2022.

Leszcyna [39] presents a systematic study aimed at identifying and analyzing various cybersecurity assessment methods. The research process was structured in two main stages, focusing first on existing literature reviews and then on individual cybersecurity methods.

The literature search revealed a significant lack of comprehensive reviews, with only two identified that were limited to specific application domains. This gap in the literature motivated the second stage of the research, which identified and analyzed thirty-two distinct cybersecurity assessment methods based on predefined selection and evaluation criteria. This study's findings, grouped into categories related to the evaluation criteria, provide insights into the methods' purpose, structure, and applicability characteristics, highlighting important gaps in their practical application. The research concluded that, while a large number of cybersecurity assessment methods exist, their practical application in real-world operational contexts is limited. Many methods are confined to pilot or demonstration sites, hypothetical scenarios, or preliminary configurations. This study identified several areas needing improvement, such as detailed documentation, evidence of practical use, and the development of supporting tools. The researchers also emphasized the necessity of following structured evaluation methodologies that employ criteria, metrics, and repeatable procedures. Future research directions include better documentation, enhanced evaluation procedures, and the creation of efficient tools to support the application of these methods. The overall goal is to bridge the gap between theoretical proposals and practical implementation to enhance cybersecurity assessment practices effectively.

Antunes et al. [40] explore the implementation of an information security and cybersecurity management project in fifty SMEs located in central Portugal. Using the ISO-27001:2013 [41] standard as a framework, the project was a collaborative effort involving a local business association, the Polytechnic of Leiria, and an IT auditing/consulting team. The study details the methodology applied and the resulting improvements in the participating SMEs' cybersecurity posture. The results indicate significant benefits, including enhanced information security management and increased cyber awareness among employees. This case study underscores the importance of tailored cybersecurity initiatives for SMEs, which are often vulnerable due to limited resources and awareness.

Slapnicar et al. [42] aim to analyze how effective internal cybersecurity audits are in managing cyber risks within organizations. The researchers developed a Cybersecurity Audit Index, which includes three main dimensions: planning, performing, and reporting. Their hypothesis was that the effectiveness of cybersecurity audits is positively related to the maturity of cyber risk management and inversely related to the probability of successful cyber attacks. This study involved a survey of auditors and Chief Audit Executives from various countries and industries, revealing significant variability in the effectiveness scores. The findings show that, while planning and performing phases are strongly correlated, they are less connected to the reporting phase. This study also found that higher Cybersecurity Audit Index scores are associated with greater maturity in cyber risk management but do not significantly reduce the likelihood of successful cyber attacks. This research is pioneering in comprehensively measuring the effectiveness of cybersecurity audits and provides valuable insights for improving cybersecurity practices and audit processes.

Antunes et al. [43] propose a flexible, web-integrated auditing system designed to meet the distinct needs of both SMEs and larger enterprises. The system aims to address the limitations of existing tools, which often lack flexibility and are tailored to specific standards, making them less suitable for heterogeneous enterprises. This new framework allows for the application of multiple standards and frameworks within the same auditing process, increasing its flexibility and adaptability. The proposed system was tested on fifty SMEs using the ISO 27001:2013 standard, demonstrating its effectiveness in collecting, storing, and analyzing auditing data. The system's architecture, based on a relational database and customizable checklists, ensures that it can accommodate various standards and streamline the auditing process. The results highlight significant improvements in the cybersecurity posture of the participating SMEs, validating the system's practical applicability and effectiveness in real-world scenarios.

The Integrated Framework for Cybersecurity Auditing presented emphasizes the need for a unified tool to perform cybersecurity audits due to the increasing frequency of cyberattacks on organizations. The proposed framework aims to streamline the cyber-

security auditing process by providing information systems auditors and cybersecurity professionals with a comprehensive set of controls, tools, and techniques. This integrated approach helps in identifying cybersecurity gaps and generating output reports that specify these vulnerabilities. The framework not only assists in securing organizations but also offers a mechanism for cybersecurity auditors to enhance their skills and effectively achieve auditing tasks [44]. Furthermore, the framework addresses various types of threats and risks, aligning with recent technologies and cybersecurity functions. It is designed to be adaptable to different organizational contexts, ensuring that auditors can tailor the audit process to specific needs and environments. By incorporating recognized software and tools such as Computer-Assisted Audit Technique (CAAT) and Generalized Audit Software (GAS), the framework enhances the efficiency and effectiveness of audits. This approach helps in automating various audit tasks and reducing the time and effort required for comprehensive cybersecurity evaluation.

Bozkus et al. [45] highlight the significant role of internal auditors in the context of cybersecurity. They emphasize that internal auditors must understand the full impact of cyber threats on the organization and include these risks in their risk-based audit plans. Auditors should be proactive in identifying emerging cybersecurity risks and have a strong partnership with the Chief Information Officer (CIO) or Chief Information Security Officer (CISO) to assess third-party service providers. Moreover, auditors should not only assess compliance with cyber-related policies but also provide assurance on the organization's overall cybersecurity program, incident response, disaster recovery, and business continuity plans. They should offer an independent review of the cybersecurity strategy before the development of policies and procedures and be involved in technology project implementation teams to ensure cyber risks are addressed from the outset. Internal auditors can contribute by benchmarking and testing the adequacy of policies against applicable frameworks, evaluating training outcomes, and ensuring alignment with the business strategy. By doing so, they help in coordinating plans and engaging management and the board in forward-looking discussions about cyber vulnerabilities.

Osipov et al. [46] discuss the implementation and effectiveness of machine learning (ML) methods for speech emotion recognition within telecommunication systems, primarily focusing on combating phone fraud. Global losses due to phone fraud in 2022 amounted to approximately USD 53 billion, prompting the need for advanced detection methods. The research identifies that men under 44 are the most susceptible to phone scams, which narrows the target demographic for the study. Utilizing a combination of polygraph data and smart bracelet readings, the researchers developed a wavelet-modified capsular neural network, 2D-CapsNet, to identify emotional states such as panic stupor during phone interactions. The neural network achieved classification accuracy metrics such as 86% accuracy, 84% precision, 87.5% recall, and an F-score of 85.7% when detecting these states through photoplethysmogram (PPG) readings. This study underscores the potential for real-time fraud detection by synchronizing smart bracelets with smartphones to monitor emotional states during phone calls. The method shows promise for integration into cyber-physical systems to detect and prevent fraudulent activities. However, limitations include reduced accuracy during physical activities like walking or running, highlighting the need for further refinement in PPG data preprocessing. Overall, this research demonstrates significant progress in using machine learning and neural networks to enhance telecommunication security by leveraging physiological data to identify and respond to fraudulent activities promptly.

Tsapin et al. [47] explore the integration of machine learning techniques to enhance the security of industrial robotic systems. The study emphasizes the growing need for robust security measures in environments wherein industrial and logistics robots operate, especially given the rising crime rates and challenges in identifying perpetrators in the Russian Federation. The authors focus on utilizing an ensemble of computer vision algorithms combined with the mathematical framework of convolutional neural networks (CNNs) to detect emergency situations in parking lots through mobile robots. The paper

presents the development and training of CNN models based on architectures such as MobileNetV2, ResNet50, and DenseNet121, incorporating Squeeze-and-Excitation blocks to improve accuracy. These enhanced models demonstrated accuracy improvements of 2–3%, achieving up to 92%. In the second phase of the research, the authors tested the performance of the trained neural networks under challenging conditions, such as low-light and adverse weather, which are common in real-world scenarios. The DenseNet121 + SE model, in particular, showed significant promise, maintaining an accuracy of 86% even in difficult conditions, while also being 40% faster than traditional methods. The study underscores the practical implications of these models in real-time applications, highlighting their potential to improve the safety and security of parking facilities by identifying vandalism and other forms of vehicle damage. The research contributes to the broader field of industrial security by demonstrating how advanced machine learning techniques can be effectively applied to enhance the capabilities of mobile robotic systems in monitoring and ensuring the safety of civilian facilities that can ultimately be audited under the critical infrastructure protection domain.

Putrus [48] emphasizes the transformative impact of artificial intelligence (AI) across various domains of cybersecurity. In information security, AI enhances threat detection, intrusion prevention, malware detection, and phishing detection, thereby strengthening an enterprise's overall security posture. In cloud security, AI's swift processing capabilities enable real-time threat detection, anomaly detection, and predictive security analytics. These AI applications in governance, risk, and compliance (GRC) improve risk assessment, fraud detection, compliance monitoring, and incident response. Additionally, within Security Operations Centers (SOCs), AI optimizes threat detection, incident response, automated triage, and adaptive security measures. The paper underscores the necessity of integrating AI with human expertise and governance to ensure effective and ethical cybersecurity practices. AI's implementation in cybersecurity also introduces challenges, such as data dependency, susceptibility to adversarial attacks, and the risk of overreliance. The complexity of deep learning models can complicate the understanding and addressing of potential issues, while scaling AI solutions face hurdles in complex environments and regulatory compliance. The paper advocates for a holistic approach that merges AI with human expertise and robust governance, alongside continuous monitoring to effectively combat evolving cyber threats. While AI can significantly enhance cybersecurity capabilities, it is not a replacement for human intelligence. Human oversight, context-aware analysis, and ethical considerations remain indispensable components of an effective cybersecurity defense strategy, ensuring AI's responsible and beneficial deployment in combating cyber threats.

ISACA [49] delves into the application of the Digital Trust Ecosystem Framework (DTEF) in ensuring the trustworthiness of AI technologies. The DTEF provides a comprehensive structure to evaluate and manage the risks associated with emerging technologies, including AI. It emphasizes the need for robust governance throughout the AI lifecycle, from design and development to deployment and monitoring. By integrating digital trust principles, the framework aims to help organizations navigate the complexities of AI adoption, ensuring quality, resilience, transparency, security, privacy, ethics, and integrity. The document highlights the pervasive influence of AI across various industries, such as healthcare, financial services, and energy, where it enhances efficiency and sustainability. It also addresses the challenges posed by the widespread use of generative AI and the evolution of shadow IT, where unauthorized AI applications may be used by employees. The DTEF guides organizations in aligning AI strategies with business objectives, ensuring compliance with legal and regulatory requirements, and maintaining human oversight to manage ethical considerations. Ultimately, the framework supports organizations in achieving trustworthy AI that complements human capabilities and positively contributes to societal and business outcomes.

4. The CyberSecurity Audit Model (CSAM 2.0)

The CyberSecurity Audit Model (CSAM 2.0) [50] is an extensive model created to evaluate cybersecurity assurance within any organization. It also offers specific guidance for nation-states looking to establish a National Cybersecurity Strategy (NCS) or evaluate the efficiency of an existing one. CSAM 2.0 is versatile, suitable for both internal and external cybersecurity audits, and supports single or multi-domain audits. It includes 18 domains, of which Domain 1 is designed for nation-states, while Domains 2–18 are applicable to any organization. The initial version of CSAM, released in February 2017, featured an overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessments, and an evaluation scorecard.

CSAM 2.0 was released in June 2023 and introduced significant updates:

- Twelve new cybersecurity domains were added.
- Physical security audits were included.
- Audits for Industrial and Manufacturing Control Systems were introduced.
- CyberSecurity Education, Training, and Awareness (CSETA) can now be audited within organizational programs.
- Vendor and supply chain security audits were added.
- Software development security audits were included.
- Additional areas such as cloud security, penetration testing, and Security Operations Center (SOC) audits were incorporated.

CSAM 2.0 encompasses an overview, methodology, resources, 30 domains, 38 sub-domains, 99 checklists, 225 controls, 549 sub-controls, 80 guideline assessments, and an evaluation scorecard.

We propose to test the following hypotheses:

H1: *Selecting specific cybersecurity domains can help auditors to better plan and conduct cybersecurity audits.*

By selecting specific cybersecurity domains, auditors can focus their efforts on key areas that are most relevant to the organization's cybersecurity posture. This targeted approach ensures that all critical aspects of cybersecurity are covered without unnecessary overlap or omission. Specific domains provide a clear framework, helping auditors to systematically address each area. This structure aids in efficient resource allocation, reducing the time and effort required for the audit.

Different organizations face different cybersecurity challenges based on their industry, size, and complexity. Selecting specific domains allows the audit to be customized to the organization's unique needs, making the findings more relevant and actionable.

H2: *Auditing cybersecurity controls will detect weaknesses or strengths of safeguards to protect organizational assets.*

Auditing cybersecurity controls involves evaluating the effectiveness of existing safeguards. This process helps identify gaps and vulnerabilities that could be exploited by cyber threats. For instance, an audit may reveal that certain controls are outdated, improperly configured, or not in compliance with current security standards, exposing the organization to risk.

In addition to finding weaknesses, auditing also highlights areas wherein the organization's cybersecurity controls are strong. Recognizing these strengths can reinforce confidence in current practices and inform strategic decisions. Effective controls identified during the audit can be documented as best practices and potentially scaled across other parts of the organization.

By regularly auditing cybersecurity controls, organizations can proactively manage risks rather than reacting to incidents after they occur. This proactive approach helps in maintaining a robust security posture. Audits can also identify emerging threats and

evolving vulnerabilities, allowing organizations to adapt their controls to stay ahead of potential attacks.

The CyberSecurity Audit Model (CSAM 2.0) significantly contributes to knowledge by providing a comprehensive framework for evaluating the effectiveness of cybersecurity audits. It does so by integrating key dimensions such as planning, performing, and reporting within the audit process. This model helps in systematically assessing the maturity of cyber risk management practices and their impact on reducing the likelihood of successful cyber attacks. Furthermore, CSAM 2.0 addresses the need for a structured approach to cybersecurity auditing, which is crucial given the evolving nature of cyber threats. By incorporating elements from widely recognized cybersecurity frameworks like ISO 27001, COBIT, and NIST, the model ensures consistency and comprehensiveness in the audit process. It also highlights the importance of continuous improvement and adaptation in cybersecurity practices, urging organizations to keep their audit plans dynamic and responsive to emerging risks. The model's detailed documentation and empirical validation make it a valuable resource for auditors, risk managers, and policymakers aiming to enhance their understanding and implementation of effective cybersecurity measures.

Table 1 highlights strengths and weaknesses between CSAM 2.0 and other globally accepted frameworks, standards, best practices and benchmarks that can be adopted for conducting cybersecurity audits.

Table 1. Comparison between CSAM 2.0 and other cybersecurity frameworks.

Frameworks	Strengths	Weaknesses
CSAM 2.0	- Comprehensive and adaptable to various organizational environments. - Includes 30 cybersecurity domains and detailed checklists, controls, and sub-controls. - Tailored for both partial and complete audits. - Effective in specific sectors like higher education.	- Newer model with limited widespread adoption. - Initial implementation may require more resources and training.
NIST SP 800-53 Rev. 5	- Extensive and detailed set of controls for security and privacy. - Widely recognized and adopted, especially in American federal agencies. - Emphasizes integration with the broader risk management framework like the Risk Management Framework (RMF).	- Can be complex and resource-intensive to implement on full-scale implementations. - Less flexible for smaller organizations or those outside the American federal space.
SOC 2	- Focuses on security, availability, processing integrity, confidentiality, and privacy. - Widely trusted by service organizations. - Offers Type I and Type II reports to assess design and operational effectiveness of controls.	- Primarily applicable to service organizations. - May not cover all aspects needed for comprehensive cybersecurity audits in diverse industries.
SOC for Cybersecurity	- Evaluates and reports on cybersecurity risk management programs. - Organized into governance, risk assessment, risk management, information, communication, and monitoring. - Helps communicate cybersecurity posture to stakeholders.	- Still relatively new, with less adoption compared to SOC 2. - More focused on reporting rather than comprehensive auditing.
PCI DSS v4.0	- Specific and rigorous standards for protecting payment card data. - Focuses on continuous compliance and stronger security measures. - Well-defined process for scoping, assessment, and reporting.	- Narrowly focused on the global payment card industry. - May not be fully applicable to organizations outside this industry.

Table 1. *Cont.*

Frameworks	Strengths	Weaknesses
NIST CSF 2.0	- Flexible framework applicable to various industries and sectors. - Focuses on identifying, protecting, detecting, responding, and recovering. - Encourages continuous improvement and alignment with business needs.	- High-level guidance may require additional detailed frameworks for specific controls. - Implementation complexity can vary depending on the organization's maturity.
CIS Controls v8	- Prioritized and actionable set of controls. - Suitable for organizations of all sizes. - Emphasizes basic, foundational, and organizational controls.	- May require integration with other frameworks for comprehensive auditing. - Focused more on best practices than formal compliance.
ISO/IEC 27001:2022	- Internationally recognized standard for information security management. - Emphasizes continuous improvement and risk management. - Suitable for organizations seeking formal certification.	- Certification process can be lengthy and resource intensive. - May require integration with more specific cybersecurity controls and frameworks for comprehensive audits.

CSAM 2.0 emerges for its comprehensive and adaptable approach when planning and conducting cybersecurity audits, tailored to specific organizational environments and allowing for the integration of detailed controls organized by domains. In contrast, frameworks like NIST SP 800-53 R5 and ISO/IEC 27001:2022 offer extensive, exhaustive controls but can be complex and resource-intensive. SOC 2 and SOC for Cybersecurity focus on service organizations and risk management, respectively, while PCI DSS v4.0 is highly specific to the global payment card industry. NIST CSF 2.0 provides flexible, high-level guidance, and CIS Controls v8 offers prioritized, actionable controls, though both may need integration with other frameworks for comprehensive auditing. Most of the existing cybersecurity frameworks are not conceived to enact cybersecurity auditing tasks, which creates superb advantages when using CSAM 2.0 for cybersecurity audits.

5. Methodology

The goal of these case studies was to implement and validate the chosen domains of the CyberSecurity Audit Model (CSAM 2.0). This practice serves as a robust framework for tackling issues in planning and conducting cybersecurity audits. While case studies are valuable for their relevance as observational studies, their findings may have limited applicability and broader implications. Following this, we developed, executed, and validated a case study using Yin's methodology [51] involving three exercises: conducting a comprehensive cybersecurity audit in three distinct Canadian higher education institutions. To protect the confidentiality and anonymity of these institutions and their participants, specific details cannot be disclosed. Our primary challenge was conducting comprehensive and timely cybersecurity audits, ensuring the inclusion of appropriate domains. Our objective was to create a comprehensive model for planning and conducting cybersecurity audits across any organization, with the ability to evaluate national cybersecurity strategies as well. Additionally, we identified a significant gap in knowledge about handling cyberattacks and cyberthreats, leading to the development of an organizational cybersecurity awareness training model foundational for any cybersecurity awareness program. The validation of CSAM 2.0 was expanded to include a second and third larger institution to confirm the effectiveness and reliability of the model, addressing the initial shortcomings observed in the initial target organization. We engaged with upper management of our target organizations and proposed our case study research. We conducted a cybersecurity pre-assessment to evaluate the current cybersecurity posture of the organization, intending to implement CSAM 2.0 similarly to our initial study [13]. These case studies were perceived as mutually beneficial by the institutions and the researchers. Data were gathered through interviews, observations, online surveys, and documentation pertinent to the

scope of the case studies. In the pre-assessment phase, the lead researcher collected data from managers, IT staff, InfoSec personnel, and senior executives through online surveys. During cybersecurity audits, evidence was gathered based on our application of CSAM 2.0, categorized according to cybersecurity domains. During the data collection phase, evidence was gathered from various sources including documents, policies, archival records, open-ended interviews, observations, structured interviews, surveys, site visits, presentations, meetings, and computer and server logs. Researchers liaised with relevant authorities to secure research data, and an internal lead project manager from each institution allocated personnel for the research case studies. The gathered data were analyzed using CSAM 2.0 indicators, employing diverse methods for data analysis. Information was documented in control forms, sub-control forms, and checklists for each audited cybersecurity domain and sub-domain.

To enhance the research methodology, a mixed-methods approach was adopted, combining quantitative and qualitative data collection and analysis to provide a comprehensive evaluation of CSAM 2.0's effectiveness across different organizational contexts.

5.1. Quantitative Analysis

Structured online surveys, questionnaires, and checklists were deployed across a diverse sample of organizations implementing CSAM, assessing the adoption extent, domain coverage comprehensiveness, and measurable improvements in cybersecurity posture before and after implementation. Statistical tools were used to analyze the data, identifying trends and correlations between CSAM 2.0 implementation and cybersecurity outcomes.

5.2. Qualitative Analysis

In-depth interviews, observations, and focus groups with cybersecurity professionals experienced with CSAM 2.0 provided insights into practical challenges and benefits, areas for improvement, and recommendations for future updates. Case studies illustrated the real-world application and impact of CSAM 2.0.

5.3. Continuous Feedback Loop

A continuous feedback loop was established to regularly incorporate field insights into CSAM 2.0 updates, involving periodic surveys and interviews post-implementation to capture ongoing user experiences and emerging cybersecurity challenges, refining CSAM 2.0 to remain robust and adaptive to evolving cyberthreats.

By integrating these methodologies, the research aimed to provide a comprehensive evaluation of CSAM 2.0, ensuring that it remains a relevant and effective tool for enhancing cybersecurity across various organizational contexts. The research methodology involved three Canadian higher education institutions (CHEI 1, CHEI 2, and CHEI 3) to validate the implementation, data validation, and outcomes of the CSAM 2.0 cybersecurity audit model, with results and discussion presented in subsequent sections of this study.

6. Results

CSAM 2.0 was implemented and validated in three distinct Canadian higher education institutions (CHEI1-CHEI3) across different time periods. The initial target organization features a central campus with over 200 employees and an annual student enrollment exceeding 4000. The cybersecurity responsibilities are overseen by the IT department. The second target organization operates from a central campus with six additional locations across six different cities. It employs over 700 staff members and serves more than 17,500 students annually. The cybersecurity operations are managed by the Information Security department. The final target organization includes a central campus with three satellite campuses, catering to more than 15,000 students annually and employing over 2500 staff members. The cybersecurity responsibilities are jointly managed by the IT and cybersecurity departments.

The evaluation methodology encompasses the following steps for auditing each cybersecurity domain:

1. Obtain the average of control evaluations by domain/sub-domain.
2. Calculate the average of sub-controls for each checklist.
3. Combine the results from Steps 1 and 2 to derive an overall average.
4. The outcome from Step 3 provides the percentage representing the audited cybersecurity domain.

Key findings include the following:

- Successful validation of CSAM 2.0 through comprehensive cybersecurity audits structured by domains across three distinct organizations.
- Presentation of audit recommendations to upper management of the target institutions to enhance their cybersecurity posture.
- Demonstration of CSAM 2.0's efficacy in assessing cybersecurity assurance and maturity levels.

Next, we will illustrate how the audit for a specific cybersecurity domain was conducted. We start by identifying the target organization and the audited domain. In this case, it pertains to our second target organization (Canadian higher education institution #2—CHEI2) and the specific CSAM 2.0 domain, which is CSAM 2.0 Domain #5 (Cyber Risks). This domain includes one sub-domain, also named Cyber Risks but coded as 5.1, covering five clauses from 5.1.1 to 5.1.5. As shown in Figure 1, the initial verification score for this domain was 80%. This percentage will be instrumental later in calculating the overall ranking and maturity score for the fifth CSAM 2.0 domain.

Reference	Sub Area	Clause	Steps	Control Evaluation	
				Yes	No
5.1	Cyber Risks	5.1.1	The organization has implemented cyber risk management	☑	☐
		5.1.2	The organization has established a clear information asset classification	☐	☑
		5.1.3	Cybersecurity controls have been implemented to mitigate risks to acceptable levels	☑	☐
		5.1.4	The organization identifies cyber risks by considering ocurrence and impact	☑	☐
		5.1.5	The cyber risk management contains defined goals and objectives	☑	☐

Figure 1. Evidence to verify the main controls for CSAM 2.0 Domain #5.

Furthermore, the next stage involved verifying the existing cybersecurity controls for how the organization managed its cyber risk function. The sub-domain "Cyber Risks" comprises 10 sub-controls detailed in the "Cybersecurity Audit Checklist: CSAM 2.0—Cyber Risks". This checklist evaluates the effectiveness of cybersecurity sub-controls based on main clauses (5.1.1 to 5.1.5), organized as follows:

- Clause 5.1.1: Subcontrols 1, 2, 3, 6, 7, and 8;
- Clause 5.1.2: Subcontrol 9;
- Clause 5.1.3: Subcontrol 4;
- Clause 5.1.4: Subcontrol 5;
- Clause 5.1.5: Subcontrol 10.

The audit outcome categorizes cybersecurity effectiveness into compliant (fully implemented controls), major nonconformity (lack of controls), or minor nonconformity (partially implemented or not fully executed controls), as depicted in Figure 2. The score for this checklist is 40% due to the limited number of fully implemented sub-controls meeting CSAM's criteria for assessing cyber risk controls. Finally, combining the initial control and sub-control values yields a final score of 60% for CSAM 2.0 Domain 5.

To present the results of our case study research, we will refer to the target organizations using the indicators CHEI1, CHEI2, and CHEI3.

Clause	No.	Checklist Questions	Findings		
			Compliant	Minor Nonconformity	Major Nonconformity
5.1.1	1	Does the organization define risk scope and boundaries?	☐	☐	☐
5.1.1	2	What criteria is used to assess cyber risks?	☐	☐	☐
5.1.1	3	What methodology is used to deal with identified risks?	☐	☐	☐
5.1.3	4	How do you manage residual risks?	☐	☐	☐
5.1.4	5	What procedures are in place to manage risk acceptance?	☐	☐	☐
5.1.1	6	Are there any risk communication and consultation processes?	☐	☐	☐
5.1.1	7	Do you have procedures for risk monitoring?	☐	☐	☐
5.1.1	8	How often do you review your risk management processes?	☐	☐	☐
5.1.2	9	What criteria was used to define your cyber asset classification?	☐	☐	☐
5.1.5	10	What are the goals and objectives of your cyber risk management?	☐	☐	☐

Figure 2. Checklist to verify cybersecurity controls for the cyber risk domain.

The audit findings classify cybersecurity controls into compliant, minor nonconformity, or major nonconformity categories. Table 2 outlines the criteria for evaluating these categories.

Table 2. CSAM 2.0 auditing findings for control assessments.

Audit Findings	Description	Examples
Compliant	The control requirements have been verified and are following the acceptable criteria	- Cybersecurity awareness training was properly documented, delivered, and evaluated
Minor nonconformity	An abnormal situation where some aspects of the control requirements have not been fulfilled	- Some inconsistencies have been found in any security report - Some InfoSec procedures have not been reviewed and updated according to the company's time frame
Major nonconformity	Failure to comply with control requirements	- Lack of upper management commitment to any major security project - Absence of the main corporate cybersecurity policy

Table 3 displays the cybersecurity maturity level for each domain and the overall maturity rating for each CHEI.

Table 3. Cybersecurity maturity rating of all participating institutions.

Nº	Domain	CHEI #1	CHEI #2	CHEI #3
1	Governance and Strategy	35%	42%	85%
2	Legal and Compliance	90%	100%	100%
3	Cyber Assets	30%	80%	75%
4	Cyber Risks	60%	70%	100%

Table 3. *Cont.*

N°	Domain	CHEI #1	CHEI #2	CHEI #3
5	Frameworks and Regulations	30%	90%	96%
6	Architecture and Networks	67%	80%	68%
7	Information, Systems and Applications	55%	87%	60%
8	Vulnerablity identification	30%	100%	74%
9	Threat Intelligence	60%	95%	90%
10	Incident Management	10%	92%	90%
11	Digital Forensics	30%	85%	50%
12	Awareness Education	60%	95%	80%
13	Cyber Insurance	91%	85%	100%
14	Active Cyber Defense	5%	60%	85%
15	Evolving Technologies	100%	80%	80%
16	Disaster Recovery	30%	89%	90%
17	Personnel	7%	85%	80%
Cybersecurity Maturity Ratiing		**51%**	**83%**	**83%**

Overall Maturity Ratings:

CHEI #2 and CHEI #3 both have high overall maturity ratings of 83%, indicating strong cybersecurity postures.

CHEI #1 has a significantly lower maturity rating of 51%, indicating that there are substantial areas for improvement.

Domain-Specific Performance:

Governance and Strategy: CHEI #1 scores particularly low (35%) compared to CHEI #3 (85%), indicating potential weaknesses in leadership and strategic planning for cybersecurity.

Legal and Compliance: CHEI #1 scores 30%, significantly lower than CHEI #3 (100%). This suggests that CHEI #1 may not be fully compliant with legal and regulatory standards.

Cyber Risks and Threat Intelligence: CHEI #1 shows low scores in these domains (40% and 10%, respectively), which are crucial areas for maintaining cybersecurity readiness.

Incident Management: Both CHEI #2 and CHEI #3 score above 90%, while CHEI #1 is at 10%, suggesting a severe gap in handling and responding to incidents.

Cyber Insurance: CHEI #1 scores highest (91%) while CHEI #2 scores 0%, highlighting a potential lack of risk transfer strategies at CHEI #2.

Areas of Strength:

CHEI #3 demonstrates strong performance across several domains, notably in Cyber Risks, Frameworks and Regulations, Information Systems and Applications, and Incident Management.

CHEI #2 also demonstrates strong performance but lacks Cyber Insurance coverage, which is critical for risk management.

Areas for Improvement:

CHEI #1 needs substantial improvements across multiple domains, especially in Governance and Strategy, Legal and Compliance, Incident Management, and Threat Intelligence.

CHEI #2 should consider implementing Cyber Insurance to complete its risk management strategy.

The recommendations can be seen in Figure 3.

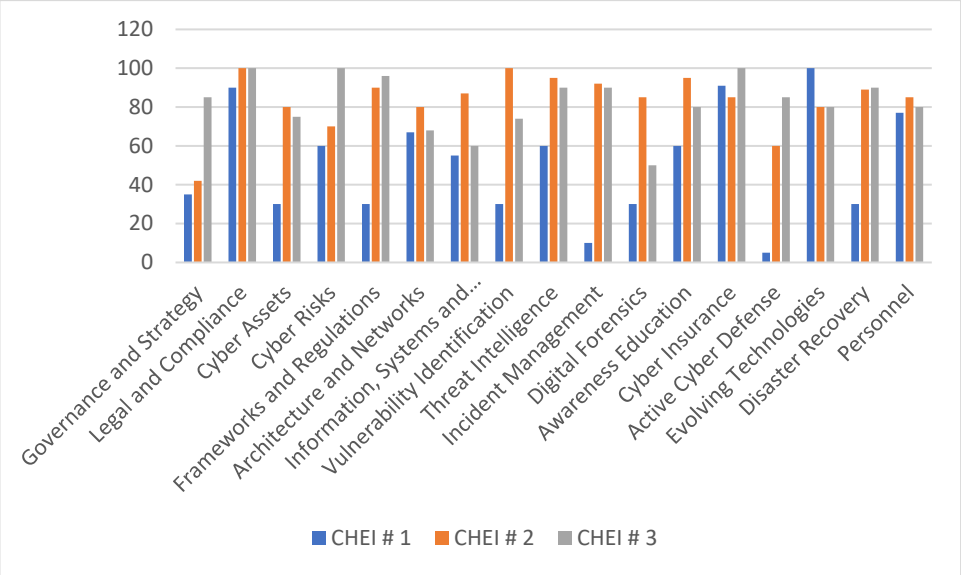

Figure 3. Institutional cybersecurity readiness comparison.

Targeted Improvement Plans:

CHEI #1 should focus on enhancing its governance framework, compliance measures, incident management capabilities, and threat intelligence processes.

CHEI #2 should look into obtaining cyber insurance to mitigate financial risks from cyber incidents.

Continuous Monitoring and Auditing:

All institutions should continuously monitor their cybersecurity posture and conduct regular audits using CSAM 2.0 to ensure that they adapt to the evolving threat landscape (Figure 4).

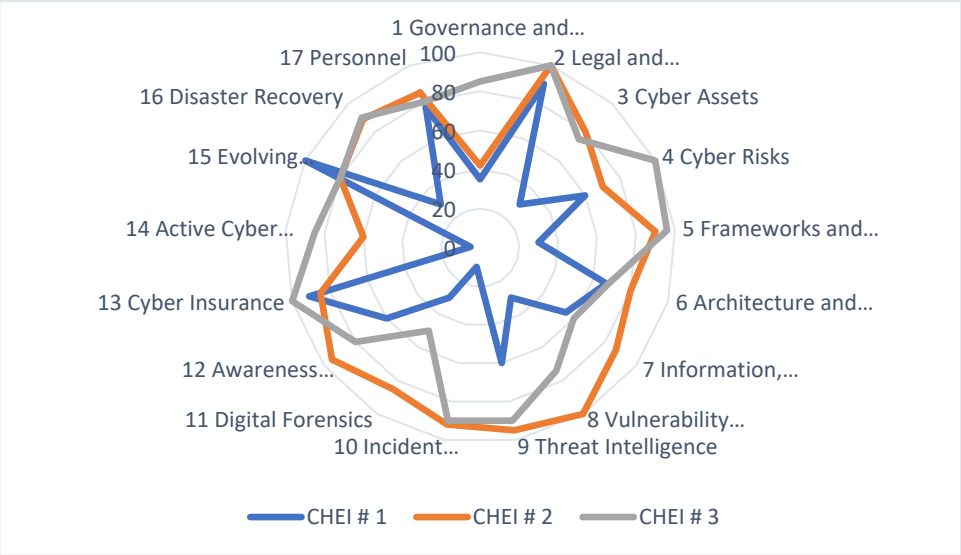

Figure 4. Radar evaluation of cybersecurity across CHEIs.

Cybersecurity Training and Awareness:

It is crucial to implement continuous training programs to ensure all personnel are fully aware of their roles and responsibilities in maintaining cybersecurity. This is particularly crucial for CHEI #1 to improve its scores in Personnel and Awareness Education.

By addressing these recommendations, institutions can significantly enhance their cybersecurity maturity and resilience against potential cyber threats.

Table 4 provides cybersecurity domain scores, their corresponding domain magnitudes (DMs), and the overall cybersecurity maturity ratings for three Canadian higher education institutions (CHEIs) where CSAM 2.0 was implemented. Domain magnitude (DM) reflects the importance or impact of each domain on the overall cybersecurity maturity rating.

Table 4. Cybersecurity domain scores with domain magnitude.

No.	Domain	CHEI #1	DM #1	CHEI #2	DM #2	CHEI #3	DM #3
1	Governance and Strategy	35	3	42	5	85	5
2	Legal and Compliance	90	5	100	5	100	5
3	Cyber Assets	30	5	80	5	75	5
4	Cyber Risks	60	5	70	5	100	5
5	Frameworks and Regulations	30	1	90	3	96	4
6	Architecture and Networks	67	5	80	5	68	5
7	Information, Systems and Applications	55	5	87	5	60	5
8	Vulnerability Identification	30	1	100	4	74	4
9	Threat Intelligence	60	1	95	3	90	4
10	Incident Management	10	2	92	4	90	4
11	Digital Forensics	30	1	85	2	50	2
12	Awareness Education	60	1	95	3	80	3
13	Cyber Insurance	91	1	85	1	100	1
14	Active Cyber Defense	5	1	60	1	85	1
15	Evolving Technologies	100	3	80	3	80	4
16	Disaster Recovery	30	5	89	5	90	5
17	Personnel	77	2	85	4	80	3
Cybersecurity Maturity Rating		**51**	**3**	**83**	**4**	**83**	**4**

Cybersecurity Assurance and Maturity Index Equation (CAMIE) for CSAM 2.0.

The CAMIE equation provides a framework for determining the index to validate the cybersecurity assurance and maturity of any CSAM 2.0 domain. Various options are available, tailored to align with the specific scope of the cybersecurity audit being conducted.

$$\text{CAMIE for all CSAM 2.0 domains} = \left[\left(\sqrt{D1^2} * \text{DM1}\right) + \cdots + \left(\sqrt{D30^2} * \text{DM30}\right)\right]/30 \quad (1)$$

$$\text{CAMIE for one CSAM 2.0 domain} = \sqrt{D1^2} * \text{DM1} \quad (2)$$

$$\text{CAMIE for two CSAM 2.0 domains} = \left[\left(\sqrt{D1^2} \ * \text{DM1}\right) + \left(\sqrt{D2^2} * \text{DM2}\right)\right]/2 \quad (3)$$

$$\text{CAMIE for 7 CSAM 2.0 domains} = \left[\left(\sqrt{D1^2} * \text{DM1}\right) + \cdots + \left(\sqrt{D7^2} * \text{DM7}\right)\right]/7 \quad (4)$$

CAMIE can be calculated using the final ratings obtained after a cybersecurity audit, based on CSAM Domain results. The domain magnitude (DM) from Table 5 is assigned by each organization to audited domains based on their criticality. For example:

Table 5. CSAM 2.0 domain criticality.

Domain Magnitude (DM)	Values	Description
Very High	5	CSAM domain is very critical for business operations
High	4	CSAM domain is critical for business operations
Moderate	3	CSAM domain could trigger a serious adverse effect on business operations
Low	2	CSAM domain could trigger a limited adverse effect on business operations
Very Low	1	CSAM domain could trigger an adverse effect on business operations

Moreover, the Cybersecurity Assurance and Maturity level can be determined as follows:

For the Nation-States domain (CSAM D1), calculate the final cybersecurity maturity rating.

For domains 2–18 (CSAM 2.0 D2-D18) in any organization, use the following criteria to map the score to a specific maturity level:

Inexistent (I): 0

Cybersecurity capabilities are not present.

Immature (Im): 1–125

The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are non-existent or very weak. The organization has not implemented a comprehensive cybersecurity program.

Developing (D): 126–250

The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused on staff, processes, controls, and regulations.

Mature (M): 251–375

While the organization has a mature environment, improvements are required in the key areas that have been identified with weaknesses.

Advanced (A): 376–500

The organization has excelled in implementing cybersecurity best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits.

Figure 5 illustrates the domain magnitude (DM) for all audited cybersecurity domains of all participating CHEIs.

The Cybersecurity Assurance and Maturity Equation (CAMIE) serves as a critical metric for calculating the cybersecurity maturity of any CSAM 2.0 domain. The findings from the case studies not only have implications for our target organizations but also pave the way for future research to review and enhance our cybersecurity model—CSAM 2.0. Table 6 illustrates overall positive trends in cybersecurity maturity and effectiveness across multiple domains. Significant enhancements are observed in Governance and Strategy, Cyber Risks, Frameworks and Regulations, and Incident Management. However, domains such as Digital Forensics and Awareness Education exhibit inconsistencies, highlighting areas that warrant additional focus and improvement.

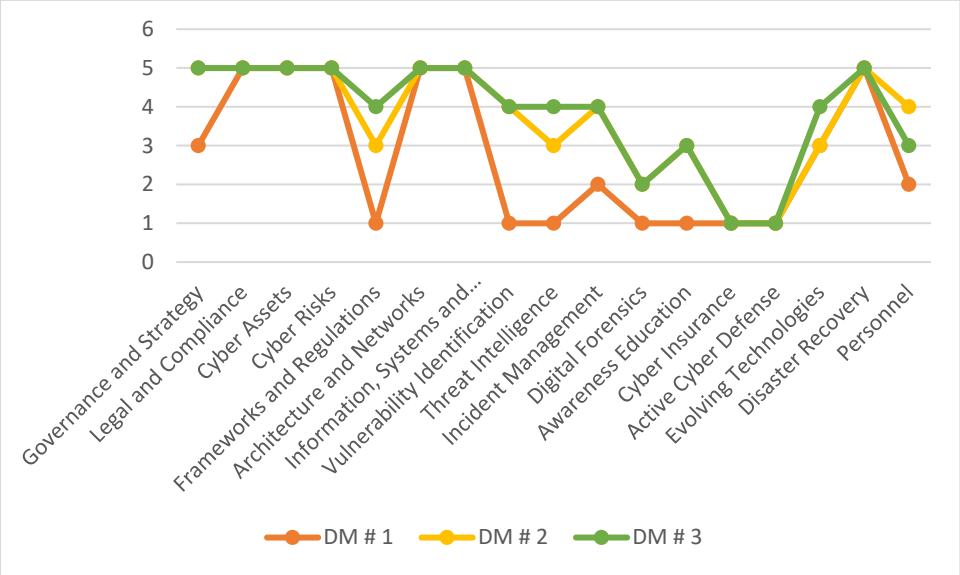

Figure 5. Comparison of audited domains in CHEIs.

Table 6. Cybersecurity domain scores with CAMIE.

No.	Domain	CHEI #1	CAMIE #1	CHEI #2	CAMIE #2	CHEI #3	CAMIE #3
1	Governance and Strategy	35	105	42	210	85	425
2	Legal and Compliance	90	450	100	500	100	500
3	Cyber Assets	30	150	80	400	75	375
4	Cyber Risks	60	300	70	350	100	500
5	Frameworks and Regulations	30	30	90	270	96	384
6	Architecture and Networks	67	335	80	400	68	340
7	Information, Systems, and Applications	55	275	87	435	60	300
8	Vulnerability Identification	30	30	100	400	74	296
9	Threat Intelligence	60	60	95	285	90	360
10	Incident Management	10	20	92	368	90	360
11	Digital Forensics	30	30	85	170	50	100
12	Awareness Education	60	60	95	285	80	240
13	Cyber Insurance	91	91	85	85	100	100
14	Active Cyber Defense	5	5	60	60	85	85
15	Evolving Technologies	100	300	80	240	80	320
16	Disaster Recovery	30	150	89	445	90	450
17	Personnel	77	154	85	340	80	240
Cybersecurity Maturity Rating		**51**	**150**	**83**	**308**	**83**	**316**

The overall cybersecurity maturity rating shows improvement from 51 to 83 based on CHEI, and from 150 to 316 based on CAMIE (Table 7), indicating overall enhanced cybersecurity effectiveness and maturity across the assessments.

Figure 6 compares the domain maturity of the audited CHEIs and their respective CAMIE values.

Figure 7 compares the results from DM and CAMIE indicators from all three participating CHEIs.

CSAM 2.0 integrates numerous cybersecurity domains that are unique and not commonly found in other cybersecurity frameworks or standards. These domains encompass the validation of controls for cyberspace, governance and strategy, compliance, cyber risk management, regulations, and threat intelligence, setting it apart from other cybersecurity frameworks and models.

Table 7. Cybersecurity domain scores with DM and CAMIE values.

No.	Domain	CHEI #1	DM #1	CAMIE #1	CHEI #2	DM #2	CAMIE #2	CHEI #3	DM #3	CAMIE #3
1	Governance and Strategy	35	3	105	42	5	210	85	5	425
2	Legal and Compliance	90	5	450	100	5	500	100	5	500
3	Cyber Assets	30	5	150	80	5	400	75	5	375
4	Cyber Risks	60	5	300	70	5	350	100	5	500
5	Frameworks and Regulations	30	1	30	90	3	270	96	4	384
6	Architecture and Networks	67	5	335	80	5	400	68	5	340
7	Information, Systems, and Applications	55	5	275	87	5	435	60	5	300
8	Vulnerability Identification	30	1	30	100	4	400	74	4	296
9	Threat Intelligence	60	1	60	95	3	285	90	4	360
10	Incident Management	10	2	20	92	4	368	90	4	360
11	Digital Forensics	30	1	30	85	2	170	50	2	100
12	Awareness Education	60	1	60	95	3	285	80	3	240
13	Cyber Insurance	91	1	91	85	1	85	100	1	100
14	Active Cyber Defense	5	1	5	60	1	60	85	1	85
15	Evolving Technologies	100	3	300	80	3	240	80	4	320
16	Disaster Recovery	30	5	150	89	5	445	90	5	450
17	Personnel	77	2	154	85	4	340	80	3	240
Cybersecurity Maturity Rating		**51**	**3**	**150**	**83**	**4**	**308**	**83**	**4**	**316**

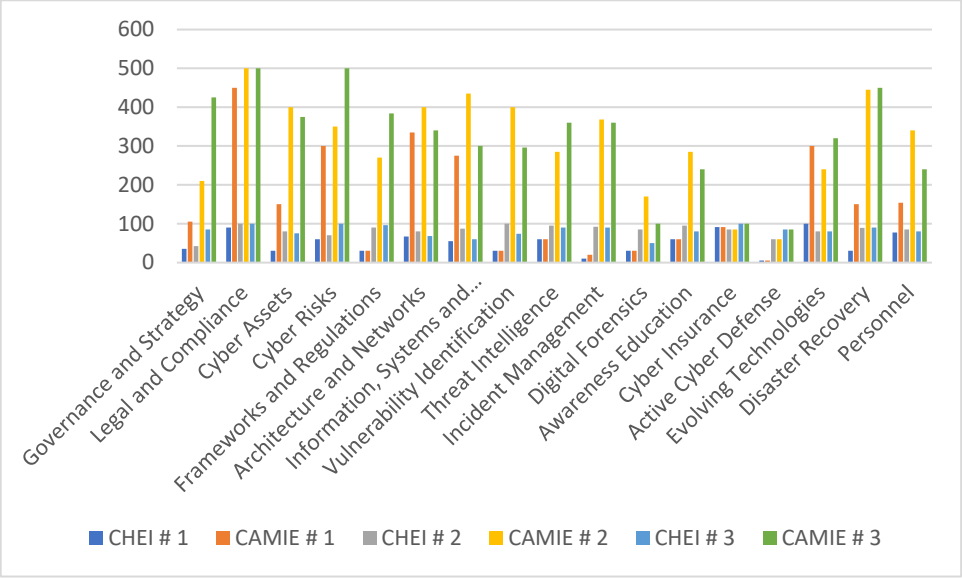

Figure 6. CHEI domain maturity using CAMIE.

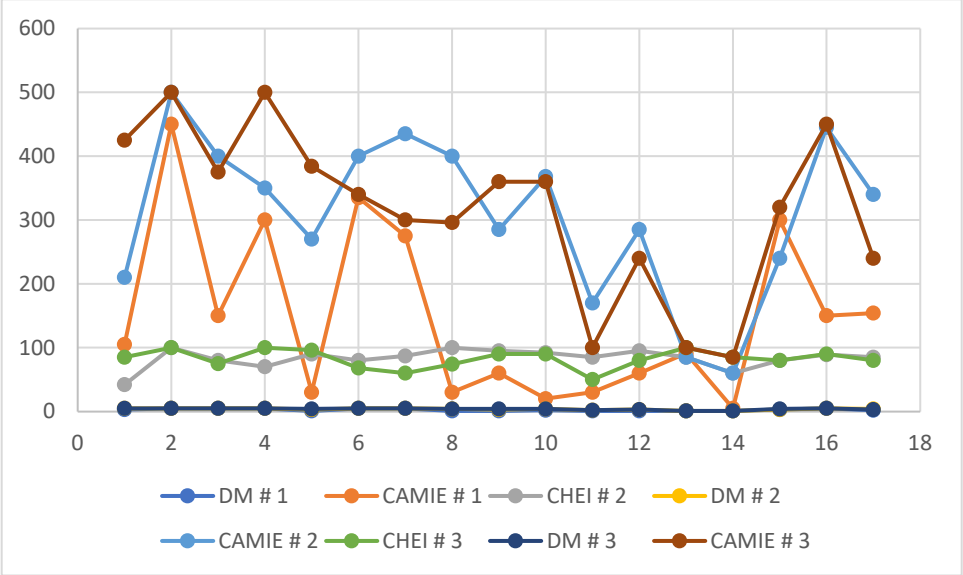

Figure 7. Comparison between DM and CAMIE.

The research presented in this paper makes significant contributions to the field of cybersecurity by empirically validating the CyberSecurity Audit Model (CSAM 2.0), an innovative and comprehensive model designed to conduct thorough cybersecurity audits across various organizational environments. Unlike existing models, CSAM 2.0 integrates multiple cybersecurity domains, offering a holistic approach to evaluating and enhancing cybersecurity controls. This framework was rigorously tested in three distinct Canadian higher education institutions, demonstrating its versatility and effectiveness in improving cybersecurity resilience by measuring the cybersecurity maturity of the target institutions. The empirical evidence gathered from these case studies underscores the model's ability to provide tailored cybersecurity strategies that address specific organizational needs, thereby contributing to a more robust and adaptive cybersecurity posture. Furthermore, this research advances the global discourse on cybersecurity by addressing the critical need for adaptable and practical audit frameworks that can evolve with the rapidly changing threat landscape. By focusing on specific domains, CSAM 2.0 offers a level of detail and comprehensiveness that is often lacking in existing audit models, making it a valuable tool for organizations aiming to enhance their cybersecurity practices. The successful validation of this model in diverse institutional contexts not only fills a significant gap in the literature but also sets a precedent for future research across various sectors. This study highlights the universal applicability of CSAM 2.0 and its potential to drive a global shift toward proactive and continuous cybersecurity risk management.

7. Discussion

This study set out to validate the CyberSecurity Audit Model (CSAM 2.0) within the context of three distinct Canadian higher education institutions. The empirical analysis demonstrated that CSAM 2.0 is effective in assessing and enhancing cybersecurity controls, highlighting its adaptability and practicality across different institutional environments. The key findings indicate that tailored cybersecurity strategies, when supported by continuous and comprehensive auditing, significantly mitigate cyber risks in higher education environments. Each institution's cybersecurity maturity rating, as derived from the CSAM 2.0 audits, provides a clear picture of their respective cyber readiness and areas requiring improvement.

The increasing sophistication and frequency of cyberattacks targeting higher education institutions necessitate robust cybersecurity frameworks. This study underscores the importance of institutions developing tailored cybersecurity strategies that reflect their unique environments. The results suggest that adopting CSAM 2.0 can lead to signifi-

cant improvements in the effectiveness of assessing cybersecurity controls. The model's flexibility allows for partial or complete audits, making it suitable for institutions with varying levels of cybersecurity maturity and resources. Moreover, the findings emphasize the necessity for continuous auditing and updating of cybersecurity practices. Higher education institutions must prioritize regular assessments to adapt to the evolving cyber threat landscape. By doing so, they can better protect sensitive academic and personal data, thus maintaining the integrity and reputation of their institutions.

While frameworks like the NIST Cybersecurity Framework (NIST CSF 2.0) [15] provide a broad approach to cybersecurity controls, they often lack detailed guidance on specific aspects such as strategy formulation and compliance. In contrast, CSAM 2.0 addresses these gaps by offering a more targeted and comprehensive approach to cybersecurity audits. This research validates CSAM 2.0's effectiveness in providing clear objectives and practical guidance for conducting both partial and complete cybersecurity audits. The comparison highlights the strengths of CSAM 2.0 in terms of its adaptability and ease of implementation across different domains and organizational sizes. This makes it a valuable tool for higher education institutions seeking to enhance their cybersecurity posture systematically and methodically.

This study makes a significant contribution to the field of cybersecurity by introducing a validated and adaptable audit model that can be tailored to different institutional contexts. The successful implementation of CSAM 2.0 in the participating higher education institutions demonstrates its potential to be scaled and applied across different industries and sectors. The model's design facilitates straightforward implementation, making it accessible to organizations of varying sizes and industries.

Additionally, the integration of the Cybersecurity Awareness TRAining Model (CATRAM 2.0) [52] alongside CSAM 2.0 underscores the importance of role-based cybersecurity training. This complementary approach ensures that staff members are not only aware of cybersecurity policies but also understand their specific responsibilities in maintaining cyber hygiene.

While this study provides significant insights, there are limitations that warrant further investigation. This study was confined to three higher education institutions in Canada, and the findings may not be entirely generalizable to other regions or sectors. Future research should aim to refine CSAM 2.0 by testing its application in a broader range of institutions and industries. This will help to establish its universal applicability and identify any sector-specific modifications that may be required. Organizations need to understand the intentions and capabilities of adversaries to enhance their cybersecurity posture, enabling them to detect, deter, delay, confuse, and anticipate potential threats, thereby navigating through uncertainties and emerging risks in the current international context [53].

Hence, the dynamic nature of cybersecurity threats necessitates ongoing refinement of audit models. Future research should focus on integrating emerging cybersecurity trends and technologies into CSAM 2.0, ensuring it remains relevant and effective amidst evolving cyber threats.

Performing auditing controls ensures that the organization complies with relevant regulations and industry standards. This compliance not only avoids legal penalties but also enhances the organization's reputation and trustworthiness. Governance frameworks benefit from audits as they provide evidence-based assessments of how well controls are implemented and maintained.

In the case studies of Canadian higher education institutions, auditing controls revealed critical insights into both strengths and weaknesses. For instance, robust access control measures were identified as a strength, while gaps in incident response planning were noted as weaknesses. These findings helped the institutions allocate resources effectively, improving their overall security posture and readiness to handle cyber threats.

Both hypotheses (H1 and H2) are supported by the structured analysis of cybersecurity domains and controls. Specific domain selection aids in focused, efficient, and relevant audits, enhancing planning and execution. Meanwhile, auditing controls provide a detailed

understanding of organizational cybersecurity, identifying both strengths to be leveraged and weaknesses to be addressed. This dual approach ensures a comprehensive evaluation and continuous improvement of the organization's cybersecurity defenses.

8. Conclusions

Validating the CyberSecurity Audit Model (CSAM 2.0) within three Canadian higher education institutions provides compelling evidence of its effectiveness as a comprehensive and adaptable cybersecurity audit tool. This study confirms that CSAM 2.0 can significantly enhance cybersecurity resilience by systematically assessing and improving cybersecurity controls customized to fit the unique requirements and settings of educational environments.

The successful implementation of CSAM 2.0 demonstrated several key benefits:

1. Enhanced Cybersecurity Readiness: The tailored strategies and continuous auditing processes facilitated by CSAM 2.0 contributed to a higher level of cybersecurity maturity within the participating institutions. This readiness is crucial in mitigating the sophisticated and frequent cyber threats faced by educational institutions.
2. Adaptability and Flexibility: CSAM 2.0's design allows for partial or complete audits across various cybersecurity domains, making it suitable for institutions with diverse resources and maturity levels. This flexibility ensures that the model can be effectively implemented in a wide range of organizational contexts.
3. Comprehensive Assessment: Unlike existing frameworks, CSAM 2.0 provides clear objectives and practical guidance for conducting detailed cybersecurity audits. This comprehensive approach ensures that all critical areas, including strategy, compliance, and control implementation, are thoroughly evaluated.
4. Role-Based Training Integration: The integration of the Cybersecurity Awareness TRAining Model (CATRAM 2.0) emphasizes the relevance of role-specific cybersecurity training. This ensures that all staff members are well-informed of their responsibilities and actively contribute to the institution's overall cybersecurity posture.

The results from this study underline the necessity for higher education institutions to adopt robust and adaptable cybersecurity frameworks like CSAM 2.0. By doing so, they can better protect sensitive data and maintain their integrity and reputation in an increasingly digital and threat-prone environment.

Future Work

While this study provides valuable insights and validates the effectiveness of CSAM 2.0, it also highlights several areas for future research and development:

1. Broader Application and Validation: Future research should aim to validate CSAM 2.0 across a wider range of higher education institutions, including those in different regions and with varying levels of resources. Additionally, testing the model in other sectors, such as healthcare, finance, and government, would help establish its universal applicability and identify any sector-specific adjustments needed.
2. Integration of Emerging Technologies: The rapidly evolving landscape of cybersecurity threats necessitates continuous updates and refinements to audit models. Future iterations of CSAM 2.0 should incorporate emerging cybersecurity technologies, such as artificial intelligence, machine learning, and blockchain, to enhance threat detection, prevention, and response capabilities.
3. Longitudinal Studies: Implementing longitudinal studies to track the long-term effectiveness of CSAM 2.0 would offer deeper insights into its impact on cybersecurity resilience over time. These studies could assess how continuous auditing and tailored strategies influence the evolution of an institution's cybersecurity maturity.
4. User Feedback and Model Refinement: Gathering feedback from institutions that have implemented CSAM 2.0 will be crucial for ongoing improvement. Understanding user experiences, challenges, and successes will inform refinements to the model, making it more user-friendly and effective.

5. Policy and Compliance Frameworks: Further research should explore the integration of CSAM 2.0 with existing policy and compliance frameworks at national and international levels. This would help institutions not only enhance their cybersecurity practices but also ensure compliance with relevant regulations and standards.
6. Economic Analysis: Investigating the economic implications of implementing CSAM 2.0, including cost–benefit analyses, can provide institutions with a clearer understanding of the financial investments required and the potential returns in terms of risk mitigation and data protection.
7. The future creation of the next version (CSAM 3.0) will identify new cybersecurity domains that will integrate and audit artificial intelligence, machine learning, deep learning, and generative AI tasks that organizations may utilize to manage emerging cyber risks. This approach will allow the researchers to identify controls that can be audited later on, for the purpose of mitigating multiple cyberthreats and cyber incidents under a defensive and offensive cybersecurity response.

In conclusion, CSAM 2.0 represents a significant advancement in cybersecurity auditing for higher education institutions. Its comprehensive, adaptable, and user-friendly design addresses critical gaps in existing frameworks and offers a robust solution for enhancing cybersecurity resilience. Continued research and development will ensure that CSAM 2.0 remains a vital tool in the fight against cyber threats, safeguarding sensitive data and supporting the ongoing mission of educational institutions.

Author Contributions: Conceptualization, R.S.; Methodology, R.S.; Software, R.S.; Validation, R.S.; Formal Analysis, R.S.; Investigation, R.S.; Resources, R.S.; Writing—Original Draft Preparation, R.S.; Writing—review and editing, R.S., J.R.B.H., J.C., J.B.H. and J.A.S.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors gratefully thank *Applied Research and Innovation Services* at the *Southern Alberta Institute of Technology in Canada*. We have maintained complete confidentiality about the institutions and the people we worked with. Here, we would like to acknowledge their support.

Conflicts of Interest: The authors declare no conflicts of interest while conducting these research case studies.

References

1. CrowdStrike. *2023 Global Threat Report*; CrowdStrike, Inc.: Austin, TX, USA, 2023; p. 42.
2. Interpol. *Annual Report 2022—Connecting Police for a Safer World*; Interpol: Lyon, France, 2023; p. 36.
3. IBM Security. *Cost of a Data Breach Report 2023*; IBM Corporation: Armonk, NY, USA, 2023.
4. Meulen, N.; Jo, E.; Soesanto, S. *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Study for the LIBE Committee*; European Union: Brussels, Belgium, 2015; ISBN 978-92-823-8288-2. [CrossRef]
5. Balbix. Balridge Cybersecurity Excellence Builder: Key Questions for Improving Your Organization's Cybersecurity Performance. 2015. Available online: https://www.nist.gov/document/baldrige-cybersecurity-excellence-builder-v11pdf (accessed on 4 August 2024).
6. Balbix. 2020 State of Enterprise Security Posture, Cybersecurity Insiders. 2020. Available online: https://www.balbix.com/app/uploads/2020-State-of-Enterprise-Security-Posture-Report.pdf (accessed on 4 August 2024).
7. Pendergast, T. How to Audit the Human Element and Assess Your Organization's Security Risk. *ISACA J.* **2016**, *5*, 5.
8. PricewaterhouseCoopers—PwC. *Cyber Threats 2020: A Year in Retrospect*; PricewaterhouseCoopers LLP: Mumbai, India, 2021.
9. Lohn, A.; Knack, A.; Burke, A.; Jackson, K. *Autonomous Cyber Defense: A Roadmap from Lab to Ops*; Center for Security and Emerging Technology: Washington, DC, USA, 2023.
10. Knack, A.; Burke, A. *Autonomous Cyber Defence: Authorised Bounds for Autonomous Agents*; The Alan Turing Institute, Center for Security and Emerging Technology: Cambridge, UK, 2024.
11. Divakaran, D.N.; Peddinti, S.T. LLMs for Cyber Security: New Opportunities. *arXiv* **2024**, arXiv:2404.11338.
12. Pleshakova, E.; Osipov, A.; Gataullin, S.; Gataullin, T.; Vasilakos, A. Next Gen Cybersecurity Paradigm towards Artificial General Intelligence: Russian Market Challenges and Future Global Technological Trends. *J. Comput. Virol. Hacking Tech.* **2024**. [CrossRef]
13. Sabillon, R.; Cano, J. Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI—Rev. Ibérica Sist. Tecnol. Informação* **2019**, 33–48. [CrossRef]

14. Sabillon, R. A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE* **2018**, *9*, 127–137. [CrossRef]
15. Sabillon, R. Delivering Effective Cybersecurity Awareness Training to Support the Organizational Information Security Function. In *Interdisciplinary Approaches to Digital Transformation and Innovation*; Rocci, L., Ed.; IGI Global: Hershey, PA, USA, 2021; pp. 284–309. [CrossRef]
16. NIST. *The NIST Cybersecurity Framework (CSF) 2.0*; U.S. Department of Commerce: Washington, DC, USA, 2020. [CrossRef]
17. Sabillon, R.; Serra-Ruiz, J.; Cavaller, V.; Cano, J. A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). In Proceedings of the 2nd International Conference on Information Systems and Computer Science—INCISCOS, Quito, Ecuador, 23–25 November 2017; pp. 253–259. [CrossRef]
18. Government of Canada. *Audit Program, Canadian Centre for Cyber Security*; Government of Canada: Ottawa, ON, Canada, 2021.
19. Government of Canada. *Placemat, Canadian Centre for Cyber Security*; Government of Canada: Ottawa, ON, Canada, 2021.
20. Government of Canada. *Audit Guide, Canadian Centre for Cyber Security*; Government of Canada: Ottawa, ON, Canada, 2021.
21. Government of Canada. *Preliminary Survey Tool, Canadian Centre for Cyber Security*; Government of Canada: Ottawa, ON, Canada, 2021.
22. Government of Canada. *Cyber Security Audit Program, Canadian Centre for Cyber Security*; Government of Canada: Ottawa, ON, Canada, 2021.
23. Deloitte. *Cybersecurity: The Role of Internal Audit*; Deloitte Development LLC: Hermitage, TN, USA, 2015.
24. Deloitte Insights. *Deloitte-NASCIO Cybersecurity Study—States at Risk: The Cybersecurity Imperative in Uncertain Times*; Deloitte Development LLC: Hermitage, TN, USA, 2020.
25. The Institute of Internal Auditors—IIA. *The IIA's Three Lines Model: An Update of the Three Lines of Defense*; The Institute of Internal Auditors Inc.: Lake Mary, FL, USA, 2020.
26. Deloitte Insights. *Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: Bold Plays for Change*; Deloitte Development LLC: Hermitage, TN, USA, 2018.
27. Hathaway, M.; Demchak, C.; Kerben, J.; McArdle, J.; Spidalieri, F. *Cyber Readiness Index 2.0—A Plan for Cyber Readiness: A Baseline and an Index*; Potomac Institute for Policy Studies: Arlington, VA, USA, 2015.
28. European Union Agency for Cybersecurity—ENISA. From January 2019 to April 2020: The Year in Review—ENISA Threat Landscape. 2020. Available online: https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport (accessed on 4 August 2024).
29. Center for Audit Quality—CAQ. *The CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience*; Center for Audit Quality: Washington, DC, USA, 2017.
30. Center for Audit Quality—CAQ. *Fraud and Emerging Tech: Artificial Intelligence and Machine Learning*; Center for Audit Quality: Washington, DC, USA; Anti-Fraud Collaboration (AFC): Washington, DC, USA, 2021.
31. AICPA & CIMA. *SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*; AICPA & CIMA: Durham, NC, USA, 2022.
32. Wertheim, S. Auditing for Cybersecurity Risk, The CPA Journal, 2019, June Issue, ISSN: 0732-8435. Available online: https://www.cpajournal.com/2019/06/19/auditing-for-cybersecurity-risk/ (accessed on 4 August 2024).
33. NIST. *Security and Privacy Controls for Information Systems and Organizations—NIST Special Publication 800-53 Revision 5*; U.S. Department of Commerce: Washington, DC, USA, 2020.
34. Secureframe. *The Ultimate Guide to SOC 2*; Secureframe: San Francisco, CA, USA, 2023.
35. AICPA & CIMA. *Comparison of SOC 2, SOC for Supply Chain, and SOC for Cybersecurity Examinations and Related Reports*; AICPA & CIMA: Durham, NC, USA, 2024; p. 10.
36. PCI Security Standards Council. *Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1*; PCI Security Standards Council: Wakefield, MA, USA, 2024.
37. Center for Internet Security. *CIS Controls Security Controls Version 8*; The Center for Internet Security, Inc. (CIS): East Greenbush, NY, USA, 2021.
38. *ISO/IEC 270001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. Edition 3. International Standard Organization: Geneva, Switzerland, 2022.
39. Leszcyna, R. Review of Cybersecurity Assessment Methods: Applicability Perspective. *Comput. Secur.* **2021**, *108*, 102376. [CrossRef]
40. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [CrossRef]
41. *ISO/IEC 270001:2013*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Standard Organization: Geneva, Switzerland, 2013.
42. Slapnicar, S.; Vuko, T.; Cular, M.; Drascek, M. Effectiveness of Cybersecurity Audit. *Int. J. Account. Inf. Syst.* **2022**, *44*, 100548. [CrossRef]
43. Antunes, M.; Maximiano, M.; Gomes, R. A Client-Centered Information Security and Cybersecurity Auditing Framework. *Appl. Sci.* **2022**, *12*, 4102. [CrossRef]
44. Al-Matari, O.M.M.; Helal, I.M.A.; Mazen, S.A.; Elhennawy, S. Integrated framework for cybersecurity auditing. *Inf. Secur. J. A Glob. Perspect.* **2021**, *30*, 189–204. [CrossRef]

45. Bozkus, S.; Caliyurt, K. Cyber Security Assurance Process from the Internal Audit Perspective. *Manag. Audit. J.* **2018**, *33*, 360–376. [CrossRef]
46. Osipov, A.; Pleshakova, E.; Liu, Y.; Gataullin, S. Machine Learning Methods for Speech Motion Recognition on Telecommunications Systems. *J. Comput. Virol. Hacking Tech.* **2023**. [CrossRef]
47. Tsapin, D.; Pitelinskiy, K.; Suvorov, S.; Osipov, A.; Pleshakova, E. Machine Learning Methods for the Industrial Robotic Systems Security. *J. Comput. Virol. Hacking Tech.* **2023**. [CrossRef]
48. Putrus, R. The Pivotal Role of AI in Navigating the Cybersecurity Landscape. *ISACA J.* **2024**, *4*, 24–29.
49. ISACA. *Using the Digital Trust Ecosystem Framework to Achieve Trustwworthy AI*; ISACA: Schaumburg, IL, USA, 2024.
50. Sabillon, R. *Cyber Security Auditing, Assurance, and Awareness through CSAM and CATRAM*; IGI Global: Hershey, PA, USA, 2021. [CrossRef]
51. Yin, R.K. *Case Study Research and Applications*, 6th ed.; Sage Publications: Thousand Oaks, CA, USA, 2018.
52. Sabillon, R.; Serra-Ruiz, J.; Cavaller, V.; Cano, J. An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *J. Cases Inf. Technol. (JCIT)* **2019**, *21*, 26–39. [CrossRef]
53. Cano M, J.J. Security Risk Management and Cybersecurity: From the Victim or from the Adversary. In *Cybersecurity in the Age of Smart Societies*; Jahankhani, H., Ed.; Advanced Sciences and Technologies for Security Applications; Springer: Cham, Switzerland, 2023. [CrossRef]