New Validation of a Cybersecurity Model to Audit the Cybersecurity Program in a Canadian Higher Education Institution

Regner Sabillon
Universidad Internacional de La Rioja (UNIR)
Logroño, Spain
0000-0003-1807-2208

Juan Ramon Bermejo Higuera
ESIT – Escuela Superior de Ingeniería y Tecnología
Universidad Internacional de La Rioja (UNIR)
Logroño, Spain
0000-0002-0197-8663

2023 Conference on Information Communications Technology and Society (ICTAS) | 978-1-6654-8930-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICTAS56421.2023.10082731

***Abstract*—This article presents the results of one empirical study that evaluated the validation of the CyberSecurity Audit Model (CSAM) for the second time in a different Canadian higher education institution. CSAM is utilized for conducting cybersecurity audits in medium or large organizations or a Nation State to evaluate and measure cybersecurity assurance, maturity, and cyber readiness. The authors review best practices and methodologies of global leaders in the cybersecurity assurance and audit arena, that puts in evidence the lack of universal guidelines to conduct extensive cybersecurity audits and the detection of existing weaknesses in general programs to deliver cybersecurity awareness training. The architecture of CSAM is described in central sections. CSAM has been tested, implemented, and validated in three research scenarios (1) a single cybersecurity domain audit (Awareness Education), (2) Cybersecurity audit of several domains (Governance and Strategy, Legal and compliance, Cyber Risks, Frameworks and Regulations, Incident Management, Cyber Insurance and Evolving Technologies) and (3) Cybersecurity audit of all model domains The study concludes by showing how the validation of the model allows to report significant information for future decision making that the target organization may correct cybersecurity weaknesses or to improve cybersecurity domains and controls.**

Keywords—cybersecurity; cybersecurity audit; cybersecurity audit model; cybersecurity assurance; cybersecurity controls; cybersecurity domains; cybersecurity maturity assessment; cyber readiness; cybersecurity scorecard; cybersecurity domain criticality

I. INTRODUCTION

Organizations are protecting their most critical cyber assets – the crown jewels and implement cybersecurity measures and programs to ensure continuous business operations, but regardless this persistent effort it is inevitable to circumvent cybersecurity breaches and cyberattacks[1].

According to the Information Systems Audit and Control Association (ISACA) [1], the origin of cybersecurity was published in a journal article in the early eighties, presenting the first proof of the concepts of self-replicating/self-propagating code linked to a computer worm. Pursuant to the fundamentals of the discipline defined by ISACA, cybersecurity is defined as "The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems" – cybersecurity and information security are often mentioned interchangeably but cybersecurity is a component of information security [2].

As reported by Cano [3], he points out that there are two types of companies: Companies that have experienced a cyberattack and Companies that have not realized it yet. Creating a cybersecurity vision is not an easy task, similarly is the implementation of basic security safeguards. Thereby, implementing controls and measures may not be enough to protect the whole organizational cybersecurity.

Gemalto [4] from its 2018 Data Breach Investigations Report (BLI) presents findings that included 4,553,172,708 breached records, 945 breach incidents, 20% of breaches with unknown compromised records, 2.2% of data breaches of encrypted files, data records were lost or stolen with this frequency:

- 291 every second
- 17,469 every minute
- 1,048,152 every hour
- 25,155,650 every day

The top sources of these breaches were malicious outsiders (56%), unknown (1%), hacktivists (2%), malicious insiders (7%) and accidental loss (34%) [5].

The European Union Agency for Cybersecurity -ENISA [6] reported that the major cybercriminal trends during 2022 include ransomware, malware, social engineering attacks, threats against data, Denial of Service (DoS) attacks, Internet threats, disinformation and supply chain cyberattacks.

IT audits are being reconsidered to include cybersecurity but there are not specific guidelines or consensus to what areas, sub-areas, domains, or sub-domains to incorporate in a cybersecurity audit. The audit scope is easier defined if the target organization has implemented a specific cybersecurity framework or standard from governing agencies like the International Organization for Standardization (ISO 27000 Series), the National Institute of Standards and Technology (NIST), the International

978-1-6654-8930-0/23/$31.00 ©2023 IEEE

Information System Security Certification Consortium (ISC)2, the SANS Institute (SysAdmin, Audit, Network and Security), the Control Objectives for Information and Related Technologies (COBIT), the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Trust Alliance (HITRUST) or the North American Electric Reliability Corporation (NERC) [7]. This approach is entirely to verify cybersecurity compliance to a specific framework or to a specific industry or sector and cybersecurity audits corroborate that controls are in place and are effective.

Donaldson et al. [8] described three different types of cybersecurity audits:

1. Threat audits: These audits target cyberthreats and the aim is to search for evidence in IT environments.
2. Assessment audits: Audits are evaluating the cybersecurity controls that are mapped against frameworks, regulatory requirements, standards or in special cases to a specific cyberthreat.
3. Validation assessments: Assessment is verified against cybersecurity controls in order to measure the effectiveness of these controls against designed and documented requirements.

The Donaldson's "Audit First" design methodology recommends that auditors should design cybersecurity controls preventive controls last instead of first. The CSAM controls were designed to ensure efficiency and effectiveness while planning and conducting the cybersecurity audits.

Our CyberSecurity Audit Model (CSAM) has been designed to address the limitations and inexistence of cybersecurity safeguards to conduct comprehensive cybersecurity or domain-specific cybersecurity audits [9].

II. The CyberSecurity Audit Model (csam)

The CyberSecurity Audit Model (CSAM) is a comprehensive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a National Cybersecurity Strategy (NCS) or want to evaluate the effectiveness of its National Cybersecurity Strategy or Policy already in place [10]. CSAM can be implemented to conduct internal or external cybersecurity audits, this model can be used to perform single cybersecurity audits or can be part of any organizational audit program to improve cybersecurity controls. Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening. The CSAM has 18 domains; domain 1 is specific for Nation States and domains 2-18 can be implemented at any organization [11].

The CyberSecurity Audit Model (CSAM) contains overview, resources, eighteen domains, twenty-six sub-domains, eighty-seven checklists, 169 controls, 429 sub-controls, eighty guideline assessment and an evaluation scorecard [12].

The goal of this research was to perform the second implementation and validation of all domains of the CyberSecurity Audit Model (CSAM) as a comprehensive model for the challenges that may arise when planning and delivering cybersecurity audits. Case studies are considered the most relevant of observational studies, any case study results are limited in generalizability and broader applications [13]. Furthermore, we needed to validate the CSAM in a second and larger higher education institution to corroborate the efficiency and reliability of the CSAM obtained in the first research study with poor results obtained for the initial target organization. We approached upper management of our target organization and presented our case study research proposal. We decided to conduct a cybersecurity pre-assessment to understand the organizational cybersecurity function and from there, plan to implement CSAM in similar way from the initial study [14] and the results of the model's validation be instrumental to understand the current cybersecurity status of the organization. The target organization management felt that this case study was a win-win opportunity for the institution and for the researchers. The principal researcher conducted interviews, observations, online surveys and collected documentation pertinent to the scope of the case study. During the pre-assessment stages, the first author collected data using online surveys from managers, IT staff, InfoSec Staff and Top Executives. Thus, we collected evidence when conducting the cybersecurity audits based on our previous experience implementing the CSAM and organized by cybersecurity domains. The data collection phase allowed us to gather evidence from multiple sources like documents, policies, archival records, open-ended interviews, observations, structured interviews, structured surveys, multiple site visits, presentations, meetings, and computer and server logs. During this phase, the researchers interacted with the proper authorities to obtain research data and the internal lead project manager from the target institution assigned the personnel participating in the research case study. The datasets provided the information that was later used to calculate final scores using the model's evaluation scoreboard that combines qualitative and quantitative metrics. Furthermore, the resulting data was analyzed based on the CSAM indicators. The researchers also utilized a variety of approaches for data analysis. For the CSAM datasets, the data was recorded in our control forms, sub-control forms and checklists for each cybersecurity domain and sub-domain that we audited. The research methodology included the second Canadian Higher Education Institutions as target (Identified as CHEI2) to validate the implementation of our main research cybersecurity audit model (CSAM), data validation and outcomes from the cybersecurity audits are presented in the *Results* and *Discussion* sections of this research study.

III. Results

This second target organization has a central campus with six additional locations in six different cities, over 700 employees, it serves more than 17,500 students annually and the cybersecurity function is managed by the Information Security department. The evaluation methodology includes these steps for auditing each cybersecurity domain:

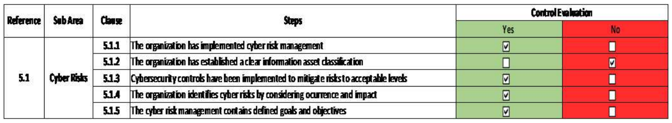
a) Obtain the average of the control evaluation by domain/sub-domain

b) Calculate the average of sub-controls for every checklist
c) Add the results from Steps a and b and obtain the average
d) The outcome from Step c provide the percentage for the cybersecurity domain that was audited

The main results include the following:

- The successful validation of the CSAM by conducting comprehensive cybersecurity audits organized by domains in different organization.
- The audit recommendations were reported to upper management of the target institutions to improve their cybersecurity posture.
- The effectiveness of CSAM to measure cybersecurity assurance and maturity.

Next, we illustrated how the audit for a specific cybersecurity domain took place. First, we identified our target organization and the domain that was audited. In this case, it is for our second target organization (Canadian Higher Education Institution # 2 – CHEI2) and the specific CSAM domain which is CSAM Domain # 5 (Cyber Risks). This domain has one sub-domain identified with the same name as the cybersecurity domain, but code is 5.1, covering five different clauses from 5.1.1 to 5.1.5. shown in "Fig. 1", this score for this initial control verification was 80%, this percentage will be useful later to calculate the total ranking and maturity value for the fifth CSAM 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	☑	□

Fig.1. Evidence to assess the controls for the CSAM Domain # 5

Furthermore, the next phase was to check the existing cybersecurity controls on how this organization was managing their cyber risk function. The Sub-domain "Cyber Risks" has 10 sub-controls that are included on the "Cybersecurity Audit Checklist: CSAM-Cyber Risks", this checklist is going to measure the effectiveness of the cybersecurity sub-controls based on the main clauses (5.1.1 to 5.1.5); these sub-controls are organized by clauses like this:

- 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 outcome from this audit verifies the cybersecurity effectiveness of the existing controls (Compliant), the lack of controls (Major Nonconformity) or simply a verification that controls are partially applied or have not been fully implemented (Minor Nonconformity). The score for this checklist is only 40 % because there were only fully implemented sub-controls that are in compliance with what criteria CSAM is assessing in terms of cyber risk controls. Finally, having the values from the initial controls and the sub-controls then we can proceed to obtain the final score which is 60% for CSAM Domain 5. For presenting the results of our case study research, we will refer to our target organizations using CHE2 indicators. The audit findings are categorized by compliant, minor nonconformity or major nonconformity. Table I presents the categories for evaluating the cybersecurity controls.

TABLE I: CSAM Audit Findings for control assessments

Audit Findings	Description	Examples
Compliant	The control requirements have been verified and are in compliance with 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

A. *Scenario I: A single cybersecurity domain audit (Awareness education)*

Table II summarizes the results and domain rating for awareness education.

TABLE II. Overall Cybersecurity domain score (Scenario III for CHEI2)

Cybersecurity Audit Model (CSAM)			
Domain	***13-Awareness Education***		
Control Evaluation	***Ratings***		***Score***
	Immature	□	**95%**
	Developing	□	
	Mature	□	
	Advanced	☒	
Advanced (A): 91-100 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.			

This particular cybersecurity domain is audited to measure the cybersecurity awareness of the target institution that can be used to understand the overall cybersecurity posture and culture of the organization.

B. Scenario II: Cybersecurity audit of several domains (Governance and Strategy, Legal and compliance, Cyber Risks, Frameworks and Regulations, Incident Management, Cyber Insurance and Evolving Technologies)

Table III summarizes the results and domain ratings for the research scenario II where selected cybersecurity domains were audited.

TABLE III. Score for selected domains (Scenario II for CHEI2)

Cybersecurity Audit Model (CSAM)						
No.	***Domain***	***Ratings***				***Score***
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☒	☐	☐	42%
3	Legal and Compliance	☐	☐	☐	☒	100%
5	Cyber Risks	☐	☒	☐	☐	70%
6	Frameworks and Regulations	☐	☐	☒	☐	90%
11	Incident Management	☐	☐	☐	☒	92%
14	Cyber Insurance	☐	☐	☒	☐	85%
16	Evolving Technologies	☐	☐	☒	☐	80%
Multiple Domain -Cybersecurity Maturity Rating		☐	☐	☒	☐	**80%**
Mature (M): 71-90% While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.						

C. Scenario III: Cybersecurity audit of all domains

The CSAM validation had a clear scope to evaluate all cybersecurity domains for CHEI2, that provided the overall rating for its cybersecurity posture. Table IV summarizes the results and domain ratings for the research scenario where all CSAM cybersecurity domains were audited [15].

TABLE IV. Cybersecurity score for all domains (Scenario I for CHEI2)

Cybersecurity Audit Model (CSAM)						
No.	***Domain***	***Ratings***				***Score***
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☒	☐	☐	42%
3	Legal and Compliance	☐	☐	☐	☒	100%
4	Cyber Assets	☐	☐	☒	☐	80%
5	Cyber Risks	☐	☒	☐	☐	70%
6	Frameworks and Regulations	☐	☐	☒	☐	90%
7	Architecture and Networks	☐	☐	☒	☐	80%
8	Information, Systems and Apps.	☐	☐	☒	☐	87%
9	Vulnerability Identification	☐	☐	☐	☒	100%
10	Threat Intelligence	☐	☐	☐	☒	95%
11	Incident Management	☐	☐	☐	☒	92%
12	Digital Forensics	☐	☐	☒	☐	85%
13	Awareness Education	☐	☐	☐	☒	95%
14	Cyber Insurance	☐	☐	☒	☐	85%
15	Active Cyber Defense	☐	☒	☐	☐	60%
16	Evolving Technologies	☐	☐	☒	☐	80%
17	Disaster Recovery	☐	☐	☒	☐	89%
18	Personnel	☐	☐	☒	☐	85%
Multiple Domain -Cybersecurity Maturity Rating		☐	☐	☒	☐	**83%**
Mature (M): 71-90% While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.						

Conducting cybersecurity audits involve that the cybersecurity practitioners and auditors dealing with and reviewing a lot of sensitive and oftentimes confidential information that cannot be revealed. Our target organization always requested that the researchers sign off Non-Disclosure Agreements (NDAs) and given the nature of the cybersecurity audits, the target organizations will limit the information that can be disclosed in the public domain. Obviously, the organizational measures will prevent disclosing sensitive information that cybercriminals will discover and gather to plan and launch future cyberattacks against these institutions participating in research studies.

The main results of this study corroborate the effectiveness of conducting cybersecurity audits that are being planned and conducted by domains, the outcomes of this audit helped upper management to improve their cybersecurity program and lastly, by measuring the organizational cybersecurity assurance and maturity based on the evaluation scoreboard that CSAM provides.

IV. Discussion

This case study has provided compelling evidence that cybersecurity audits [16] are significant to any organization by ensuring that security controls are in place, that they are effective and additionally to determine cybersecurity areas or domains that have weak controls including nonexistent controls that will induce major nonconformities for not adequately protecting cyber assets. Our radar chart displays the domain rankings from our target institutions in “Fig. 2”. These are the values from Table IV.

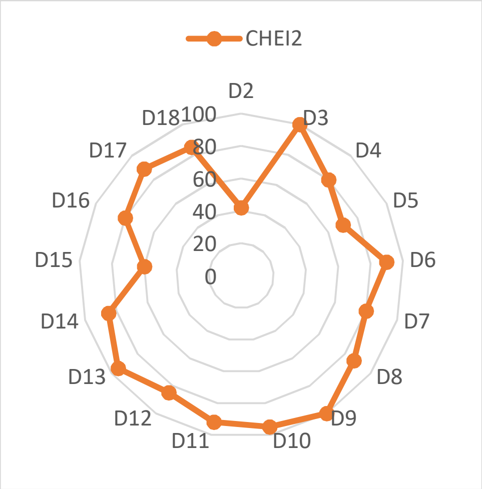


Fig.2. Evidence to assess the controls for the CSAM Domain # 5

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

The CAMIE equation can help identify the index to validate the cybersecurity assurance and maturity of any CSAM domain. Different possibilities exist that are defined in alignment with the scope of the cybersecurity audit to be conducted. CAMIE can be calculated by using the final ratings after a cybersecurity audit has been completed by CSAM Domain results. Where *D* is the final domain score obtained and *DM* is the Domain Magnitude (Table V) that each organization will assign to each audited domain based on enterprise criticality, after the domain audit has been conducted and completed.

TABLE V. CSAM Domain Criticality

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

For instance, Equation (1) depicts the results for a full audit, “(2)” for one cybersecurity domain, “(3)” for two CSAM domains or for seven randomly selected domains in “(4)”.

$$\text{CAMIE for all CSAM domains} = [(\sqrt{D1^2} * DM1\,) + \cdots + (\sqrt{D18^2}\text{*DM18})]/18 \tag{1}$$

$$\text{CAMIE for one CSAM domain} = \sqrt{D1^2}\ \text{* DM1} \tag{2}$$

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

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

Table VI presents the CAMIE outcomes classified by target organization and by CSAM domains. CSAM incorporates many cybersecurity domains that are not found in other cybersecurity frameworks or standards. CSAM cybersecurity domains include the verification of controls for cyberspace, governance and strategy, compliance, cyber risk management, regulations and threat intelligence that are not found in other cybersecurity frameworks nor in cybersecurity models.

TABLE VI. CAMIE results by target organization

CSAM Domains	**CHEI2**		
	Score (%)	***DM***	***CAMIE***
D2	42	5	210
D3	100	5	500
D4	80	5	400
D5	70	5	350
D6	90	4	360
D7	80	5	400
D8	87	5	435
D9	100	4	400
D10	95	4	380
D11	92	4	368
D12	85	2	170
D13	95	3	285
D14	85	1	85
D15	60	1	60
D16	80	4	320
D17	89	5	445
D18	85	3	255
Totals	**83**	**4**	**319**

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

We calculate the final cybersecurity maturity rating of the Nation States domain (CSAM D1). And for domains 2-18 (CSAM D2-D18), we calculate the final cybersecurity maturity rating of any organization by using the following criteria:

The score can be mapped 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 to 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.

CONCLUSIONS

The results of this study show that cybersecurity audits conducted by domains can be very effective to assess controls and responses to cyberthreats. Thus, the delivery of cybersecurity training based on organizational roles and responsibilities contributes to persuading personnel to create and maintain awareness in their workplaces as well as in their personal lives [17]. The initial limitation of our first study is that CSAM has been validated in a single organization, time constraints, lack of interest for the topics and lack of engagement were some of the challenges that we had to overcome from some of the participants. Another limitation is that the first CSAM domain (D1) has not been tested yet as this is applicable to a Nation, Province, and State. Hence, in this second engagement the participating organization was very interested in validating the CSAM, as they were in the process of organizing and improving their cybersecurity function and the overall cybersecurity program. The Cybersecurity Assurance and Maturity Equation (CAMIE) is a suitable metric key that measures the cybersecurity maturity of any CSAM domain. The case study findings have implications for our target organization but at the same time, implications for future research to review and expand our cybersecurity model- the CSAM as we are planning the design of CSAM version 2.0.

To address current limitations, future research may include new cyber areas or additional domains that can be integrated into CSAM, even future opportunities for creating mappings with other cybersecurity frameworks, standards, or policies and utilizing CSAM to plan and conduct additional cybersecurity audits in more organizations from different industries and sectors. Cybersecurity is a very dynamic field that keeps evolving as the cyberthreat landscaping continuously changes. Organizations must commit to conducting extensive cybersecurity audits to be prepared for dealing with cyber incidents, cyberthreats and cyberattacks. CSAM can add value to any organization for all different stages of cybersecurity audits.

REFERENCES

[1] ISACA, Transforming Cybersecurity. Rolling Meadows: ISACA, 2013.

[2] ISACA, Cybersecurity Fundamentals. Rolling Meadows: ISACA, 2015

[3] J. Cano, “Cyberattacks-The Instability of Security and Control Knowledge,” ISACA Journal, vol.5, pp. 1-5, 2016.

[4] Gemalto, “Data Privacy and New Regulations Take Center Stage: 2018 First Half Review,” September 2018.

[5] S. Tweneboah-Koduah, F. Atsu and R. Prasad, “Reaction of Stock Volatility to Data Breach: An Event Study”, Journal of Cyber Security and Mobility, vol 9, issue 3, pp. 355-384, 2020, doi: 10.13052/jcsm2245-1439.931

[6] ENISA, “ENISA Threat Landscape 2022: July 2021 to July 2022”, European Union Agency for Cybersecurity, October 2022, ISBN 978-92-9204-588-3, DOI: 10.2824/764318

[7] M.G.T. Espinoza, J.R.N. Melendrez, L.A.N. Clemente, "A Survey and an IoT Cybersecurity Recommendation for Public and Private Hospitals in Ecuador", Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 518-528, 2020.

[8] S. Donaldson, S. Siegel, C. Williams and A. Aslam, Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats. New York: Apress, 2018, pp. 377-428.

[9] R. Sabillon, "Audits in Cybersecurity." Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM, IGI Global, 2021, pp.126-148. https://doi.org/10.4018/978-1-7998-4162-3.ch007

[10] R. Sabillon, J. Serra-Ruiz, V. Cavaller and J. Cano, "A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)," 2017 International Conference on Information Systems and Computer Science (INCISCOS), 2017, pp. 253-259, doi: https://doi.org/10.1109/INCISCOS.2017.20

[11] R. Sabillon, Cybersecurity Auditing, Assurance and Awareness Through CSAM and CATRAM: Emerging Research and Opportunities. IGI Global. doi: http://doi:10.4018/978-4162-3, 2021.

[12] R. Sabillon y J. Cano, “Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones”. Edición Especial: Ciberseguridad y Ciberdefensa. Revista Ibérica de Sistemas e Tecnologias de Informaçao (RISTI). Portugal. 32 (06), 33-48, doi: 10.17013/risti.32.33-48, 2019

[13] R. Sabillon, A Practical Model to Perform Comprehensive Cybersecurity Audits. Enfoque UTE, 9(1), pp. 127 - 137. https://doi.org/10.29019/enfoqueute.v9n1.214, 2018.

[14] R. Sabillon, The CyberSecurity Audit Model (CSAM), In I.Management Association (Eds.), Research Anthology on Business Aspects of Cybersecurity, pp.77-139, IGI Global. http://doi:10.4018/978-1-6684-3698-1.ch005, 2022

[15] R. Sabillon, "The CyberSecurity Audit Model (CSAM)." Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM, IGI Global, 2021, pp.149-232. https://doi.org/10.4018/978-1-7998-4162-3.ch008

[16] R. Sabillon, Audits in Cybersecurity, In I.Management Association (Eds.), Research Anthology on Business Aspects of Cybersecurity, pp. 1-18. IGI Global. http://doi:10.4018/978-1-6684-3698-1.ch001, 2022.

[17] R. Sabillon, "The Cybersecurity Awareness Training Model (CATRAM)." Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM, IGI Global, 2021, pp.233-257. https://doi.org/10.4018/978-1-7998-4162-3.ch009