A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance:

The CyberSecurity Audit Model (CSAM)

Regner Sabillon
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya (UOC)
Barcelona, Spain
regners@athabascau.ca

Jordi Serra-Ruiz
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya (UOC)
Barcelona, Spain
jserrai@uoc.edu

Victor Cavaller
Information and Communication Sciences
Universitat Oberta de Catalunya (UOC)
Barcelona, Spain
vcavaller@uoc.edu

Jeimy Cano
School of Business
Universidad del Rosario
Bogota, Colombia
jeimy.cano@urosario.edu.co

***Abstract*— Nowadays, private corporations and public institutions are dealing with constant and sophisticated cyberthreats and cyberattacks. As a general warning, organizations must build and develop a cybersecurity culture and awareness in order to defend against cybercriminals. Information Technology (IT) and Information Security (InfoSec) audits that were efficient in the past, are trying to converge into cybersecurity audits to address cyber threats, cyber risks and cyberattacks that evolve in an aggressive cyber landscape. However, the increase in number and complexity of cyberattacks and the convoluted cyberthreat landscape is challenging the running cybersecurity audit models and putting in evidence the critical need for a new cybersecurity audit model. This article reviews the best practices and methodologies of global leaders in the cybersecurity assurance and audit arena. By means of the analysis of the current approaches and theoretical background, their real scope, strengths and weaknesses are highlighted looking forward a most efficient and cohesive synthesis. As a resut, this article presents an original and comprehensive cybersecurity audit model as a proposal to be utilized for conducting cybersecurity audits in organizations and Nation States. The CyberSecurity Audit Model (CSAM) evaluates and validates audit, preventive, forensic and detective controls for all organizational functional areas. CSAM has been tested, implemented and validated along with the Cybersecurity Awareness TRAining Model (CATRAM) in a Canadian higher education institution. A research case study is being conducted to validate both models and the findings will be published accordingly.**

Keywords—cybersecurity; cybersecurity audit; cybersecurity audit model; cybersecurity assurance; cybersecurity controls; cybersecurity domains

I. INTRODUCTION

Organizations are trying to protect cyber assets and implement cybersecurity measures and programs, but despite this continuing effort it is unavoidable to avoid cybersecurity breaches and cyberattacks.

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 *"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 shown by Cano [3], he highlights that there are two kinds 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 measures. Thereby, implementing controls and measures may not be enough to protect the whole corporate cybersecurity.

Gemalto [4] from its 2016 Breach Level Index (BLI) presents findings that included 1,378,509,261 breached records, 1,792 breach incidents, 52.2% of breaches without a certain number of compromised records, only 4.2% of data breaches of encrypted files, data records were lost or stolen with this frequency:

- 44 every second
- 2,623 every minute
- 157,364 every hour
- 3,776,738 every day

The top sources of these breaches were malicious outsiders (68%), State sponsored (1%), hacktivists (3%), malicious insiders (9%) and accidental loss (19%). The major cybercriminal trends during 2016 included the target of wider nets by hackers, the theft of accounts and personal identifiable information to target high value cyber victims, the infiltration of entertainment and social media sites to launch cyberattacks and the increase of ransomware attacks like the latest global *Wanna Cry* ransomware cyberattacks.

IT audits are being redefined to include cybersecurity but there aren't clear guidelines or consensus to what areas, sub-

978-1-5386-2644-3/17 $31.00 © 2017 IEEE
DOI 10.1109/INCISCOS.2017.20

areas, domains or sub-domains to include in a cybersecurity audit. The audit scope is easier assigned if the target organization has implemented a specific cybersecurity framework or standard from any organization like the International Organization for Standardization (ISO 27032), the National Institute of Standards and Technology (NIST), the International Organization for Standardization ISO 27001, the International 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). This approach is exclusively to verify cybersecurity compliance to a specific framework or to a specific industry or sector and cybersecurity audits verify that controls are in place and are effective.

Donaldson et al. [5] 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.

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

II. Literature Review

Every time a group of auditors will be participating in an IT, Information Security or compliance audit, there will be consistent phases like planning, defining objectives and scope, clarifying the terms of engagements, conducting the audit, verifying evidence, evaluating risks, reporting the audit findings and schedule follow up tasks. Planning a cybersecurity audit is not different than any type of audit but can take a lot of effort due to the complexity of many cybersecurity domains.

According to Protiviti [6], cybersecurity is positioned as the top technology challenge for IT audit leaders and professionals and organizations should consider reviewing on a continuous basis their IT audit plans to address the cybersecurity threats and emerging technologies. This study shows than conducting cybersecurity audits are more important in certain geographic areas than others – North America (70%), Europe (58%), Latin America (56%), Oceania (53%), Middle East (50%), Africa (49%) and Asia (35%). However, North America is the only area where conducting cybersecurity audits are within the Top 3 priorities when it comes to auditing. Protiviti [7], also points out imperative key considerations for directors including culture, competitiveness, compliance and cybersecurity. Cybersecurity internal audits can assist board of directors and senior management in these particular ways:

1. Assessment of corporate processes to weigh the attention to high-value information and systems
2. Better understanding of the cyberthreat landscape
3. Evaluation of the organizational cyber incident response readiness

Deloitte [8] considers the importance of conducting internal audits to verify the cybersecurity control's effectiveness, cyber risk management is based on roles and responsibilities:

1. First Line of defense: Business and IT functions
2. Second Line of defense: Information and technology risk management
3. Third Line of defense: Internal audits

Deloitte's cybersecurity framework emphasizes that some cybersecurity domains can be assessed through existing IT but most cyber capabilities are not reviewed by the internal audits' scope. This particular framework includes risk/compliance management, development life cycle, security program, third-party management, information/asset management, access management, threat/vulnerability management, data management and protection, risk analytics, crisis management and resiliency, security operation and security awareness and training. Furthermore, Deloitte's framework is aligned with industry frameworks like 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).

ISACA [9] highlights on its report the relevance of implementing cybersecurity controls as part of an overall framework and strategy, the need for assurance that can be achieved by management reviews, cyber risk assessments and cybersecurity controls audits.

Hollingsworth summarized from his In-house cybersecurity audit study [10], that the whole audit process produced evidence and remediation requirements to develop better cybersecurity controls; the involved audit team was able to remediate system documentation and processes weaknesses during the pre-audit phase and he concluded that Senior management support and attention to cybersecurity audits is becoming a standard for business circles and other sectors.

Ross indicates that one global challenge in evaluating cybersecurity preparedness is the absence of standards to conduct cybersecurity audits. Simple, subtle and meaningful questions for auditors include:

Are we secure against cyberattacks?

What exactly is the cybersecurity audit process?

What percentage of our data is encrypted?

How many programs have not been maintained for a specific amount of time?

In addition, there aren't any metrics to measure cybersecurity audits and the cybersecurity audit topic is poorly understood as it transforms really quickly [11]. Khan considers that to cover a meaningful scope for planning a cybersecurity audit,

the auditors must include all relevant areas of any organization; these areas are customer operations, finance, human resources, IT systems and applications, legal, purchasing, regulatory affairs, physical security and all applicable third parties that have relationships with the business [12].

III. The CyberSecurity Audit Model (CSAM)

The CyberSecurity Audit Model (CSAM) proposed in this article, is a new exhaustive 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. The CSAM can be implemented to conduct internal or external cybersecurity audits, this model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls. 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. The organization can be any small, medium or large enterprise, the model is also applicable to any Non-Profit Organization (NPO).

The CyberSecurity Audit Model (CSAM) contains overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessment and an evaluation scorecard "Fig. 1".

A. Overview

This section introduces the model organization, the working methodology and the possible options for implementation.

B. Resources

This component provides links to additional resources to help understanding some of the cybersecurity topics:

- Cybersecurity: NIST Computer Security Resource Center [13], Financial Industry Regulatory Authority (FINRA) cybersecurity practices [14] and Homeland Security cybersecurity [15].
- National Cybersecurity Strategy (NCS): North Atlantic Treaty Organization (NATO) cybersecurity strategy [16], European Union Agency for Network and Information Security (ENISA) cybersecurity strategy [17] and Organisation for Economic Co-operation and Development (OECD) comparative analysis of national cybersecurity strategies [18].
- Governance: PricewaterhouseCoopers Board cybersecurity governance [19] and MITRE cybersecurity governance [20].
- Cyber Assets: NERC critical cyber assets [21].
- Frameworks: Foresite common cybersecurity frameworks [22], United States Computer Emergency Readiness Team (US-CERT) framework [23] and ISACA's implementing the NIST cybersecurity framework [24].
- Architecture: Trusted Computer Group (TCG) architect's guide [25] and US Department of Energy's IT security architecture [26].
- Vulnerability Management: SANS vulnerability assessment [27] and Homeland Security vulnerability assessment and management [28].
- Cyber Threat Intelligence: SANS – Who's using cyberthreat intelligence and how? [29].
- Incident Response: Computer Security Incident Response Team (CSIRT) frequent asked questions [30].
- Digital Forensics: SANS forensics whitepapers [31].
- Awareness: National Cyber Security Alliance – Stay safe online [32] and PCI DSS -Best practices for implementing security awareness program [33].
- Cyber Defense: SANS- The sliding scale of cybersecurity [34].
- Disaster Recovery: Financial Executives International (FEI) Canada – Cybersecurity and business continuity [35].
- Personnel: Kaspersky – Top 10 tips for educating employees about cybersecurity [36].

C. Domains

The CSAM contains 18 domains. Domain 1 has been designed specifically for Nations States and domains 2-18 are applicable to any organization "Fig. 2".

D. Sub-domains

All domains have at least one sub-domain but in certain cases there might be several sub-domains per domain.
The sub-domains are:

- Cyberspace
- Governance
- Strategy
- Legal and Compliance
- Cyber Asset Management

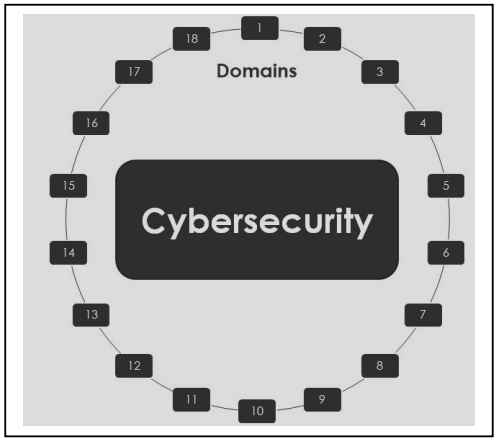


Fig. 1. The CyberSecurity Audit Model (CSAM)

- Cyber Risks
- Frameworks and Regulations
- Architecture
- Networks
- Information
- Systems
- Applications
- Vulnerability Management
- Threat Intelligence
- Incident Management
- Digital Forensics
- Awareness Education
- Cyber Insurance
- Active Cyber Defense
- Evolving Technologies
- Disaster Recovery
- Onboarding
- Hiring
- Skills
- Training
- Offboarding

E. Controls

Each domain has sub-domains that are assigned a reference number. Controls are identified by clause numbers and an assigned checklist. In order to verify the control evaluation, the cybersecurity control is either in place or inexistent.

F. Checklists

Each checklist is linked to a specific domain and the subordinated sub-domain. The checklist verifies the validity of the cybersecurity sub-controls in alignment with a control clause. The cybersecurity auditors have the option to collect evidence to verify the sub-control compliance "Fig. 3".

G. Sub-Controls

The Sub-Controls are evaluated using the checklists.
The assessment of each sub-control can be in compliance, with a minor nonconformity or with a major nonconformity:

Domains	Domains
1- Nation States	10- Threat Intelligence
2- Governance and Strategy	11- Incident Management
3- Legal and Compliance	12- Digital Forensics
4- Cyber Assets	13- Awareness Education
5- Cyber Risks	14- Cyber Assurance
6- Frameworks and Regulations	15- Active Cyber Defense
7- Architecture and Networks	16- Evolving Technologies
8- Information, Systems and Applications	17- Disaster Recovery
9- Vulnerability Identification	18- Personnel

Fig. 2. The CyberSecurity Audit Model (CSAM) domains

-Compliant: The cybersecurity sub-control is active and aligned with the specific requirements.
-Minor Nonconformity: The cybersecurity sub-control has not been fulfilled and it represents a minor risk.
-Major Nonconformity: The cybersecurity sub-control does not exist or it is a complete failure and it represents an unacceptable risk.

H. Guideline Assessment

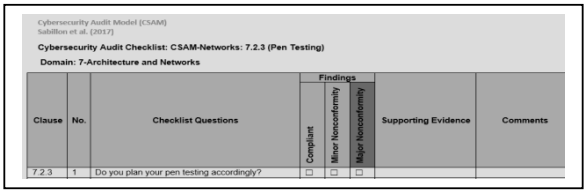
The guideline assessment only applies to the Nation States domain. The guidelines are evaluated for cybersecurity culture, National Cybersecurity Strategy (NCS), cyber operations, critical infrastructure, cyber intelligence, cyber warfare, cybercrime and cyber diplomacy.

I. Evaluation Scorecard

The control, guideline and sub-control evaluation is calculated after the audit has been completed. The evaluation consists in assigning scores and ratings for each control, guideline and sub-control "Fig. 4".
We calculate the final cybersecurity maturity rating of the Nation States domain by using the following criteria. The score can be mapped to a specific maturity level:

Immature (I): 0-30
The Nation State does not have any plans to manage its cyberspace. A National Cybersecurity Strategy (NCS) or Policy is inexistent.
Developing (D): 31-70
The Nation State is starting to focus on national cybersecurity. If technologies are in place, the Nation State needs to focus on key areas to protect cyberspace.
Mature (M): 71-90
While the Nation State has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.
Advanced (A): 91-100
Nation State has excelled in national cybersecurity and cyberspace practices. There is always room for improvement. Nation State could become an international leader and help other Nation States with cybersecurity and cyberspace matters.
And for domains 2-18 "Fig. 5", 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:
Immature (I): 0-30
The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak.


Cybersecurity Audit Model (CSAM)
Sabillon et al. (2017)
Cybersecurity Audit Checklist: CSAM-Networks: 7.2.3 (Pen Testing)
Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings: Compliant	Findings: Minor Nonconformity	Findings: Major Nonconformity	Supporting Evidence	Comments
7.2.3	1	Do you plan your pen testing accordingly?	☐	☐	☐		

Fig. 3. A Checklist of the CyberSecurity Audit Model (CSAM)

Domain		1.Nation States
Sub-Domain		1.1 Cyberspace
Control Evaluation		0-3 Immature 4-5 Developing 6-7 Mature 8 Advanced
Yes	✓	
Guideline Assessment		0-30 Immature 31-50 Developing 51-69 Mature 70-100 Advanced
Compliant	✓	

Fig. 4. Cybersecurity Maturity ratings for the Nation States domain

The organization has not implemented a comprehensive cybersecurity program.

Developing (D): 31-70

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 towards staff, processes, controls and regulations.

Mature (M): 71-90

While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

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.

The Institute of Internal Auditors (IIA) [37] emphasizes that internal audit plays an essential role to evaluate any organization's cybersecurity risk by addressing:

> "*Who has access to the organization's most valuable information?*
> *Which assets are the likeliest targets for cyberattacks?*
> *Which systems would cause the most significant disruption if compromised?*
> *Which data, if obtained by unauthorized parties, would cause financial or competitive loss, legal ramifications, or reputational damage to the organization?*
> *Is management prepared to react timely if a cybersecurity incident occurred?"*

As a result, The Institute of Internal Auditors (IIA) introduced the *Cybersecurity Risk Assessment Framework* stressing that when components are not designed or operating well, the repercussions will not include any plans to deal with cyberthreats and emerging risks. The *Cybersecurity Risk Assessment Framework* covers the following components:

1. Cybersecurity Governance
2. Inventory of Information Assets for Data, Infrastructure and Applications
3. Standard Security Configurations
4. Information Access Management
5. Prompt Response and Remediation
6. Ongoing Monitoring

Cybersecurity Audit Model (CSAM)						
No.	Domain	Ratings				Score
		I	D	M	A	
2	Governance and Strategy	☐	☐	☐	☐	
3	Legal and Compliance	☐	☐	☐	☐	
4	Cyber Assets	☐	☐	☐	☐	
5	Cyber Risks	☐	☐	☐	☐	
6	Frameworks and Regulations	☐	☐	☐	☐	
7	Architecture and Networks	☐	☐	☐	☐	
8	Information, Systems and Apps.	☐	☐	☐	☐	
9	Vulnerability Identification	☐	☐	☐	☐	
10	Threat Intelligence	☐	☐	☐	☐	
11	Incident Management	☐	☐	☐	☐	
12	Digital Forensics	☐	☐	☐	☐	
13	Awareness Education	☐	☐	☐	☐	
14	Cyber Insurance	☐	☐	☐	☐	
15	Active Cyber Defense	☐	☐	☐	☐	
16	Evolving Technologies	☐	☐	☐	☐	
17	Disaster Recovery	☐	☐	☐	☐	
18	Personnel	☐	☐	☐	☐	
Final Cybersecurity Maturity Rating		☐	☐	☐	☐	

Fig. 5. Overall Cybersecurity Maturity ratings for Organizations

IV. Discussion

This study presents the design of the CyberSecurity Audit Model (CSAM). The aim of the this model is to introduce a cybersecurity audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS). This model was envisioned as a seamless and integrated cybersecuity audit model to assess and measure the level of cybersecurity maturity and cyber readiness in any type of organization, no matter in what industry or sector the organization is positioned. Moreover, by adding guidelines assessment for the integration of a national cybersecurity policy, program or strategy at the country level.

Many cybersecurity frameworks are mostly oriented towards a specific industry like the *"PCI DSS"* for credit card security, the *"NERC CIP Cyber Security"* for the bulk power system or the *"NIST Cybersecurity Framework"* for protecting national critical infrastructure. But, all the existing frameworks do not provide a one-size fits all for planning and conducting cybersecurity audits. The necessity to mapping against specific cybersecurity frameworks is because of regulatory requirements, to satisfy the demands of industry regulators, to comply with internal or external audits, to satisfy business purposes and customer requirements or simply by improving the enterprise cybersecurity strategy.

We compared our model in "Table I." to highlight the main features against *"The Cybersecurity Framework (CSF) Version 1.1: NIST (2017)"* and *"The Audit First Methodology: Donaldson et al. (2015)"*. The CSAM is not for a specific industry, sector or organization – On the contrary, the model can be utilized to plan, conduct and verify cybersecurity audits everywhere. The CSAM has been designed to conduct partial or complete cybersecurity audits either by a specific domain, several domains or the comprehensive audit for all domains.

TABLE I. COMPARISON OF SOME CYBERSECURITY AUDIT MODELS

Audit Model or Framework	Description
The Cybersecurity Framework (CSF) Version 1.1: NIST (2017) [38]	The initial version was conceived in 2014 to improve cybersecurity of critical infrastructure. The version 1.1 manages cybersecurity risks for critical infrastructure.It is composed of the Framework Core, the Framework Implementation Tiers and the Framework profiles. The Framework Core includes five functions – Identify, Protect, Detect, Respond and Recover; then each of these functions have categories and subcategories. In addition, the Core contains Informative resources like cybersecurity standards, guidelines and best practices. The Tiers define cybersecurity context organized from partial to adaptive tier. The Profile presents the outcomes based on organizational needs. The current profile can later be compared with a target profile.
The Audit First Methodology: Donaldson et al. (2015) [39]	This methodology considers other cybersecurity controls and leaves preventive control excecution until the end. This audit includes five different phases: 1. Threat analysis: This phase identifies Confidentiality, Integrity and Availability (CIA) threats that may impact IT and corporate data. Threat impact and indicators are defined. 2. Audit controls: It includes the design of threat audit controls. 3. Forensic controls: This phase helps to implement the required forensic controls for the enterprise cybersecurity functional areas: 1) Systems administration 2) Networks 3) Applications 4) Endpoints, servers and devices 5) Identity, authentication and access 6) Data protection and cryptography 7) Monitoring, vulnerabilities and patch management 8) Availability, disaster recovery and physical protection 9) Incident management 10) Supply chain and asset management 11) Policy, audit, e-Discovery and training 4. Detective controls: Detective controls are designed to alert, detect, stop and repel cyberattacks. 5. Preventive controls:These controls block undesired activities and stop them from ocurring.
The CyberSecurity Audit Model (CSAM): Sabillon et al. (2017)	The CSAM comprises overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessment and an evaluation scorecard. Domain 1-Guideline assessment are specific for Nation States and domains 2-18 are applicable to any type of organization. Certain domains have specific sub-domains where controls are evaluated. Then the checklists verify compliance about specific sub-controls based on domain/sub-domain. The scorecard results determine the domains rating and score that will produce the overall cybersecurity maturity rating.

CONCLUSIONS

This study introduces the CyberSecurity Audit Model (CSAM) design and all its components, the aim of this model is to evaluate and measure the cybersecurity assurance, maturity and cyber readiness in any organization. In addition, the model can evaluate the effectiveness of cybersecurity guidelines for any Nation State linked to its national cybersecurity strategy or policy.

The CSAM was tested, implemented and validated along with the Cybersecurity Awareness TRAining Model (CATRAM) in a Canadian higher education institution. A research case study is being conducted to validate both models and the findings will be published accordingly.

Since there aren't universal acceptance or standardization in terms of defining cybersecurity audit scopes, aims and domains, further research is required and encouraged in the cybersecurity areas of assurance and 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 NV, "2016 Mining for Database Gold: Findings from the 2016 Breach Level Index," March 2017.
[5] S. Donaldson, S. Siegel, C. Williams and A. Aslam, Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. New York: Apress, 2015, pp. 200-201.
[6] Protiviti, "A Global Look at IT Audit Best Practices: Assessing the International Leaders in an Annual ISACA/Protiviti Survey," Protiviti Inc, 2017.
[7] Protiviti, "Board Perspectives: Risk Oversight," Protiviti Inc, 2017.
[8] Deloitte, "Cybersecurity: The role of Internal Audit," Deloitte Development LLC, 2015.
[9] ISACA, "Auditing Cyber Security: Evaluating Risk and Auditing Controls," ISACA, 2017.
[10] C. Hollingsworth, "Auditing fro FISMA and HIPAA: Lessons Learned Performing an In-House Cybersecurity Audit," ISACA Journal, vol. 5, pp. 1-6, 2016.
[11] S. Ross, "Cybersecurity for a "Simple" Auditor," ISACA Journal, vol.6, pp. 1-2, 2015.
[12] M. Khan, "Managing Data Protection and Cybersecurity-Audit's Role," ," ISACA Journal, vol. 1, pp. 1-3, 2016.
[13] National Institute of Standards and Technology (NIST), "NIST Special Publications SP", 2017.
Available at <http://csrc.nist.gov/publications/PubsSPs.html>
[14] Financial Industry Regulatory Authority (FINRA), "Report on Cybersecurity Practices", pp 1- 46, February 2015.
Available at
<https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf>
[15] U.S. Department of Homeland Security, "Cybersecurity," September 2016.
Available at <https://www.dhs.gov/topic/cybersecurity>
[16] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Cyber Security Strategy Documents," August 2015.
Available at < https://ccdcoe.org/strategies-policies.html>
[17] Ministry of Economic Affairs and Communication, "2014-2017 Estonia Cybersecurity Strategy," ENISA, 2017.
Available at < https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf>
[18] Organisation for Economic Co-Operation and Development (OECD), "Cybersecurity Policy Making at a Turning Point," OECD, 2012.
Available at
<http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>
[19] Pricewaterhouse Coopers (PwC), "PwC's Board Cybersecurity Governance Framework," PwC, 2016.
Available at
<https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf>
[20] D. Bodeau, S. Boyle, J. Fabius-Greene and R. Graubart, "Cyber Security Governance," MITRE, 2010.
Available at<
https://www.mitre.org/sites/default/files/pdf/10_3710.pdf>

[21] North American Electric Relaibility Corporation (NERC), "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets," NERC, 2010.
Available at <www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf>
[22] Foresite, "Quick guide to common Cybersecurity Frameworks," June 2016.
Available at < https://www.foresite.com/blog/quick-guide-to-common-cybersecurity-frameworks/>
[23] United States Computer Emergency Readiness Team (US-CERT), "Cybersecurity Framework," US-CERT, 2017.
Available at < https://www.us-cert.gov/ccubedvp/cybersecurity-framework>
[24] ISACA, Implementing the NIST Cybersecurity Framework. Rolling Meadows: ISACA, 2014.
[25] Trusted Computing Group, "Architect's Guide: Cybersecurity," 2013.
Available at < https://www.trustedcomputinggroup.org/wp-content/uploads/Architects-Guide-Cybersecurity.pdf>
[26] U.S. Department of Energy, "IT Security Architecture," February 2007.
Available at <https://energy.gov/sites/prod/files/cioprod/documents/DOE_Security_Architecture.pdf>
[27] R. Boyce, "Vulnerability Assessment: The Pro-Active Steps to Secure your Organization," SANS Institute, 2001.
Available at < https://www.sans.org/reading-room/whitepapers/threats/vulnerability-assessments-pro-active-steps-secure-organization-453>
[28] Department of Homeland Security, "Vulnerability Assessment and Management," NICSS, 2012.
Available at < https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/vulnerability-assessment-and-management >
[29] D. Shackleford, "Who's using Cyberthreat Intelligence and how?," SANS Institute, 2015.
Available at <https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767 >
[30] CERT Division, "CSIRT Frequently Asked Questions," Carnegie Mellon University, 2017.
Available at <https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm>
[31] SANS Institute, "SANS Forensics Whitepapers," SANS Institute, 2017.
Available at <https://digitalforensics.sans.org/community/whitepapers>
[32] National Cyber Security Alliance, "Stay Safe Online," NCS, 2017.
Available at < https://staysafeonline.org/ncsam/>
[33] PCI Security Standards Council, "Best Practices for implementing a Security Awareness Program," PCI DSS, October 2014.
Available at <https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf>
[34] R. Lee, "The Sliding Scale of Cybersecurity," SANS Institute, 2015.
Available at < https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240>
[35] Financial Executives International (FEI), "Financial Executives, Cyber Security & Business Continuity," Canadian Executives Research Foundation (CFERF), 2014.
Available at <https://www.feicanada.org/enews/file/CFERF%20studies/2013-2014/IBM%20Cyber%20Security%20final3%202014.pdf >
[36] Kaspersky Lab, "Top 10 Tips for Educating Employees about Cybersecurity," AO Kaspersky Lab, 2015.
Available at <http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf>
[37] The Institute of Internal Audits (The IIA), "Assessing Cybersecurity Risk: Roles of the Three Lines of Defense," The IIA, September 2016.
[38] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity", version 1.1, January 2017.
[39] S. Donaldson, S. Siegel, C. Williams and A. Aslam, Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. New York: Apress, 2015, pp. 201-204.