Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 4

2023

Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law

Bernard Ngalim
University of the Free State, 2020574279@ufs4life.ac.za

Recommended Citation

Ngalim, Bernard (2023) "Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 4.
DOI: https://doi.org/10.32727/8.2023.29
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/4

Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law

Abstract

This paper reviews cybersecurity laws and regulations in Cameroon, focusing on cybersecurity and information security audits and risk assessments. The importance of cybersecurity risk assessment and the implementation of security controls to cure deficiencies noted during risk assessments or audits is a critical step in developing cybersecurity resilience. Cameroon's cybersecurity legal framework provides for audits but does not explicitly enumerate controls. Consequently, integrating relevant controls from the NIST frameworks and ISO Standards can improve the cybersecurity posture in Cameroon while waiting for a comprehensive revision of the legal framework. NIST and ISO are internationally recognized as best practices in information security systems and cybersecurity risk management. This paper highlights the lack of specific international law provisions addressing cybersecurity audits and risk assessments. Overall, the paper highlights the importance of continuous risk assessment and monitoring, implementation of security controls, and compliance with organizational policies, relevant laws and regulations to ensure the adequate protection of information systems. Finally, the paper underscores the importance of improving Cameroon's cybersecurity regulations by integrating provisions from NIST and ISO.

Keywords

NIST, ISO, Cybersecurity, Audits, Risk Assessment, Information Security Systems

Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law

Bernard Ngalim
Human Rights Center
University of the Free State
Bloemfontein, South Africa
2020574279@ufs4life. ac. za
ORCID ID: 0009-0009-5278-9078

Abstract - This paper reviews Cybersecurity laws and regulations in Cameroon, focusing on Cybersecurity and information security audits and risk assessments. The importance of Cybersecurity risk assessment and the implementation of security controls to cure deficiencies noted during risk assessments or audits is a critical step in developing Cybersecurity resilience. Cameroon's Cybersecurity legal framework provides for audits but does not explicitly enumerate controls. Consequently, integrating relevant controls from the NIST frameworks and ISO Standards can improve the Cybersecurity posture in Cameroon while waiting for a comprehensive revision of the legal framework. NIST and ISO are internationally recognized as best practices in information security systems and Cybersecurity risk management. This paper highlights the lack of specific international law provisions addressing Cybersecurity audits and risk assessments. Overall, the paper highlights the importance of continuous risk assessment and monitoring, implementation of security controls, and compliance with organizational policies, relevant laws and regulations to ensure the adequate protection of information systems. Finally, the paper underscores the importance of improving Cameroon's Cybersecurity regulations by integrating provisions from NIST and ISO.

Keywords - Cameroon, Cybersecurity, Cybersecurity audits, Information security assessment, NIST, ISO, cyber-attacks

I. Introduction

Cameroon, like many other countries in the world, is not immune to the challenges posed by cyber threats requiring constant cybersecurity audits and risk assessments. Cybersecurity audits and risk assessments evaluate an organization's cybersecurity controls [1]. Internal audit teams or independent auditors audit an organization's cybersecurity posture to verify compliance with policies and procedures [2]. On the other hand, cybersecurity risk assessments are conducted internally to provide a high-level analysis of an organization's overall cybersecurity maturity, analyze the effectiveness of cybersecurity controls, and identify potential vulnerabilities and threats [3]. These evaluations are becoming increasingly relevant because the landscape of online business has significantly transformed in recent times due to the rapid technological advancements and the adoption of assets that connect business operations to cyberspace [4]. The increased reliance on information technology systems and the internet has brought about significant opportunities for businesses and individuals in Cameroon [5]. Despite the benefits of technology, information systems and data are vulnerable to cyber-attacks which can result in significant losses [6]. This has led to the enactment of laws, regulations, standards, and frameworks that seek to protect individuals and organizations from cyber-attacks. With the growth of digital transformation in Cameroon, the country has experienced increased cyber-attacks, and data breaches [7]. In 2021, the National Agency for Information and Communication Technologies (ANTIC) reported that Cameroonians lost $16 million to online scamming, phishing, skimming and other cyber-related crimes [8]. Private organizations lost more than US$8 million over the past decade due to intrusions into their information systems [9]. These cyber-attacks compromise the fundamental principles of information security systems, which include the confidentiality, integrity, and availability of information that is stored and processed [10]. In response to the growing risks and threats posed by cybersecurity, the government of Cameroon began developing a legal framework in 2010 to address these challenges and protect its information security systems. Key among these is Cameroon's Cybersecurity and Cybercrime Law of 2010. The law seeks to regulate the use of the internet and ensure that crimes committed through cyberspace, and the information and security systems are recognized and sanctioned as cybercrimes [11]. The purpose of this paper is to critically examine the legal requirements for conducting cybersecurity risk assessments and auditing cybersecurity and information systems in Cameroon. The paper will identify and discuss the key laws and regulations that have been enacted by the Cameroonian government to govern cybersecurity auditing and risk assessments, highlight the challenges hindering the effective implementation of these laws, and propose solutions to address these challenges. The paper will also draw lessons

from international frameworks and standards regulating information security risk assessments and cybersecurity audits particularly the International Standard Organization's (ISO) standards and the United States' National Institutes for Standards and Technology Special Publications (NIST SP). The first section provides an overview of the cybersecurity landscape. The next section describes the nature and extent of cyber threats, the sectors mostly affected, and the impact of cyber-attacks on the economy. Then the third part reviews laws regulating cybersecurity audits and risk assessments and the need for information security systems and cybersecurity audits. The article uses cybersecurity interchangeably with information security.

II. OVERVIEW OF INFORMATION SECURITY SYSTEMS AND CYBERSECURITY AUDITING

Organizations that depend on information technology to achieve their business objectives and are connected to other organizations that rely on information technology must protect their information systems from cyber-attacks [12]. Information systems face potential risks and dangers that can harm not just the organization that owns the system but also individuals, other organizations, and even the nation as a whole [13]. These threats can take advantage of an information system's security vulnerabilities to access, alter, or disrupt the information being processed, stored, or transmitted by the organization [14]. The three main types of harms that can result from these threats include the loss of confidentiality, integrity, and availability of processed, stored, or transmitted information [15]. To protect information systems and the confidential data stored in an organization's information systems from attacks, it is essential to have a clear understanding of the information contained, its sources, and the associated risks through an audit [16]. The understanding of information contained within the information technology systems is necessary to implement effective security measures that can mitigate the identified risks and prevent unauthorized access, modification, or disclosure of the information [17]. By taking a proactive approach in identifying risks to information security, organizations can reduce the likelihood of cyber threats and minimize the impact of potential security incidents through risk management [18]. Risk identification would include a detailed evaluation and examination of an organization's information technology systems to identify potential security risks and vulnerabilities and compliance with policies, procedures, and controls [19]. It is a comprehensive process that involves reviewing all aspects of an organization's information systems, including hardware, software, network architecture, and data storage, to assess the level of protection against cyber threats [20]. The goal of information systems and cybersecurity audits and risk assessments is to identify weaknesses in an organization's security measures and recommend improvements to ensure the confidentiality, integrity, and availability of its data and systems [21]. Overall, information security and cybersecurity risk assessments and audits are crucial steps in protecting an organization's valuable assets from cyber-attacks. According to Borky and Bradley, risk identification and compliance requires having tools and processes in place to monitor and analyze security-related events [22]. These include detecting and recording any suspicious activity, analyzing this data to identify potential threats, and reporting any incidents that may indicate a compromise or unauthorized action [23]. It is important to have risk assessment and audits in place to ensure that organizational, technological, and personal security procedures are being followed and to identify any potential threats before they can cause harm to an organization's information security system. Chapple adds that risk identification and audits verify that an organization adheres to its internal policies, follows established industry standards, and meets all legal and regulatory obligations [24].

A. Need to regularly audit cybersecurity in Africa.

The prevailing state of cybersecurity infrastructure in African businesses reveals a significant deficiency, with over 90% of these entities lacking the necessary measures required to safeguard their operations [25]. This highlights a critical gap in the technology, policies, and procedures required to protect computer systems, networks, and data from cyber threats such as hacking, phishing, malware, and ransomware. Consequently, these businesses are at a heightened risk of experiencing data breaches, financial losses, and reputational damage. According to the International Police (INTERPOL), online scams, digital extortion, business email compromise, ransomware, and botnets are the most pressing cyber threats in Africa [26]. INTERPOL warns cybercriminals are becoming more advanced, systematic, and complex in their operations [27]. The transnational nature of cybercrime poses significant obstacles to investigations and legal action across various jurisdictions [28]. Kshetri rightly argues that there has been an increase in cyberattacks in Africa because many computer systems in the continent are vulnerable, and cybersecurity practices in Africa are often not strong enough to prevent these attacks [29]. The proliferation of pirated software in Africa makes computer systems vulnerable to cyber-attacks since such software does not receive necessary security updates and patches [30]. The continuous shift to digitalization in Africa means that business information is now more vulnerable to all the cybersecurity threats [31]. This paper posits that to protect themselves, businesses need to implement strong information security systems and cybersecurity measures to ensure that their data remains secure and confidential. Strong information systems security and cybersecurity measures are required to ensure business continuity and minimize the impact of cybersecurity incidents on businesses through the adoption of an information security management system [32]. Accordingly, organizations must adopt adequate protection of information assets, safeguard their operations, and maintain their competitive edge. However, African organizations must first recognize the value of information as an asset and implement proper protection and management measures to prevent loss, exposure, or destruction [33]. One such measure is conducting an information security system's audit that can provide organizations with crucial insights into the risks associated with

their cybersecurity networks [34]. This paper argues that Cameroonian businesses must adopt an information security risk assessment and cybersecurity audit posture that will enable them to identify and address security loopholes and potential vulnerabilities before cyber attackers and hackers can exploit them. Briefly, by following best practices, organizations can ensure that their cybersecurity audits effectively identify potential risks to their systems and data. Consequently, organizations can protect themselves from cyber threats by implementing best practices to fix threats detected during cybersecurity audits and risk assessments. This approach can help organizations to strengthen their cybersecurity posture and reduce the likelihood of a successful cyber-attack. In adopting a cyber resilient posture, Cameroonian organizations must understand that cyber threat actors do not wait for legislation but attack businesses irrespective of the strength of domestic laws.

B. The Most Vulnerable Industries to Cyber-attacks in Africa

Globally, in 2022, the manufacturing industry faced the highest number of cyber-attacks, followed by finance, insurance and consumer services [35]. In Africa, the financial cost of cyber-attacks for businesses has been increasing [36]. In 2013, the highest estimated costs were $47 million in Côte d'Ivoire and $27 million in Senegal [37]. In 2017, while Nigeria had an estimated annual loss of $649 million, and Kenya lost about $210 million, with financial institutions, government, and e-commerce being the top three most impacted industries in Africa [34]. In addition to these threats, Ajiji rightly argues that small businesses in Africa are also at risk of cyber-attacks as they often struggle with inadequate budgets for cybersecurity and a lack of consulting professionals for leadership and processes [39]. Despite these statistics, 96 percent of "cybersecurity incidents go unreported or unresolved, meaning that cyber threats in Africa are likely much worse than recognized" [40]. This underscores the importance of investing in cybersecurity measures and increasing awareness about cyber threats in the region. Without these efforts and the expansion of businesses and more reliance on cyberspace for operations, organizations and individuals in Africa will witness more cyber-attacks resulting in significant financial, reputational, and even physical harm.

The above statistics reveal that almost all sectors of business, government, and even individuals are at risk of cybersecurity attacks in Africa. As the world becomes increasingly digitized and more businesses open up to information technology, the threat of cyber-attacks is growing in Africa. This emphasizes the obligation that businesses, governments, and individuals must take steps to protect their information systems against attacks. This paper suggests investing in cybersecurity measures such as firewalls, antivirus software, and encryption amongst others although they may be expensive to obtain in Africa. Businesses and governments should also conduct regular security audits to identify vulnerabilities and address them before they can be exploited by attackers. Additionally, it is important for organizations to have a robust cybersecurity incident response system in place so that they can quickly respond to and contain any cyber-attacks that do occur [41]. Individuals must also take steps to protect themselves from cyber-attacks because cyber threat actors can target them both as individuals and professionals [42]. Individual steps to protect against cybersecurity threats and attacks could include using strong passwords, being cautious when opening emails or clicking on links from unknown sources, and keeping software and devices up to date with the latest security patches [43]. Individuals need to regularly back up their data so that they can recover it in the event of a cyber-attack.

III. REGULATING INFORMATION SECURITY RISK ASSESSMENT AND CYBERSECURITY AUDITS

The fast-paced advancements in information technology have outpaced international laws, leaving gaps in legal frameworks and posing challenges in enforcing technology-related laws and protecting individuals and organizations from potential harm [44]. Hollis posits that the difficulties in applying international law to cybersecurity arise from the silence of specific treaties addressing cybersecurity issues [45]. Although there is no specific international law regulating cyberthreats, we can rely on customary international law rules or use existing law regulating specific aspects of law and apply them to cybersecurity issues. However, it has been challenging to determine what states have been doing to regulate cyberspace [46]. Although the African Union Convention on Cybersecurity and Personal Data Protection and the Budapest Convention on Cybercrime have been adopted by the African Union and the Council of Europe, respectively, neither convention specifically regulates auditing information security systems.

In the absence of international law governing cybersecurity audits, organizations can turn to NIST SP and ISO standards for guidance on cybersecurity audits and risk assessments. These frameworks encourage information systems audits and risk assessments by providing security requirements, controls and audit and assessment methodologies. Both standards focus on risk management and encourage the continuous monitoring, assessing, and responding to information security risks as they arise [47]. This risk management strategy helps an organization determine its compliance with cybersecurity regulations, standards, frameworks and policies [48]. These standards encourage organizations to establish internal policies, guidelines, and protocols to determine their risk appetite and establish mechanisms for risk treatment [49]. This strategic approach enables organizations to proactively anticipate and effectively handle challenges, ensuring operational resilience and preparedness for business continuity despite the threat landscape.

As there is currently no legally binding international framework for cybersecurity auditing or risk assessment, this section will examine Cameroon's audit requirements in light of

industry best practices. Specifically, the focus will be on the NIST SP frameworks and ISO standards. These frameworks are widely recognized and adopted by organizations around the world as a benchmark for best practices in cybersecurity auditing and risk assessment. An analysis of ISO 27001 and NIST frameworks show that they provide a comprehensive and systematic approach to cybersecurity auditing and risk assessment. They also offer guidelines and standards for organizations to establish, implement, maintain, and continually improve their information security management systems. Adherence to these frameworks, although non-obligatory, can help organizations mitigate cybersecurity risks, protect their critical assets, and enhance their overall cybersecurity posture. Moreover, compliance with these frameworks can also enhance an organization's credibility, reputation, and competitive advantage, as it demonstrates a commitment to information security best practices and a proactive approach to managing cybersecurity risks. As such, understanding how Cameroon's audit requirements align with these frameworks can provide valuable insights into the country's requirements for cybersecurity preparedness and identify areas for improvement. It is essential to clarify that ISO 27001 [50] and NIST [51] are voluntary standards organizations can implement to demonstrate their commitment to information security.

A. *An overview of Cameroon's cybersecurity legal framework*

Like most cybersecurity laws, Cameroon's information security law seeks to protect information systems, define offenses, and set obligations on using information and communication systems. The law requires operators, certification authorities, and electronic communication service providers to perform mandatory security audits [52]. Also, organizations operating electronic networks and information systems, processing personal data, and using or connected to electronic networks open to the public are subject to mandatory and periodic audits [53]. The law authorizes ANTIC to mandatorily and periodically audit electronic communication networks and information systems [54]. While the law does not explicitly mention risk assessment or business continuity, it requires providers to ensure availability and set up filters to protect personal data and privacy, which can be considered as risk assessment and business continuity planning forms [55]. To guarantee the privacy, reliability, and accessibility of information systems, operators need to actively apply technical and administrative strategies for securing services and managing risks [56]. Moreover, they have to set up ANTIC approved mechanisms to avoid disruptions, preserve system integrity, and safeguard data from radiation or unauthorized access [57]. Cybersecurity audits can be performed by either ANTIC or by private auditors who have received accreditation from ANTIC [58].

B. *Overview of Critical Terms*

1) *Audit*

ISO 19011 and Cameroon's cybersecurity law define an audit as a systematic evaluation or examination process that follows a structured and organized approach to assessing systems and determining the extent to which specific criteria are met or fulfilled [59]. However, there are some differences between the two definitions. The ISO 19011 definition is more general and can apply to various audits, while the Cameroon cybersecurity law definition focuses explicitly on security audits. The ISO 19011 definition emphasizes the independence and documentation of the process, whereas the Cameroon cybersecurity law definition does not. Instead, Cameroon's process includes a more detailed list of information security components and resources that should be examined. These include security actors, policies, actions, procedures, and various resources (organizational, technical, human, and financial) [60]. Furthermore, the Cameroon cybersecurity law definition mentions compliance tests and controls as part of the examination process, while the ISO 19011 definition does not [61]. According to ISO 27001, organizations seeking ISO compliance should perform internal audits to assess their information security management system's alignment with internal organizational requirements and ISO standards [62]. The NIST framework uses risk assessment instead of audit. However, without defining audits, NIST SP dedicates a complete control family to audits and accountability [63]. By understanding these different approaches and incorporating their strengths, organizations can develop robust audit and risk assessment practices that ensure the security and integrity of their information systems.

2) *Risk Assessment*

NIST 800-30, Cameroon cybersecurity law, and ISO 27001 underline the significance of assessing risks and security measures. "Risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur" [64]. The framework recommends risk assessments throughout the system development life cycle, considering various adverse impacts on different aspects of an organization and national security [65]. This approach encourages organizations to conduct risk assessment at all levels of business, irrespective of the type and size of business. Meanwhile, Cameroon's cybersecurity law focuses on operators evaluating their security systems and fostering cooperation between operators and users to execute security practices, measures, and techniques [66]. On the other hand, ISO 27001 highlights the essential requirements for organizations to establish a comprehensive information security risk assessment and management process [67]. ISO's risk assessment process emphasizes the importance of incorporating criteria for risk acceptance, consistent assessment, risk ownership identification, consequence analysis, likelihood determination, risk level evaluation, and overall risk evaluation to enhance security awareness and facilitate effective mitigation measures [68]. Risk assessments can be done at different stages

of the risk management process and throughout the system development life cycle [69]. This includes looking at information related to system design, testing results, and supply chain-related information [70]. Risk assessments help organizations choose the best controls through which they could mitigate or prevent risks and are important for determining early capabilities and tailoring guidance to prevent cyber-attacks [71]. The outcome of a risk assessment process should be documented and retained to inform security and business decisions [72].

3) Information Security System

The NIST definition of cybersecurity focuses on preventing damage to and restoring computers, electronic communication systems, and services, including the information contained within these systems [73]. It specifically highlights the importance of authentication and nonrepudiation, which are crucial aspects of ensuring secure communication and transactions [74]. The supplemental information security definition broadens the scope of this focus, encompassing the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction [75]. The information security definition also reinforces the significance of confidentiality, integrity, and availability. Cameroon's cybersecurity law governs electronic communications networks and information systems and seeks to build trust in information systems [76]. This objective underscores the non-repudiation principle and the integrity requirement that governs the cybersecurity space. By outlining trust as an objective sought by the Cameroon's cybersecurity law, the legislator also reminds businesses managing individual and personal information of the necessity to protect their reputation and assure customers of the safety of their information.

Cybersecurity is the "preservation of the confidentiality, integrity, and availability of information in Cyberspace" [77]. This definition aligns with the NIST's emphasis on preventing damage to and restoring computers, electronic communication systems, services, and the information in these systems. It explicitly underlines the importance of authentication and nonrepudiation, which are essential for secure communication and transactions. Although Cameroon's law is titled cybersecurity, the notion of cybersecurity alone restricts the scope of coverage since cybersecurity is only a component of information security. Taherdoost rightly argues that "information security fully includes cybersecurity as one of its components. Cybersecurity, on the other hand, is responsible to ensure the security of information against cyber threats and cyber-attacks while it is processed, stored, or transported " [78]. Although Cameroon's law is termed cybersecurity and cybercrime, it encompasses the breadth of information security, defines key terms in light of information security and mandates controls to protect information systems [79].

IV. Cybersecurity auditing process

Cybersecurity audits are important, as they are crucial in identifying risks, planning remediation strategies, and protecting systems from further cybersecurity attacks. Information security risks impact organizations internally and the impacts of their exploitation from a cyberattack could spread and harm their users, clients, partners and their information system systems. Stakeholders have a vested interest in understanding the information security posture of organizations they interact with. The ISO recognizes these vested interests and categorizes three types of audits and notes that organizations that audit their internal systems conduct first-party audits to understand their information security posture [80]. Clients and other stakeholders dealing with an organization conduct second-party audits to understand the type of security risks they could be exposed to during business [81]. Governments and third-party auditors conduct independent audits on behalf of the government or certification bodies [82]. Cameroon's law recognises only third-party audits where ANTIC or an organization accredited by ANTIC performs a third-party audit for specific organizations identified by ANTIC [83]. According to NIST, internal information risk assessments can provide a better understanding of the organization's security posture, access to internal resources and information, and a continuous improvement process [84]. Internal assessments can also be more cost-effective and timely than external assessments [85]. NIST advises that external assessments can provide an objective and independent perspective on an organization's security posture, specialized expertise, and a fresh perspective to identify vulnerabilities and weaknesses [86]. Although external assessors can help to benchmark an organization's security posture by comparing it to industry best practices and standards, they can be more expensive and time-consuming [87]. This background on auditing provides a foundation for understanding the auditing and risk assessment processes. The next section will review these processes in more detail.

A. Hierarchical Approach to Risk Assessment and Audits

The three tiers of organizational risk assessments and audits include the organizational, business process, and information system levels at any stage in the development lifecycle [88]. As organizations increasingly rely on information systems and face growing security threats, it is crucial for management to focus on information security for business continuity [89]. Addressing these challenges through effective information governance not only ensures compliance with laws and regulations but also supports good business practices and overall organizational survival [90]. Management involvement and commitment are crucial for the effective implementation of an Information Security Management System (ISMS) and the protection of information within an organization [91]. Organizational level assessments provide a high-level view of an organization's commitment to information security protecting, information security risks and risk management strategies supported by the organizational leadership [92]. Conducting an organizational-level assessment can help identify risks that affect the organization as a whole and develop risk management strategies

that align with the organization's mission and goals. Such assessments may not provide detailed information on specific risks, which can limit their usefulness for making informed risk management decisions. The legal framework in Cameroon does not provide clear instructions for auditing organizational and functional aspects of information security. Although Cameroon's legal framework mandates that audit reports cover the organizational and structural IT security posture, it falls short in offering auditors adequate controls and guidelines to follow during the audit process [93]. Based on this shortcoming, Cameroonian operators can significantly improve their governance-level information security by adopting and implementing the guidance provided by NIST and ISO. NIST and ISO include comprehensive organization-level controls addressing an organization's overall information security management through robust policies, procedures, and governance [94]. In addition to organizational-level audits, conducting business-level and information technology system-level audits can provide a more focused view on specific aspects of an organization's information security. These levels of assessment can help identify and address risks that may not be apparent at the organizational level.

Business process level assessments allow for a more detailed analysis of risks associated with specific business functions. According to NIST, a mission or business process-level assessment "focuses on risks associated with specific mission or business processes within the organization" and the purpose of this assessment is to "identify and evaluate the risks associated with the mission or business processes and to determine the appropriate security and privacy controls needed to manage those risks" [95]. Advantages of this level of assessment include the ability to identify risks that are unique to specific business processes and to develop risk management strategies that are tailored to those processes. Cameroon's legal framework mandates that certain industries perform audits on their management methods and security protocols within their businesses [96]. ISO provides a comprehensive set of physical and personnel controls to guide business level operations to safeguard business units against cybersecurity risks [97]. These controls are designed to protect an organization's assets, including its information, infrastructure, and personnel, by addressing potential vulnerabilities and threats. By implementing these controls, organizations can enhance their overall security posture and reduce their risk of cyber-attacks. This ensures that companies adhere to the necessary security standards and maintain a strong security posture at all business units.

Information system-level assessments focus on risks related to specific information systems and their components. Conducting technical assessments, such as penetration testing and vulnerability scanning, as part of the organization's overall security and privacy program give a clear picture of technological risks [98]. Some technical controls include access control, network security, cryptography, application security, and incident management to protect information assets from unauthorized access, modification, or destruction [99]. Although Cameroon's legal framework emphasizes information and network security, it only explicitly mentions penetration and intrusion tests to assess security posture [100]. While these tests are important for identifying vulnerabilities in an organization's information security infrastructure, they represent only an aspect of a comprehensive information security program. Based on these technical risk assessments, organizations develop effective security and privacy controls based on the results of these assessments [101]. Information system-level assessments can also provide detailed information on specific risks, which can be useful for making informed risk management decisions [102]. However, information system-level assessments may not capture the broader risk landscape that affects the organization as a whole, and they may not provide insights into risks that are related to business processes or organizational governance. Overall, each level of risk assessment has its advantages and disadvantages, and organizations should carefully consider their needs and resources when deciding which level or levels of assessment to use [103]. As Cameroonian legislators consider future legal reforms, they should remember that combining cybersecurity risk assessments across multiple organizational levels can provide a more comprehensive view of an organization's risk landscape. This approach will ensure that the information security risk management in Cameroon is aligned with the organization's mission and goals.

B. Critical Considerations for the Auditing Process

Both NIST 800-53 and ISO 19011 describe processes that involve several stages or phases and have the goal of evaluating, documenting and improving information security systems. NIST SP 800-53 and ISO 27001 provide guidance on selecting and implementing appropriate controls to protect information assets from threats and risks [104]. The stages or phases of each process are similar but have different names: initiation, planning, execution, reporting, remediation and verification for the assessment process; and audit program management, audit planning, audit preparation, audit performance, audit reporting and audit follow-up for the audit process [105]. An important lesson Cameroon can learn from NIST and ISO 19011 is the detailed established processes for evaluating and improving cybersecurity and information systems by defining security controls and providing detailed guidance for the systems audits and control implementation.

With the rapidly evolving technological space, cloud computing has become critical for business advancement forcing NIST and ISO to compete with assessment and control frameworks. An in-depth assessment of NIST 800-53 Rev.3 revealed it did not include cloud-specific controls. However, NIST 800-53 rev.5 includes many cloud-relevant controls [106]. ISO/IEC WD 27017 and ISO/IEC 27018 standards apply to information security management, security controls for using cloud computing, and data protection controls for public cloud computing, respectively [107]. NIST 800-53 has over 860 controls and enhancements, with approximately 17% being cyber resiliency oriented, but it can be challenging to identify

which controls support resiliency and in what aspect [108]. As businesses move to cloud computing, Cameroonian businesses and lawmakers must understand that cyber threats will persist and that there's a need to cultivate cyber resilience to protect their businesses, online and in the cloud. It is also relevant that Cameroonian authorities and business understand that in adopting cloud computing, "resiliency is needed to complement these measures, both to make them more effective and so that when the adversary does breach the perimeter, the organization is able to maintain and maximize mission operations while containing and otherwise minimizing the spread and actions of the adversary" [109].

C. Continuous Monitoring and the Life-cycle Approach

Continuous monitoring of information security and cybersecurity practices can be considered a form of cybersecurity risk assessment and auditing since they involve the ongoing review and assessment of an organization's security controls and practices to ensure that they are effective in protecting against threats and vulnerabilities [110]. This can help organizations continuously identify and address potential security issues before they become major problems, and can also provide valuable information for improving their overall security posture. Cameroon's information security framework does require ANTIC to organize audits once per year and does not recommend organizations to continuously monitor their systems for any vulnerabilities or attacks [111]. However, ANTIC can request that the Minister of Telecommunications modifies the audit frequency [112]. This provision does not resolve the question of constant threats and vulnerabilities facing the information and cybersecurity infrastructure. Continuous monitoring of communication traffic is important for taking precautions against possible attacks and preventing harmful packets from entering the system while ensuring that legitimate packets are not delayed or blocked [113]. YImaz *et al.* , also highly emphasize the importance of continuously monitoring employees who work for an organization [114]. It is important to understand that NIST and ISO controls also provide people controls, including employees, because an information systems attacker could be an employee of the organization [115]. This control must be implemented with a view to the privacy concerns of employees. Another paper will review the importance of employing peoples controls and compare that to Cameroon's legal framework.

V. Conclusion

In conclusion, auditing cybersecurity or performing risk assessments of information security systems is a crucial process that organizations must undertake regularly to protect their information systems and mitigate cyber threats to ensure business continuity. Cyber threats are constantly evolving, and organizations must be proactive in identifying vulnerabilities and implementing measures to mitigate risks. Cameroon's cybersecurity legal framework provides a good foundation for organizations in the country to implement effective cybersecurity risk management strategies. The ISO 27001 and NIST frameworks are widely recognized as best practices for cybersecurity auditing and risk assessment. Compliance with these frameworks can help organizations enhance their overall cybersecurity posture, protect their critical assets, and improve their credibility and reputation. While these frameworks are voluntary, organizations in Cameroon can benefit from aligning their cybersecurity audit requirements with these frameworks. Cameroon's cybersecurity legal framework provides a comprehensive approach to cybersecurity risk management. The framework focuses on critical terms such as audit, risk assessment, and information security system but fails to give detailed processes and controls to remediate vulnerabilities in the information security system. Organizations must understand these terms to effectively implement cybersecurity risk management strategies and conduct effective cybersecurity audits.

The cybersecurity risk assessment and auditing process in Cameroon should follow a hierarchical approach to risk assessment and audits. The process should begin with identifying assets and assessing their criticality, followed by identifying threats and vulnerabilities, assessing the likelihood and impact of risks, and finally implementing controls and monitoring their effectiveness. The audit process should be structured and organized, with clear objectives, scope, and criteria. It should involve a comprehensive examination of the organization's security actors, policies, actions, procedures, and resources. Continuous monitoring and a lifecycle approach are critical to effective cybersecurity risk management and auditing. Organizations must regularly review and update their risk assessments and controls to ensure they remain effective in mitigating emerging threats. Regular audits remain a vital instrument to identify shortcomings in an organization's information security posture and lead to the necessity of implementing corrective measures.

Cybersecurity auditing is a vital tool for protecting information systems and mitigating cyber threats in Cameroon. The ISO 27001 and NIST frameworks are widely recognized as best practices for cybersecurity auditing and risk assessment. Compliance with these frameworks can help organizations enhance their overall cybersecurity posture and improve their credibility and reputation. Cameroon's cybersecurity legal framework provides a good foundation for organizations to implement effective cybersecurity risk management strategies. The cybersecurity auditing process should follow a hierarchical approach to risk assessment and audits, involve a structured and organized audit process, and incorporate continuous monitoring and a lifecycle approach. By adopting these best practices, organizations in Cameroon can effectively protect their information systems and mitigate cybersecurity risks. The current cybersecurity regulatory landscape in Africa is haphazard and gives the orientation to adopt a single continental legal framework like the European Union's Directive 2016/1148 that requires member states to adopt "common level of network and information security throughout the European Union" [116]. Consequently, countries like Portugal have transposed European legal regulations like the Budapest Convention into national law. [117]. Although this uniform regulatory framework looks tempting, national circumstances including business

advancement levels, especially, the financial and economic resiliency should be a critical factor in adopting harmonized laws.

REFERENCES

[1] Negin Aminian, Cybersecurity Audit vs. Cybersecurity Assessment: What's the Difference? Available at Cybersecurity Audit vs. Cybersecurity Assessment: What's the Difference (securityscorecard.com) Last accessed on 21 May 2023.

[2] *Ibid.*

[3] *Ibid.*

[4] R. Von Solms, and J. Van Niekerk. "From information security to cybersecurity." computers & security 38 (2013):6 97-102. https://www.profsandhu.com/cs6393_s19/Solms-Niekerk2013.pdf

[5] Okala, Digital 2022: Cameroon, available at Digital 2022: Cameroon — DataReportal – Global Digital Insights. Accessed 20 May 2023.

[6] Lee Raine, Jenna Anderson, Jennifer Connolly, Cyber Attacks Likely to Increase, available at Cyber Attacks Likely to Increase | Pew Research Center. Accessed 15 May, 2023.

[7] Amindeh Blaise Atabong, Cameroon hoping to join Budapest Convention to curb cybercrime, Available at https://itweb.africa/content/dgp45qa6eKmvX9l8. Accessed 30 April, 2023.

[8] *Ibid.*

[9] *Ibid.*

[10] Dhavy Gantsou, Invited Paper: VANET Security: Going Beyond Cryptographic-Centric Solutions, (ed) Advances in Intelligent Systems and Computing, Volume 306. 2014.

[11] Section 1 of the Cybersecurity Law.

[12] NIST Special Publication 800-39 (2011), Managing Information Security Risk. Page 1. (Going forward NIST SP 800-39).

[13] NIST SP 800-39, Page 1.

[14] *Ibid.*

[15] *Ibid.*

[16] Borky JM, Bradley TH. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering. 2018 Sep 9:345–404. doi: 10.1007/978-3-319-95669-5_10. PMCID: PMC7122347.

[17] NIST Special Publication 800-37 (2), (2018) Risk Management Framework for Information Systems and Organizations. Page 3. (Going forward NIST SP 800-37(2).

[18] Borky JM, Bradley TH. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering. 2018 Sep 9:345–404. doi: 10.1007/978-3-319-95669-5_10. PMCID: PMC7122347.

[19] Jadhav, Krishna. (2023). THE ROLE OF CYBERSECURITY AUDITS. Available at https://www.researchgate.net/publication/367559332_THE_ROLE_OF_CYBER_SECURITY_AUDITS#fullTextFileContent . Accessed 30 April 2023.

[20] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano. "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model(CSAM)." In 2017 International Conference on InformationSystems and Computer Science (INCISCOS), pp. 253-259.IEEE, 2017. (PDF) THE ROLE OF CYBERSECURITY AUDITS.

[21] Cueva-Ruiz, Leoncio & Amado, Misael & Carrasco, Jeremy & Andrade-Arenas, Laberiano. (2022). Implementation of Information Security Audit for the Sales System in a Peruvian Company. International Journal on Advanced Science, Engineering and Information Technology. 12. 1189. 10.18517/ijaseit.12.3.13969.

[22] Borky JM, Bradley TH. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering. 2018 Sep 9:345–404. doi: 10.1007/978-3-319-95669-5_10. PMCID: PMC7122347.

[23] Ibid.

[24] Mike Chapple, Certified Information Security Management, Study Guide, Sybex.2022.

[25] Alexander Ayertey Odonkor, Unveiling the cost of cybercrime in Africa, 27-Oct-2020. Available at https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html Accessed 30 April 2023.

[26] International Police, African Cyberthreat Assessment Report 2021. Available at INTERPOL report identifies top cyberthreats in Africa. Accessed 1 May 2023.

[27] *Ibid.*

[28] *Ibid.*

[29] Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527

[30] *Ibid.*

[31] *Ibid.*

[32] ISO 27001 on Information Security, cybersecurity and privacy protection - information security management systems - Requirements. Page v. (Going forward ISO 27001).

[33] Proença, Diogo & Borbinha, José. (2018). Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. 10.1007/978-3-319-93931-5_8.

[34] Jadhav, Krishna. (2023). THE ROLE OF CYBERSECURITY AUDITS. Available at https://www.researchgate.net/publication/367559332_THE_ROLE_OF_CYBER_SECURITY_AUDITS#fullTextFileContent . Accessed 30 April 2023.

[35] Ani Petrosyan, Share of cyber attacks in global industries worldwide 2022, Available at https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/. Accessed 1 May, 2023

[36] Landry Signé and Kevin Signé, Global cybercrimes and weak cybersecurity threaten businesses in Africa. Available at Global cybercrimes and weak cybersecurity threaten businesses in Africa (brookings.edu). Accessed 2 May 2023.

[37] *Ibid.*

[38] *Ibid.*

[39] Makeri Ajiji, Yakubu. (2020). Strategy and Cyber Prevention on Small Business in Africa (COVID-2019). Review of World Economics. Vol.8,. 22-28. 10.17265/2328-7144/2020.01.003.

[40] Nathaniel Allen, Africa's Evolving Cyber Threats. Available at https://africacenter.org/spotlight/africa-evolving-cyber-threats/. Accessed 2 May 2023.

[41] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. *et al*. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak* 20, 146 (2020). https://doi.org/10.1186/s12911-020-01161-7

[42] *Ibid.*

[43] Juliana De Groot, 4 Steps to Prevent Phishing Attacks. Available at https://www.digitalguardian.com/blog/phishing-attack-prevention-how-identify-prevent-phishing-attacks. Last consulted 19 May 2023.

[44] Rowena Rodrigues, Legal and human rights issues of AI: Gaps, challenges and vulnerabilities, Journal of Responsible Technology, Volume 4, 2020, 100005, ISSN 2666-6596.

[45] Duncan Hollis, A Brief Primer on International Law and Cyberspace. Available at https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763. Accessed on 2 May 2023.

[46] *Ibid.*

[47] Cynthia Brumfield & Brian Huaghli, Cybersecurity Risk Management, Mastering the Fundamentals using the NIST Cybersecurity Framework, Wiley 2022. Page XIX.

[48] *Ibid.*

[49] Clause 6.1.3 of ISO 27001: 2022.

[50] Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, Vol. 33 No. 7, pp. 76-105. https://doi.org/10.1108/TQM-09-2020-0202

[51] In Lee, Cybersecurity: Risk management framework and investment cost analysis, Business Horizons, Volume 64, Issue 5, 2021, Pages 659-671, ISSN 0007-6813, https://doi.org/10.1016/j.bushor.2021.02.022. (https://www.sciencedirect.com/science/article/pii/S0007681321000240.)

[52] Section 13 of Law No. 2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality in Cameroon. (Cybersecurity Law going forward).

[53] Section 2 of Decree No 2012/1643/PM of 14 June 2021 laying down the conditions and procedures for the mandatory security audit 14 TUN 2012 electronic communications networks and systems of information (Cybersecurity Auditing Decree going forward).

[54] Section 32 of the Cybersecurity Law.

[55] Section 31 of the Cybersecurity Law.

[56] Section 26 of the Cybersecurity Law.

[57] Section 26 of the Cybersecurity Law.

[58] Sections 3 and 4 of the Cybersecurity Decree.

[59] Clause 3.1 of ISO19011 on Guidelines for auditing management systems and Section 4(9) of the Cybersecurity Law.

[60] Section 9 of the Cybersecurity Law.

[61] *Ibid.*

[62] Clause 9.2 of ISO 97001.

[63] Section 3.3 of NIST SP 800-53.

[64] Chapter 2.3 of NIST Special Publication 800 30 Revision 1, Guide for Conducting Risk Assessments. (Going forward NIST 800 30 Rev. 1).

[65] NIST 800-30 Rev. 1.

[66] Section 30 of the Cybersecurity Law.

[67] Clause 6.1.2 ISO 27001: 2022.

[68] *Ibid.* and Risk Assessment Control 3 of NIST 800-53 Rev. 5.

[69] Risk Assessment Control 3 of NIST 800-53 Rev. 5.

[70] *Ibid.*

[71] *Ibid.*

[72] Clause 8.2 of ISO 27001: 2022.

[73] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a13 0revised.pdf. Adopted by NIST Special Publication 800-37 Revision 2.

[74] 44 USC. § 3542.

[75] 44 USC § 3552 (b)(3).

[76] Section 1 of the Cybersecurity Law.

[77] Clause 4.20 of ISO/IEC 27032:2012

[78] Hamed Taherdoost, Cybersecurity vs. Information Security, Procedia Computer Science, Volume 215, 2022, Pages 483-487, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.050.

[79] Section 1 of the Cybersecurity Law.

[80] Clause 3.1 of ISO19011 on Guidelines for auditing management systems.

[81] *Ibid.*

[82] *Ibid.*

[83] Article 4 of the Cybersecurity Law.

[84] Appendix K of NIST SP 800-30 Rev. 1.

[85] *Ibid.*

[86] *Ibid.*

[87] *Ibid.*

[88] RA Control 3 and AU Control 1 of NIST 800 53 Rev. 5, (2020).

[89] Edward B. McCabe and Greg Witte, Certified Information Security Manager, Review Manual, 16th edition, 2021.

[90] *Ibid.*

[91] Latinovic, Tihomir & Sikman, Ljilja. (2020). ISO 27001 – INFORMATION SYSTEMS SECURITY, DEVELOPMENT, TRENDS, TECHNICAL AND ECONOMIC CHALLENGES, Journal Annals of Hunedoara.

[92] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

[93] Section 9 Cybersecurity Auditing Decree.

[94] ISO 27001:2022 standard for information security management systems and NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

[95] NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

[96] Section 9 Cybersecurity Auditing Decree.

[97] NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

[98] NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

[99] ISO 27001:2022 standard for information security management systems and NIST Special Publication.

[100] Section 9 Cybersecurity Auditing Decree.

[101] For Security Controls see ISO 27001 Annex A and Chapter 3 of the NIST 800 53 Rev. 5.

[102] Palaniappan Shamala, Rabiah Ahmad, Mariana Yusoff, A conceptual framework of info structure for information security risk assessment (ISRA), Journal of Information Security and Applications, Volume 18, Issue 1, 2013, Pages 45-52, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2013.07.002. (https://www.sciencedirect.com/science/article/pii/S221421261300029X)

[103] Clause 9.1 of ISO 27001: 2022.

[104] Chapter 3 of NIST SP 800-53 Rev 5 and Annex A of ISO 27001.

[105] See generally NIST SP 800-30 Rev. 1 and ISO 19011.

[106] Tariq, Muhammad Imran, et al. "Analysis of NIST SP 800-53 rev. 3 controls effectiveness for cloud computing." *computing* 3.4 (2016).

[107] Ibid.

[108] Deb Bodeau Richard Graubart, Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls, MITRE Technical Report, 2013. Available at Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls (dtic.mil).

[109] Deb Bodeau Richard Graubart, Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls, MITRE Technical Report, 2013. Available at Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls (dtic.mil).

[110] NIST 800-137 on Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations. See Also, RA 5 on Vulnerability Monitoring and Scanning.

[111] Section 5 of the Cybersecurity Auditing Decree.

[112] *Ibid.*

[113] E. N. Ylmaz, B. Ciylan, S. Gönen, E. Sindiren and G. Karacayılmaz, "Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect," 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2018, pp. 81-85, doi: 10.1109/SGCF.2018.8408947.

[114] Ibid.

[115] Table A.1 Point 6 f ISO 27001:2022. See also Controls 3.14 of NIST 800-53 Rev 5.

[116] Carvalho, J.V., Carvalho, S. & Rocha, Á. European strategy and legislation for cybersecurity: implications for Portugal. Cluster Comput 23, 1845–1854 (2020).

[117] *Ibid.*