Management of enterprise cyber security: A review of ISO/IEC 27001:2022

Masike Malatji
Digital Transformation and Innovation
Graduate School of Business Leadership (SBL), University of South Africa (UNISA)
Midrand, Johannesburg, South Africa
malatm1@unisa.ac.za

2023 International Conference On Cyber Management And Engineering (CyMaEn) | 978-1-6654-9329-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/CyMaEn57228.2023.10051114

Abstract— **The ISO/IEC 27001 standard is one of the most widely used and accepted standards for information security worldwide. On 25 October 2022, the third edition of the standard was published as ISO/IEC 27001:2022 to address global cybersecurity challenges and improve digital trust. This paper sought to compare and contrast the ISO/IEC 27001:2022 and ISO/IEC 27001:2013 through the lens of the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework (CF) for critical infrastructure protection, version 1.1. This is because the security controls referenced in Annex A of the ISO/IEC 27001 standard are prominently referenced in each of NIST CF's five Functions – Identify; Protect; Detect; Respond; Recover – for its implementation. The author sought to establish whether and how the ISO/IEC 27001:2022 has been improved for enterprise systems security. Descriptive statistics were utilised to determine the frequency distribution of each ISO/IEC 27001:2022 security control for each NIST CF Function. It was found that the NIST CF's Protect Function has a higher frequency distribution of security controls than the other four Functions. Interestingly, the distribution was at 52% for both the ISO/IEC 27001:2022 and ISO/IEC 27001:2013. It was concluded that the ISO/IEC 27001:2022 is a slight improvement to the ISO/IEC 27001:2013 as it also introduced eleven new security controls one of which addresses the protection of cloud computing services, which have increasingly been adopted by many businesses.**

Keywords— cyber security, ISO/IEC 27001, information security, information systems, ISMS, NIST

I. Introduction

Cyberattacks are disruptive, costly, and increasing concern to businesses, governments, and nation-states alike [1]–[3]. To quantify some of the cybersecurity concerns, the World Economic Forum (WEF) [4] released its first global cybersecurity outlook flagship report which identifies current and future cybercrime trends and challenges. The report highlights that there was a global increase of 125% in cyberattacks with evidence indicating a continued uptick in 2022 and subsequent years [4]. Coupled with recent high-profile cyberattacks globally, the WEF report is a reminder that existing information and cybersecurity frameworks and standards must adapt to ensure continued data and infrastructure protection [5]. However, cybersecurity frameworks and cybersecurity standards are different and serve different purposes in an enterprise [6]

According to the National Institute of Standards and Technology (NIST) [7], the word 'framework' refers *to "a layered structure indicating what kind of programs can or should be built and how they would interrelate and is generally more comprehensive than a protocol and more prescriptive than a structure."* Cybersecurity frameworks thus provide comprehensive guidelines that span several security domains and generally do not outline detailed steps required to be carried out for the implementation of security controls [8]. These provide users with some degree of freedom to customise their security arrangements to meet the organisation's cybersecurity needs [9]. In other words, users describe the security scope, risk evaluation, and implementation processes through a cybersecurity framework's defined general structure [10]. This kind of flexibility can also help reduce the implementation costs associated with security programs [8].

There are three types of cybersecurity frameworks in general [11]. According to Dedeke and Masterson [11], these are frameworks developed by international standards organisations, those initiated by the private sector including professional bodies, and lastly governments-led public-private partnerships cybersecurity framework initiatives [11]. Examples of these include the United States of America's NIST Special Publication (SP) 800 series (e.g., NIST SP 800-53 for security and privacy controls, NIST SP 800-82 for industrial control systems, and NIST Cybersecurity Framework for critical infrastructure protection, version 1.1), COBIT and the United Kingdom's Cyber Assessment Framework [5], [11]–[13]. To ensure cyber resilience [14], organisations should therefore adopt appropriate cybersecurity frameworks for the implementation of information and cybersecurity standards [2].

When it comes to cybersecurity standards, NIST [7] defines the word 'standard' as *"a document, established by consensus and approved by a recognised body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context."* Information and cybersecurity standards, therefore, recommend a set of common and specific security practices, methods, and processes aimed at safeguarding an organisation's information systems and critical infrastructure. Unlike cybersecurity frameworks, information and cybersecurity standards outline step-by-step procedures on how specific security practices, methods, and processes should be implemented. There are various information and cybersecurity standards such as the International Standardisation Organisation (ISO)/ International Electrotechnical Commission (IEC) 27000 family of standards for managing information security of enterprise systems including the ISO/IEC 27001 (information security), ISO/IEC 27400 (Internet of Things (IoT) security) and ISO/IEC 27005 (security risk management), the International Society of Automation (ISA)/IEC 62443 standard for addressing security vulnerabilities in industrial automation and control systems, and the Institute of Electrical and Electronics Engineers (IEEE) 2144.1 standard for addressing blockchain-based IoT data management [2], [5], [15]. Therefore, the effective implementation of information and cybersecurity standards is unlikely to be optimal nor is it advisable without the appropriate cybersecurity framework [11], [16]. The difference between a cybersecurity framework and a cybersecurity standard, therefore, is that a framework provides an overarching systematic approach to security [11], whereas a standard provides a step-by-step procedure on how to secure and manage specific aspects of an organisation's information assets [8]. As standards usually only manage specific security aspects of an organisation's information systems, a combination of various but appropriate standards may be required [17], [18].

Although it is not the only available information and cybersecurity standard, the ISO/IEC 27001 standard is one of the most widely used worldwide and it is the core standard in the ISO/IEC 27000 family of standards [8], [19]. On 25 October 2022, the ISO/IEC (2022) standardisation body published the third edition of the ISO/IEC 27001 standard, and by implication the ISO/IEC 27002:2022, *"to address global cybersecurity challenges and improve digital trust."* The ISO/IEC 27001:2022 (Information security, cybersecurity and privacy protection — Information security management systems — Requirements) standard serves as a guideline that specifies what organisations should do for implementing an information security management system (ISMS) within contexts [20]. This paper aimed to compare and contrast the ISO/IEC 27001:2022 and ISO/IEC 27001:2013 through the NIST CF, version 1.1, lens, to establish whether and how the ISO/IEC 27001:2022 has been updated to improve enterprise security. It should be noted that how the ISO/IEC 27001:2022 has been improved in comparison to the ISO/IEC 27001:2013 is already documented by the responsible Technical Committee of the ISO/IEC bodies [20]. The changes are documented in the ISO/IEC 27001:2022-TC where 'TC' stands for tracked changes (also known as the ISO/IEC 27001:redline:2022(E)). Corresponding mapping of security controls in the ISO/IEC 27002:2022 and ISO/IEC 27002:2013 standards has also been carried out in the ISO/IEC 27002:2022 document [21]. Therefore, the author merely sought to determine whether and how the new and merged security controls referenced in Annex A of the ISO/IEC 27001:2022 standard impact the NIST CF, version 1.1, Functions. It should be noted that at the time of writing this paper discussions were already underway to update the NIST CF to version 2.0 to keep pace with threat and technology trends and integrate lessons learned over the past five years [22].

The rest of this paper is structured as follows. In the first section, the background and context, including the study frame of reference, grounds for comparison (ISO/IEC 27001:2013 to ISO/IEC 27001:2022 improvements, if any), and study aim are provided. Section II provides an overview of the structural elements of the ISO/IEC 27001 standard. The study frame of reference for comparative analysis is elaborated upon in Section III with the methods of analysis described in Section IV. The results are presented, and findings discussed in Section V. The paper concludes with recommendations in Section VI.

II. ISO/IEC 27001 Standard Overview

The ISO/IEC 27001 standard specifies the requirements for establishing, implementing, maintaining, monitoring, reviewing, and continually improving ISMSs [19], [20]. An ISMS is essentially a governance structure that is comprised of a set of practices, methods, and processes with which to manage information security risks [23]. The standard is anchored on seven mandatory ISMS requirements for ISO certification, also known as clauses, which concern more the management system rather than security controls, and these are [24]:

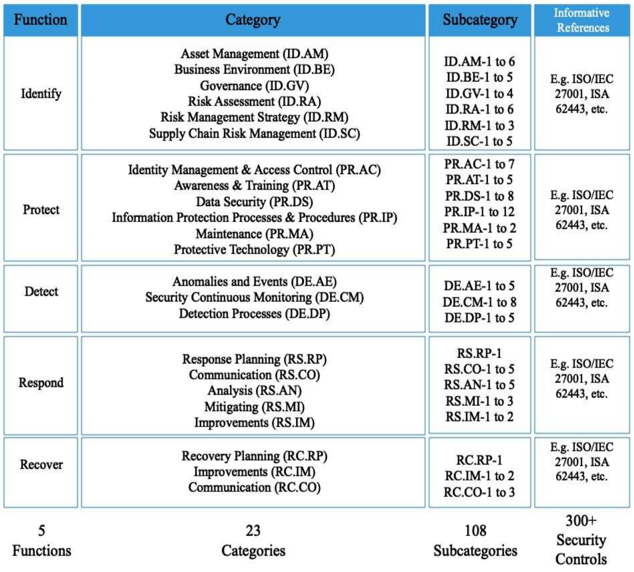
- Context of the organisation (Clause 4)
- Leadership (Clause 5)
- Planning (Clause 6)
- Support (Clause 7)
- Operation (Clause 8)
- Performance evaluation (Clause 9)
- Improvement (Clause 10)

The ISO/IEC 27001 standard does not formally prescribe specific security controls as these are set out in more detail in the ISO/IEC 27002 [25]. The ISO/IEC 27001 standard merely references security controls in its Annex A [26]. That is, where an organisation chose to deploy information security controls from Annex A of the ISO/IEC 27001 standard for compliance, the ISO/IEC 27002 is more appropriate to provide guidelines on how to implement those controls [27]. The ISO/IEC 27002 is therefore primarily a catalogue of best practice information security controls but only as guidelines and recommendations than prescriptions [19]. Information and communication technology (ICT) practitioners can then select these as appropriate for their business environments to achieve a baseline best practice protection. Specifically, the ISO/IEC 27001:2013 had 114 controls and seven clauses (clauses 4 to 10 as bulleted above). Moreover, the publication title of the ISO/IEC 27001:2013 standard was *"Information technology — Security techniques — Information security management systems — Requirements"* [28] before its withdrawal on 25 October 2022. The next section describes the NIST CF frame of reference within which the ISO/IEC 27001:2022 and ISO/IEC 27001:2013 have been compared and contrasted.

III. Study Frame of Reference

Because the NIST CF provides an overarching systematic approach to managing the cybersecurity risk of critical infrastructure and enterprises in any industry sector, it is the lens through which the author conducted a comparative analysis of the ISO/IEC 27001:2022 and ISO/IEC 27001:2013. The NIST CF advocates for a risk-based approach to managing cybersecurity challenges and is comprised of the Framework Core, Framework Implementation Tiers, and Framework

Profiles [29]. The Framework Core comprises the organisation's cybersecurity activities and controls to achieve specific cybersecurity outcomes and it is arranged into Functions, Categories, Subcategories, and Informative References [16], [29]. Fig. 1 shows the four components of the NIST CF's Framework Core [29], [30].



Function	Category	Subcategory	Informative References
Identify	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Supply Chain Risk Management (ID.SC)	ID.AM-1 to 6 ID.BE-1 to 5 ID.GV-1 to 4 ID.RA-1 to 6 ID.RM-1 to 3 ID.SC-1 to 5	E.g. ISO/IEC 27001, ISA 62443, etc.
Protect	Identity Management & Access Control (PR.AC) Awareness & Training (PR.AT) Data Security (PR.DS) Information Protection Processes & Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)	PR.AC-1 to 7 PR.AT-1 to 5 PR.DS-1 to 8 PR.IP-1 to 12 PR.MA-1 to 2 PR.PT-1 to 5	E.g. ISO/IEC 27001, ISA 62443, etc.
Detect	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)	DE.AE-1 to 5 DE.CM-1 to 8 DE.DP-1 to 5	E.g. ISO/IEC 27001, ISA 62443, etc.
Respond	Response Planning (RS.RP) Communication (RS.CO) Analysis (RS.AN) Mitigating (RS.MI) Improvements (RS.IM)	RS.RP-1 RS.CO-1 to 5 RS.AN-1 to 5 RS.MI-1 to 3 RS.IM-1 to 2	E.g. ISO/IEC 27001, ISA 62443, etc.
Recover	Recovery Planning (RC.RP) Improvements (RC.IM) Communication (RC.CO)	RC.RP-1 RC.IM-1 to 2 RC.CO-1 to 3	E.g. ISO/IEC 27001, ISA 62443, etc.
5 Functions	23 Categories	108 Subcategories	300+ Security Controls

Fig. 1. NIST CF Framework Core.

Firstly, the Framework Core's cybersecurity activities and controls are executed through five concurrent and continuous Functions—Identify, Protect, Detect, Respond, and Recover [29]. Secondly, the 23 Categories are the required cybersecurity outcomes for each Function while, thirdly, the 108 Subcategories represent security controls to address each Category adequately [27], [29]. Lastly, the example Informative References are the existing information and cybersecurity standards, guidelines, and practices on how each Subcategory may be operationally implemented [29]. That is, it is possible to assign security controls from the ISO/IEC 27001 to each Function of the Framework Core, via the Subcategories, based on the Informative References component of the Framework Core [30]. It can also be seen in the Informative References component that, as asserted by [17] and [18], various security control standards may be required as appropriate. This may include the ISO/IEC 27001 standard under review in this paper, ISA 62443, and the Centre for Internet Security [29]. The four-character codes in Fig.1 are abbreviations for the NIST CF Function-Category combination. For example, AM.ID in Fig. 1 represents the Identify (ID) Function and Asset Management (AM) Category. The rest of the codes in Fig. 1 can be viewed in the NIST [29] framework for critical infrastructure protection by clicking here. The methods utilised in the study are summarised next.

IV. Methods

Data collection procedure. All security controls of both the ISO/IEC 27001:2013 and ISO/IEC 27001:2022 standards as referenced in Annex A were thematically reviewed through the five NIST CF Functions as the main data sources. Because the ISO/IEC 27002:2022 complements Annex A of the ISO/IEC 27001:2022 standard [19], it was also reviewed in conjunction with the ISO/IEC 27001:2022.

Data analysis technique. Descriptive statistics were utilised to analyse and visualise the overall frequency distribution of each ISO/IEC 27001 security control within the NIST CF Functions. The findings are discussed in the next section.

V. Analysis and Discussions

A. *ISO/IEC 27001:2013 results and findings*

Thematic analysis of the ISO/IEC 27001:2013 security controls is summarised in Fig. 2.

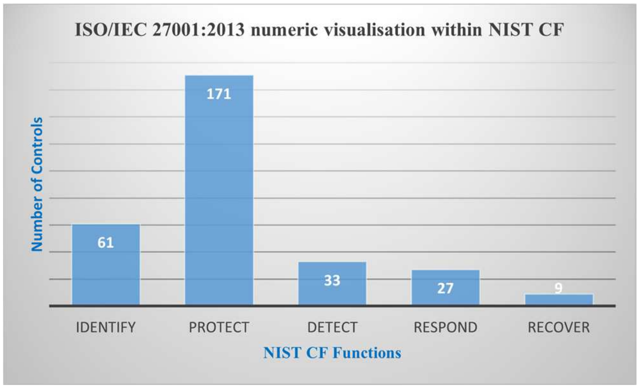


Fig. 2. Numeric visualisation of ISO/IEC 27001:2013 security controls within NIST

Thematic analysis of Annex A of the ISO/IEC 27001:2013 standard indicate that there are 114 security controls. Fig. 2 shows that of the 114 security controls, 61 have thematically been mapped to the NIST CF Identify, 171 to the Protect, 33 to the Detect, 27 to the Respond, and 9 to the Recover Functions. The grand total of the security controls in Fig. 2 is 301 instead of 114 because some of the controls could be mapped to more than one NIST CF Function. In other words, there are repetitive controls distributed to different NIST CF Functions. The same results in Fig. 2 can be visualised differently through frequency distribution as shown in Fig. 3.

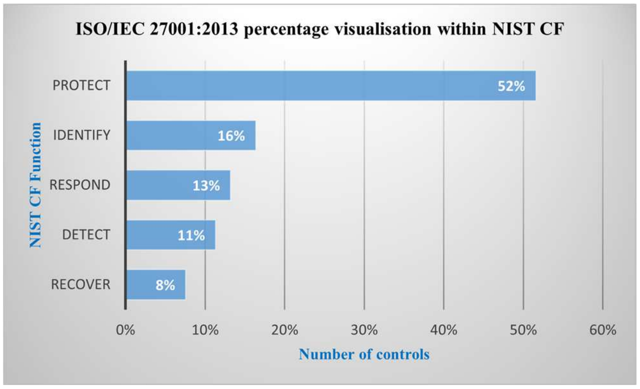


Fig. 3. Percentage visualisation of ISO/IEC 27001:2013 security controls within NIST

It is clear from Fig. 3 that the Protect Function has a higher percentage of the ISO/IEC 27001:2013 security controls distribution than the other NIST CF Functions. One can conclude therefore that the ISO/IEC 27001:2013 is more offensive than defensive in nature as the Protect Function is basically about the type and quantity of security measures put in place to prevent potential cyberattacks. Next, the ISO/IEC 27001:2022 results are compared to the ISO/IEC 27001:2013 findings.

B. *ISO/IEC 27001:2022 results and findings*

Thematic analysis of the ISO/IEC 27001:2022 security controls is summarised in Fig. 4.

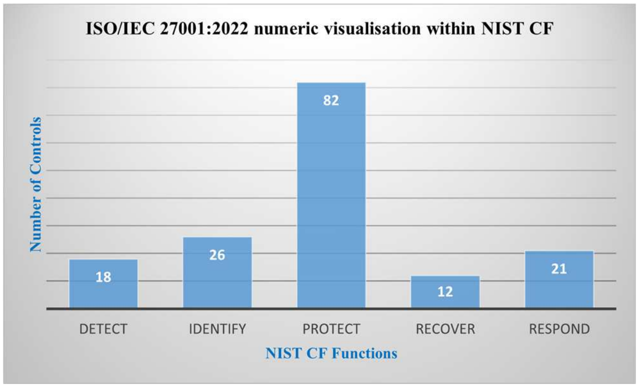


Fig. 4. Numeric visualisation of ISO/IEC 27001:2022 security controls within NIST

Thematic analysis of Annex A of the ISO/IEC 27001:2022 standard indicate that there are 93 security controls. Fig. 4 shows that of the 93 security controls, 18 have thematically been mapped to the NIST CF Detect, 26 to the Identify, 82 to the Protect, 12 to the Recover, and 21 to the Respond Function. Similarly, the grand total of the security controls in Fig. 4 is 159 instead of 93 because some of the controls could be mapped to more than one NIST CF Function. The same results in Fig. 4 were visualised through descriptive statistics as shown in Fig. 5.

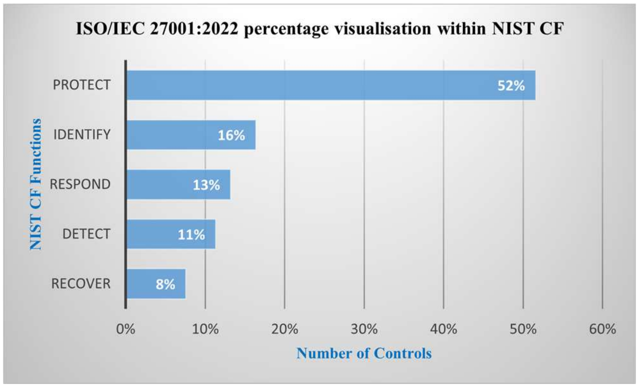


Fig. 5. Percentage visualisation of ISO/IEC 27001:2022 security controls within NIST

Like the ISO/IEC 27001:2013 results, Fig. 5 shows that the ISO/IEC 27001:2022 security controls are more distributed towards the Protect than the other NIST CF Functions. Similarly, the ISO/IEC 27001:2022 is also more offensive than defensive. Furthermore, a comparison of clauses 4 to 10 mentioned previously in Section II reveals that there are several but minor changes in ISO/IEC 27001:2022. Additional new content has been added especially in subclauses 4.2, 6.2, 6.3, and 8.1. In addition, terminology and rephrasing of some sentences and clauses have been included in ISO/IEC 27001:2022. However, the titles and order of clauses 4 to 10 remain the same as listed in Section II. In terms of the control changes, firstly, 35 controls have remained the same. Secondly, 57 controls were merged into 24 controls. Thirdly, 23 controls were renamed while, fourthly, one security control has been split into two controls. Lastly, 11 new security controls were added to the ISO/IEC 27001:2022 standard. These are (i) Threat intelligence; (ii) Information security for the use of cloud services; (iii) ICT readiness for business continuity; (iv) Physical security monitoring; (v) Configuration management; (vi) Information deletion; (vii) Data masking; (viii) Data leakage prevention; (ix) Monitoring activities; (x) Web filtering; (xi) Secure coding.

Although, for example, the ‘information security for the use of cloud services’ has been mapped to the Identify Function of the NIST CF, the current NIST CF version 1.1 does not explicitly emphasise cloud computing cybersecurity [31]. Perhaps this is something the future NIST CF version 2.0 could reconcile. Given the controls changes outlined above, the total number of security controls has decreased from 114 to 93 in ISO/IEC 27001:2022 and these are grouped into four dimensions, namely, organisational, people, physical and technological.

VI. Conclusion

This paper aimed to compare and contrast the ISO/IEC 27001:2022 and ISO/IEC 27001:2013 through the NIST CF, version 1.1, lens, to establish whether and how the ISO/IEC 27001:2022 has been updated to improve enterprise systems security. Figures 3 and 5 showed that the frequency distribution of security controls within the NIST CF as referenced in Annex A of both the current (ISO/IEC 27001:2022) and withdrawn (ISO/IEC 27001:2013) standards is the same. Moreover, the security controls distribution showed in both these figures that the Protect Function is more emphasised by both standards than the other NIST CF Functions. The findings also revealed new security controls in the ISO/IEC 27001:2022 not currently recommended in the NIST CF, version 1.1. Notably, the NIST CF, version 1.1, does not explicitly emphasise cloud computing cybersecurity and this is one of the new security controls added to the ISO/IEC 27001:2022.

With remote workers, digital nomads and the ubiquitous nature of IoT devices connecting to enterprise networks, perhaps the next amendment or edition of the ISO/IEC 27001:2022 could refer to *“information security for use of IoT devices”* and leave the details as currently provided in the ISO/IEC 27400:2022 (Cybersecurity — IoT security and privacy — Guidelines). This would serve to acknowledge that IoT security and privacy have gradually become intertwined with enterprise systems security, the same way that cloud security has. In summary, there are five improved changes to the ISO/IEC 27001:2022 standard: (i) Clauses 4 to 10 have undergone several but minor changes; (ii) Eleven new security controls have been added to Annex A; (iii) The number of security controls in

Annex A has decreased from 114 to 93; (iv) Security controls in Annex A have been grouped into four dimensions; and (v) the title of the standard has also changed to reflect a focus on global cybersecurity challenges and digital trust.

References

[1] A. Basuchoudhary and N. Searle, ‘Snatched secrets: Cybercrime and trade secrets modelling a firm’s decision to report a theft of trade secrets’, *Comput. Secur.*, vol. 87, p. 101591, Nov. 2019, DOI: 10.1016/j.cose.2019.101591.

[2] B. Y. Ozkan and M. Spruit, ‘Cybersecurity Standardisation for SMEs: The Stakeholders’ Perspectives and a Research Agenda’, *Int. J. Stand. Res. IJSR*, vol. 17, no. 2, pp. 41–72, 2019, doi: 10.4018/IJSR.20190701.oa1.

[3] H. Younies and T. N. Al-Tawil, ‘Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)’, *J. Financ. Crime*, vol. 27, no. 4, pp. 1089–1105, Jun. 2020, doi: 10.1108/JFC-04-2020-0055.

[4] WEF, ‘Global Cybersecurity Outlook 2022’, *World Economic Forum*, 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/ (accessed Oct. 31, 2022).

[5] J. Srinivas, A. K. Das, and N. Kumar, ‘Government regulations in cyber security: Framework, standards and recommendations’, *Future Gener. Comput. Syst.*, vol. 92, pp. 178–188, Mar. 2019, DOI: 10.1016/j.future.2018.09.063.

[6] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, ‘Analysis of Cybersecurity Standard and Framework Components’, *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 3, pp. 417–432, Dec. 2020.

[7] NIST, ‘Framework - Glossary | CSRC’, 2022a. https://csrc.nist.gov/glossary/term/framework (accessed Nov. 01, 2022).

[8] H. Taherdoost, ‘Understanding Cybersecurity Frameworks and Information Security Standards&mdash;A Review and Comprehensive Overview’, *Electronics*, vol. 11, no. 14, Art. no. 14, Jan. 2022, DOI: 10.3390/electronics11142181.

[9] D. Bilusich, L. Chim, R. A. Nunes-Vaz, and S. Lord, ‘THERE IS NO SINGLE SOLUTION TO THE “INSIDER” PROBLEM BUT THERE IS A VALUABLE WAY FORWARD’, presented at the RISK ANALYSIS 2018, Seville, Spain, 2018, vol. 121, pp. 135–146. DOI: 10.2495/RISK180121.

[10] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, ‘Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal’, *J. Cybersecurity Priv.*, vol. 1, no. 2, Art. no. 2, Jun. 2021, DOI: 10.3390/jcp1020012.

[11] A. Dedeke and K. Masterson, ‘Contrasting cybersecurity implementation frameworks (CIF) from three countries’, *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 373–392, Jan. 2019, DOI: 10.1108/ICS-10-2018-0122.

[12] H. Shoaee, J. Bagherinejad, and J. Rezaee Nour, ‘Towards the Analysis of Information Technology Governance and Productivity Based on COBIT Framework: An Empirical Study in E-Banking’, *Teh. Vjesn. - Tech. Gaz.*, vol. 29, no. 6, Dec. 2022, doi: 10.17559/TV-20220115074214.

[13] T. Wallis, C. Johnson, and M. Khamis, ‘Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive’, *Inf. Secur. Int. J.*, vol. 48, pp. 36–68, 2021, doi: 10.11610/isij.4812.

[14] R. Azmi, W. Tibben, and K. T. Win, ‘Review of cybersecurity frameworks: context and shared concepts’, *J. Cyber Policy*, vol. 3, no. 2, pp. 258–283, May 2018, DOI: 10.1080/23738871.2018.1520271.

[15] S. Dong, J. Cao, D. Flynn, and Z. Fan, 'Cybersecurity in smart local energy systems: requirements, challenges, and standards, *Energy Inform.*, vol. 5, no. 1, p. 9, Jun. 2022, DOI: 10.1186/s42162-022-00195-7.

[16] S. J. Shackelford, S. Russell, and J. Haut, ‘Bottoms up: A Comparison of Voluntary Cybersecurity Frameworks’, *UC Davis Bus. Law J.*, vol. 16, no. 2, pp. 217–260, 2016 2015.

[17] R. Leszczyna, 'Standards with cybersecurity controls for smart grid—A systematic analysis, *Int. J. Commun. Syst.*, vol. 32, no. 6, p. e3910, 2019, DOI: 10.1002/dac.3910.

[18] S. Park and K. Lee, ‘Advanced Approach to Information Security Management System Model for Industrial Control System’, *Sci. World J.*, vol. 2014, p. e348305, Jul. 2014, DOI: 10.1155/2014/348305.

[19] E. Humphreys, *Implementing the ISO/IEC 27001 ISMS Standard, Second Edition*. Boston, MA: United States of America: Artech House, 2016.

[20] ISO/IEC, ‘ISO - ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements’, 2022. https://www.iso.org/standard/82875.html (accessed Oct. 31, 2022).

[21] ISO, ‘ISO/IEC 27002:2022’, *ISO*, 2022b. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/56/75652.html (accessed Nov. 04, 2022).

[22] NIST, ‘Updating the NIST Cybersecurity Framework – Journey To CSF 2.0’, *NIST*, 2022b, Accessed: Nov. 03, 2022. [Online]. Available: https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

[23] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, ‘The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda’, *TQM J.*, vol. 33, no. 7, pp. 76–105, Jan. 2021, DOI: 10.1108/TQM-09-2020-0202.

[24] A. Alexei, ‘ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF MOLDOVA THROUGH THE ISO 27001 STANDARD’, *J. Soc. Sci.*, vol. IV(1), Mar. 2021, doi: 10.52326/jss.utm.2021.4(1).11.

[25] A. N. Fajar, H. Christian, and A. S. Girsang, ‘Evaluation of ISO 27001 implementation towards information

security of cloud service customer in PT. IndoDev Niaga Internet', *J. Phys. Conf. Ser.*, vol. 1090, p. 012060, Sep. 2018, doi: 10.1088/1742-6596/1090/1/012060.

[26] B. Shojaie, H. Federrath, and I. Saberi, 'Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A', in *2014 Ninth International Conference on Availability, Reliability and Security*, Fribourg, Switzerland, Sep. 2014, pp. 259–264. doi: 10.1109/ARES.2014.41.

[27] A. Calder, *Nine Steps to Success: An ISO 27001 Implementation Overview, North American edition*. IT Governance Ltd, 2017.

[28] ISO, 'ISO/IEC 27001:2013', *ISO*, 2022a. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html (accessed Nov. 04, 2022).

[29] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1', National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, 2018. DOI: 10.6028/NIST.CSWP.04162018.

[30] E. Koza, 'Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security', p. 14, 2022.

[31] M. Malatji, A. L. Marnewick, and S. Von Solms, 'Cybersecurity capabilities for critical infrastructure resilience', *Inf. Comput. Secur.*, vol. 30, no. 2, pp. 255–279, 2021, DOI: 10.1108/ICS-06-2021-0091.