International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Strategic Approaches to Cybersecurity Audits for Control Evaluation

Deeksha A[1], Soniya Deepthi[2], Disha[3], Divya S Nayak[4],
Information Science and Engineering
Alva's Institute of Engineering and Technology
Guide: Dr. Rachana P
Email: dishaajeru@gmail.com

Abstract
This article presents an empirical study evaluating the effectiveness of the CyberSecurity Audit Model (CSAM 2.0) at a Canadian higher education institution. CSAM 2.0 is a comprehensive model used to assess cybersecurity assurance, maturity, and readiness in medium to large organizations and at the national level. It allows for the effective evaluation of security controls across various cybersecurity domains. The study highlights global best practices in cybersecurity audits, highlighting the lack of standardized guidelines and weaknesses in cybersecurity training programs. The paper details CSAM 2.0's structure and architecture, sharing results from three research scenarios: (1) a single audit focusing on awareness education, (2) audits in multiple domains such as governance, legal compliance, and incident management, and (3) a full audit covering all model domains. The study concludes that CSAM 2.0 offers valuable insights for improving cybersecurity practices and addressing vulnerabilities.

Keywords:
Cybersecurity, Cybersecurity Audits, Cybersecurity Audit Model, Cybersecurity Assurance, Cybersecurity Maturity, Control Evaluation, Risk Management, Incident Response, Cybersecurity Domains, Cybersecurity Training.

I. INTRODUCTION

Organizations are constantly working to protect their most valuable digital assets and implement robust cybersecurity strategies to maintain seamless business operations. However, despite these proactive measures, cybersecurity breaches and cyberattacks continue to pose significant challenges and remain an ongoing risk.

The European Union Agency for Cybersecurity (ENISA) reported key cybercriminal trends in 2023, including:

- Top cyber threats: DDoS, ransomware, social engineering, information manipulation, supply chain attacks, and malware.
- Phishing remains the primary attack vector, with a significant rise in social engineering attacks, fueled by AI and new techniques.
- Cybercriminals are increasingly targeting cloud infrastructure.
- Threat actors continue to professionalize their "as-a-Service "programs [1].

ISACA recommends continuous cybersecurity review to assess the design and effectiveness of control measures. This includes informal assessments and comprehensive audits of all cybersecurity arrangements within organizations [2].

Annual cybersecurity audits offer organizations the opportunity to assess and strengthen their controls, and identify areas for improvement, and should be adopted as a key practice to advance the maturity of their cybersecurity programs [3].

Key elements of cybersecurity audits include evaluating cybersecurity policies, creating a comprehensive cybersecurity strategy, assessing staff cyber competencies, and promoting risk-based audit initiatives within the organization [4].

Drascek et al. [5] proposed several best practices for internal auditors to improve the effectiveness of the cybersecurity audits they conduct:

1. Upskill: By increasing the auditor's competencies to obtain industry certifications.
2. Outsource or co-source the internal audit function if the Internal Audit Functions (IAF) are not satisfactory, but stay within accepted parameters.

Cybersecurity demands constant attention due to the ever-changing threat landscape, and organizations should measure the effectiveness of their security safeguards. Auditors are required to develop skills and capabilities to conduct successful cybersecurity audits [6].

The CyberSecurity Audit Model (CSAM 2.0) has been developed to address limitations and the absence of cybersecurity guidelines to conduct comprehensive cybersecurity audits organized by domains [7].

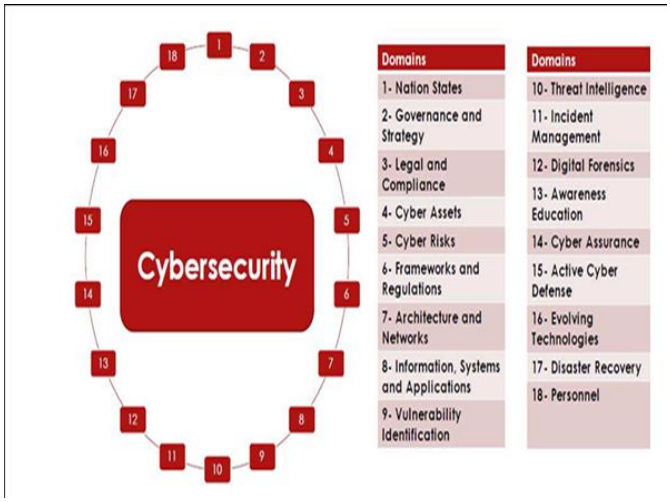
II. The Cybersecurity Audit Framework (CSAM 2.0)

The Cybersecurity Audit Framework (CSAM 2.0) is an advanced model designed to assess and improve the cybersecurity posture of organizations. It provides a structured approach for evaluating the effectiveness of cybersecurity controls, ensuring that all critical security domains are addressed. CSAM 2.0 helps organizations measure cybersecurity assurance, maturity, and readiness by focusing on areas such as risk management, governance, compliance, incident response, and emerging technologies.

Key components of CSAM 2.0 include:

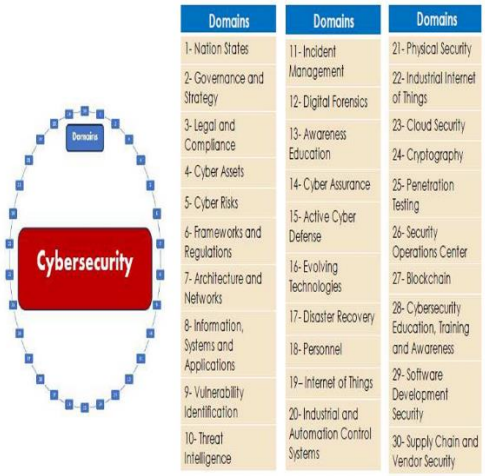
1. Comprehensive Assessment: The framework allows for detailed audits across various cybersecurity domains, ensuring that both technical and procedural controls are in place.
2. Maturity and Readiness Evaluation: CSAM 2.0 measures how mature an organization's cybersecurity practices are and assesses its preparedness for potential cyber threats.
3. Risk-Based Approach: The model integrates a risk management perspective, ensuring that cybersecurity efforts are aligned with organizational priorities and vulnerabilities.
4. Continuous Improvement: It emphasizes the need for ongoing assessments and improvements to keep up with evolving cybersecurity threats and best practices.
5. Global Best Practices: The framework draws upon global cybersecurity standards and best practices to ensure thorough and effective audits.

CSAM 2.0 has been successfully tested in various scenarios, including single-domain audits and full-scale, multi-domain assessments, providing valuable insights for enhancing cybersecurity controls and addressing potential vulnerabilities.



CSAM 2.0 (Fig. 2) was released in June 2023 as the next version of CSAM. The key changes in version 2.0 introduced the following additions:

- Twelve new cybersecurity domains were added.
- Physical security audits are now part of this version.
- Audits for Industrial and Manufacturing Control Systems were introduced.
- Cybersecurity Education, Training, and Awareness (CSETA) can now be audited as part of the organizational program.
- Vendor and supply chain security audits were introduced.
- Software development security audits were added to this new version of the model.
- Additional areas such as cloud security, penetration testing, and Security Operations Center (SOC) audits were also incorporated.



III. RESULTS

The CSAM 2.0 was implemented and validated at a Canadian higher education institution in Alberta, which has multiple campuses, over 2,500 employees, and serves more than 15,000 students annually. Cybersecurity is managed by the CIO and CISO offices. The audit methodology involved calculating control evaluations, averaging sub-controls, and combining results to determine the audited cybersecurity domain's percentage. The study successfully validated CSAM 2.0 through comprehensive audits across various domains, providing recommendations to improve the institution's cybersecurity posture. CSAM 2.0 effectively measured cybersecurity assurance and maturity.

One of the scenarios focused on auditing the institution's cybersecurity awareness domain. This domain focuses on evaluating how well employees and students understand cybersecurity policies, such as password management and phishing awareness. Based on audit results, CSAM 2.0 provided recommendations to improve cybersecurity practices, such as enhancing training and data protection measures. The model effectively measured cybersecurity maturity and assurance.

Table I: Overall Cybersecurity Domain Score (Scenario I)

Cybersecurity Audit Model (CSAM 2.0)			
Domain	**13-Awareness Education**		
Control Evaluation	Ratings		%
	Immature	☐	
	Developing	☐	
	Mature	☒	**80**
	Advanced	☐	
Mature (M): 71-90 While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.			

Table II: Score for Selected Domains (Scenario II)

Table II: Score for Selected Domains (Scenario II) likely presents the results of an audit conducted across multiple cybersecurity domains as part of Scenario II. This scenario involves evaluating several key cybersecurity areas within the institution, such as governance, incident management, compliance, and risk management. The table shows the scores assigned to each domain based on their effectiveness and maturity, to identify areas that need improvement. The scores help assess how well each domain aligns with best practices and security standards, providing a clear overview of the institution's overall cybersecurity posture.

Cybersecurity Audit Model (CSAM 2.0)						
No.	Domain	Ratings				%
		I	D	M	A	
2	Governance and Strategy	☐	☐	☒	☐	85
3	Legal and Compliance	☐	☐	☐	☒	100
5	Cyber Risks	☐	☐	☐	☒	100
6	Frameworks and Regulations	☐	☐	☐	☒	96
11	Incident Management	☐	☐	☒	☐	90
14	Cyber Insurance	☐	☐	☐	☒	100
16	Evolving Technologies	☐	☐	☒	☒	80
19	Internet of Things (IoT)	☐	☒	☐	☐	50
23	Cloud Security	☐	☒	☐	☐	70
28	Cybersecurity Education, Training and Awareness (CSETA)	☐	☒	☐	☐	63
Mul ple Domains -Cybersecurity Maturity Ra ng						
Mature (M): 71-90 While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.		☐	☐	☒	☐	83

IV. DISCUSSION

This case study emphasizes the importance of cybersecurity audits in assessing security controls and responses to cyber threats. It highlights the value of role-based cybersecurity training and the use of standardized frameworks like CSAM 2.0 for comprehensive audits. The Cybersecurity Assurance and Maturity Index Equation (CAMIE) is introduced as a tool for measuring cybersecurity assurance and maturity across different domains. CAMIE calculates an index based on final audit ratings and the Domain Magnitude (DM), which reflects the criticality of each audited domain within the organization.

Table V: CAMIE Results by Target Organization

Domain Magnitude (DM)	Values	Description
Very High	5	CSAM domain is extremely 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

Table V: CAMIE Results by Target Organization likely presents the calculated Cybersecurity Assurance and Maturity Index Equation (CAMIE) results for the specific target organization being audited. This table shows the final scores for each cybersecurity domain based on the audit results, reflecting the organization's cybersecurity assurance and maturity in various areas.

Each domain's CAMIE score is calculated by combining the final ratings from the audit and the Domain Magnitude (DM) from Table IV, which considers the criticality of each domain to the organization. The table provides an overview of the organization's strengths and weaknesses in its cybersecurity practices, helping decision-makers identify areas that require improvement. The CAMIE results serve as a comprehensive metric for evaluating how well the organization has addressed cybersecurity risks and maturity across its domains.

CSAM Domains	CHEI3		
	Score (%)	*DM*	*CAMIE*
D2	85	5	425
D3	100	5	500
D4	75	5	375
D5	100	5	500
D6	96	4	384
D7	68	5	340
D8	60	5	300
D9	74	4	296
D10	90	4	360
D11	90	4	360
D12	50	2	100
D13	80	3	240
D14	100	1	100
D15	85	1	85
D16	80	4	320
D17	90	5	450
D18	80	3	240
D19	50	2	100
D21	95	5	475
D23	70	5	350
D24	80	3	240
D25	80	3	240
D26	50	3	150
D28	63	3	189
D30	50	5	250
Totals	**78**	**4**	**295**

CONCLUSION

This study highlights the critical role of cybersecurity audits for higher education institutions and other organizations, showcasing the successful validation of the CyberSecurity Audit Model (CSAM 2.0) across three research scenarios: auditing a single cybersecurity domain, multiple domains, and all domains. The results demonstrate the effectiveness and dependability of CSAM 2.0 in assessing cybersecurity assurance and maturity. The CAMIE metric proves to be a useful tool for evaluating cybersecurity maturity across various domains. By conducting thorough cybersecurity audits, organizations can improve security controls, enhance their response to cyber threats, and strengthen their overall cybersecurity posture. CSAM 2.0 provides a standardized, adaptable framework for these audits, allowing organizations to tailor assessments to their unique needs. This research contributes valuable knowledge to the field of cybersecurity assurance and audit, offering practical tools and insights for organizations aiming to improve their cybersecurity preparedness.

REFERENCE:

1. ENISA, “ENISA Threat Landscape 2023: July 2022 to June 2023”, European Union Agency for Cybersecurity, October 2023, ISBN 978-92-9204-588-3, DOI: 10.2824/782573.
2. ISACA, “Cybersecurity Audit Certificate: Study Guide”, ISBN 976-1-60420-759-0, 2018.
3. ISACA, “Auditing Cyber Security: Evaluating Risk and Auditing Controls”, 2017.
4. E. Chimwanda, “Essentials for an Effective Cybersecurity Audit”, Industry News, ISACA, April 2022.
5. M. Drascek, S. Slapnnicar, T. Vuko, and M. Cular, “How Effective Is Your Cybersecurity Audit”, ISACA Journal, vol. 2022. Available at: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/how-effective-is-your-cybersecurity-audit
6. I. Cooke and R.V. Raghu, “IS Audit Basics: Auditing Cybersecurity”, ISACA Journal, vol. 2, 2019. Available at: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/is-audit-basics-auditing-cybersecurity
7. R. Sabillon and J.R. Bermejo Higuera, “New Validation of a Cybersecurity Model to Audit the Cybersecurity Program in a Canadian Higher Education Institution”, 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2023, pp. 1-6, doi: 10.1109/ICTAS56421.2023.10082731.