Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government

2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) | 979-8-3503-3943-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICoCICs58778.2023.10277024

1st Eko Yon Handri
Faculty of Computer Science
University of Indonesia
Depok, Indonesia
eko.yon@ui.ac.id

2nd Prasetyo Adi Wibowo Putro
Faculty of Computer Science
University of Indonesia
Depok, Indonesia
prasetyo.adi01@ui.ac.id

3rd Dana Indra Sensuse
Faculty of Computer Science
University of Indonesia
Depok, Indonesia
dana@cs.ui.ac.id

***Abstract*—Implementing a cybersecurity framework plays a critical role in protecting e-government systems and infrastructure from cyber threats and attacks. However, there is no consensus on prioritizing the five core components: identify, protect, detect, respond, and recover. It is also unclear whether these components should be implemented equally or customized. Similarly, no agreement exists on the importance of people, processes, and technology in implementing a cybersecurity framework. This paper aims to address this gap by evaluating and comparing the priorities of the five core components and three aspects using the Analytic Hierarchy Process (AHP). The evaluation outcomes emphasize that the identify component takes precedence over the other core components, underscoring the significance of preventive measures against cyberattacks. In addition, the people aspect received the highest priority among the three implementation aspects, which highlighted the critical role of individuals in successfully implementing process-related measures and leveraging technological advancements. This research provides valuable insights for designing strategies and implementing effective and sustainable cybersecurity measures in e-government. By prioritizing the identify component and recognizing the importance of people, organizations can improve their ability to protect against threats and ensure the resilience of e-government systems.**

Keywords — cybersecurity, e-government, cybersecurity framework, people process technology, analytic hierarchy process

I. Introduction

In the rapidly evolving e-government landscape, protecting data and information has become mandatory. E-government has become vulnerable to cyberattacks, data breaches, and other threats. Therefore, implementing an effective and appropriate cybersecurity framework is essential to protect organizational data and information technology (IT) assets from security threats and vulnerabilities in e-government systems [1]. For this reason, implementing cybersecurity frameworks has become a commonly used approach in protecting e-government systems. A cybersecurity framework is a systematic approach that provides guidance and steps to identify, protect, detect, respond, and recover systems affected by security threats. However, there is no consensus on prioritizing the five core components: identify, protect, detect, respond, and recover. It is also unclear whether these components should be implemented equally or customized to implement cybersecurity effectively and sustainably.

The prioritization of cybersecurity implementation in e-government has considerable implications for the success of data and information protection, which includes aspects such as people, processes, and technology. In many conditions, the technological aspects are always used as the primary solution in mitigating cyber-attacks [2]. But in fact, human factors are also the leading cause of 85% of data breaches, either through credential theft, phishing, misuse, or other simple mistakes [3]. At the same time, the process aspect relates to policies, procedures, and operational practices also ensure system security. In all aspects, there is no clear agreement on the priority of which aspects should get the primary attention in implementing the cybersecurity framework.

The objective of this research is to obtain comprehensive understanding of the prioritization of all these aspects. Therefore, this research will use the Analytical Hierarchy Process (AHP) method to evaluate and compare priorities for the five core components and the three aspects in the context of the cybersecurity framework in e-government. The AHP method developed by Saaty has proven to be highly effective in handling complex multicriteria problems, and it is widely applicable across different domains and sectors [4][5], including e-government. The results are expected to provide valuable insights and recommendations for designing effective and sustainable cybersecurity strategies for e-government in the future.

II. Literature Review

A. Cybersecurity Framework

When a cyberattack occurs, an organization must understand its business processes in order to properly manage cybersecurity risks. Because each organization has a different level of risk, it needs a method to protect the organization from various threats in the form of a cybersecurity framework [6]. A cybersecurity framework is a structure required by organizations to be protected from cyberattacks by providing guidelines in the implementation process so that it meets the requirements of security standards [7]. The most well-known cybersecurity framework is the Cybersecurity Framework published by the National Institute of Standards and Technology (NIST) in the United States. The framework comprises five cores of interacting components: Identify, Protect, Detect, Respond, and Recover [6]. This component forms a comprehensive guide to building and strengthening cybersecurity within organizations. However, these five core components are commonly used in various cybersecurity

frameworks with different approaches and not exclusive to the NIST cybersecurity framework as many understand it.

According to the NIST Cyber Security Framework[6], the five-core framework is defined below:

- Identify - Establish a comprehensive organizational understanding to manage cybersecurity risk across systems, personnel, assets, data, and capabilities.
- Protect - Develop and execute suitable safeguards to ensure the uninterrupted delivery of critical services.
- Detect – Develop and implement appropriate measures to promptly identify any cybersecurity events that may occur.
- Respond - Implement and execute suitable measures to respond promptly and effectively to any detected cybersecurity incidents.
- Recover - Develop and execute plans to ensure resilience and restore impaired capabilities or services following a cybersecurity incident.

Several frameworks also use the five core components, such as ISO/IEC 27001:2022, CIS Controls, and COBIT. All three frameworks also use similar core components both explicitly and implicitly. ISO/IEC 27001:2022 uses the five core components described expressly in the security controls in ISO 27002:2022 [8]. While CIS Controls does not directly identify the five core components, it provides security controls that cover them to protect the organization from threats: Control 1 is concerned with identification, Control 3 and Control 13 involve measures to preserve the system, Control 6 is concerned with detection, and Control 19 involves steps to response and recover security incident [9]. Like CIS Controls, COBIT does not explicitly mention these five core components, but provides principles and guidance relevant to identifying, protecting, detecting, responding, and recovering in the context of IT governance and cybersecurity: the APO (Align, Plan, and Organize) domain relates to strategy and planning that involves identify security risk, the BAI (Build, Acquire, and Implement) field refers to aspects of protection and detection, the DSS (Deliver, Service and Support) and EDM (Evaluate, Direct, and Monitor) field relate to ensure effectiveness of security controls that deals with incident response and recovery after the incident[10].

B. People, Process, and Technology

As previously explained, technology is always used as the primary solution in mitigating cyberattacks in cybersecurity[2]. However, cybersecurity is more than just a technical issue because it involves people, process, and technology, commonly referred to as PPT [11]. Whitman et al. (2012) argued that PPT is short for policies, people, and technology [12]. In this term, the process is similar to policies.

The people aspect includes individuals involved in cybersecurity, so managing cybersecurity is not only the responsibility of IT operators or IT divisions but also all employees and managers. The technology used to mitigate cyberattack still pose inherent risks due to new or outdated technologies. Of course, the process aspect is also very important to ensure the continuity of the organization when experiencing cyberattacks that can harm the organization and threaten personal data by providing legal or law enforcement. These three aspects are interrelated and play a role in ensuring effective cybersecurity.

The relationship between people and technology is very apparent, with the concept of the right man behind the gun. Technology can be maximally utilized effectively and efficiently if held by the right person. Likewise, between process and people, the construction of process always involves people aspects as integration of experts knowledge from various sources [13].

C. Analytic Hierarchy Process (AHP)

Saaty proposed the Analytic Hierarchy Process (AHP) as a quantitative method for selecting alternatives using multicriteria for decision-making involving many components that cannot be measured or intangible [4]. The AHP method relies on expert's judgment to determine priority scales in a pairwise comparison between criteria. It is then calculated get the weight of each criterion to be considered for decision-making. Many studies used the AHP method to obtain the best decision in Multiple Criteria Decision Making (MCDM) for manufacturing, government, industry, and supply chain management (SCM) [5].

Following are the steps of the AHP method for breaking down complex and unstructured problems in a hierarchical order to generate priorities and make an organized decision[4]:

1. Define the problem and determine the desired knowledge;
2. Define the structure of decision hierarchy starting from the top with the decision goal, followed by broad objectives, intermediate criteria, and finally, a set of alternatives;
3. Create pairwise comparison matrices to compare elements of each criterion with respect to the criterion in the level above;
4. Utilize the priorities obtained from these comparisons to assign the weight, repeat this process for each criterion, and calculate global priority by summing all the weighted values.

To obtain a prioritized scale, the AHP method requires expert assessment [4]. Saaty and Özdemir state that the determination of the number of experts is not based on the sample size, but on how much and how well the experts know the research subject based on several criteria such as education, length of experience, and level of achievement in society [14]. However, to maintain the consistency limit, the number of experts is recommended to be no more than 7 or 8 judges.

The consistency is determined by the Consistency Ratio (CR) value. If the CR value is zero, it means the decision made from the judgment of experts is consistent. It is acceptable if the CR value is less than 0. Otherwise, the result is closer to randomness, so they must be reassessed. The CR value is calculated by equation 1, which requires the Consistency Index (CI) and Reference Index (RI) values.

$$CR = \frac{CI}{RI} \leq 0.1 \quad (1)$$

The CI value is calculated by the maximum eigenvector (λ_{max}) where it is the result of a pairwise comparison matrix

and number of experts (n) as shown in equation 2. While RI value is given by Saaty, as shown in Table I.

$$CI = \frac{\lambda_{max} - n}{n-1} \quad (2)$$

TABLE I. RI REFERENCE VALUE (SAATY, 2008)

Order of Randomness	1	2	3	4	5	6	7	8	9	10
Reference Index (RI)	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

III. RESEARCH METHODOLOGY

The following research questions were constructed to achieve the objectives of this research:

RQ1: What core component is the top priority for implementing a cybersecurity framework in e-government?

RQ2: What aspect is the top priority for implementing a cybersecurity framework in e-government?

RQ3: What are the recommendations in designing effective and sustainable cybersecurity framework strategies for e-government based on the results of the priority evaluation of the people, process and technology aspects?

This research took a mixed quantitative and qualitative approach toward evaluating the cybersecurity framework implementation in e-government. The primary instruments of this research consisted of an AHP pairwise comparison questionnaire, open-ended and closed-ended questions. The questionnaire was answered by the informants through an online form and then the feedback was collected and validated according to the prescribed method. We used purposive sampling with 8 (eight) experts who were purposefully selected based on their extensive background in academia, practitioner, and government officer, with each informant possessing 10-20 years of experience in cybersecurity. The background details of the experts are shown in the graph below.

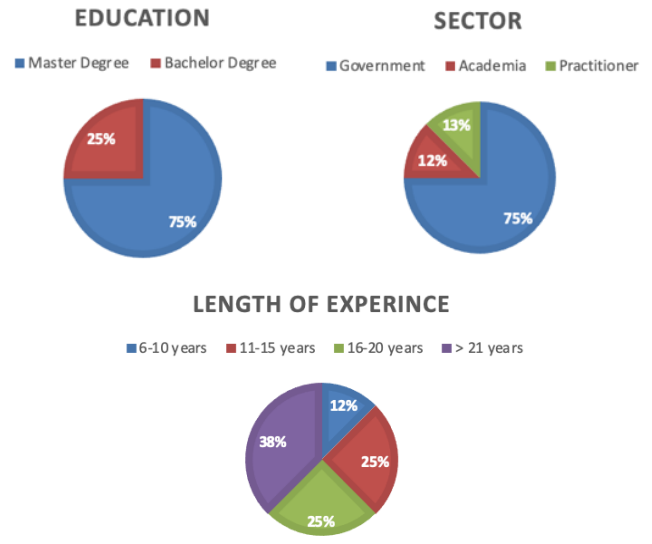

Fig. 1. Experts Profiles

According to Saaty's guideline, the next step of the AHP method after defining the problem, is to formulate a hierarchy of the criteria and the alternatives to achieve decision goal at the top of the hierarchy. The goal is to choose the top priority aspects for cybersecurity framework implementation. The criteria consist of five core cybersecurity components, namely identify, detect, protect, respond, and recover. And the alternatives are people, process, and technology that will be chosen to achieve the goal. Fig. 2 is the structure of the decision hierarchy that has been constructed.

Once the decision hierarchy is defined, the next step is to collect data through a questionnaire of experienced cybersecurity experts as informants. The Informants will be asked to compare each pair of criteria and sub-criteria based on the intensity of importance, as shown in Table II. To maintain data validity and reliability, the questionnaire will be tested on several informants before being disseminated to ensure the questions asked were clear and well-understood

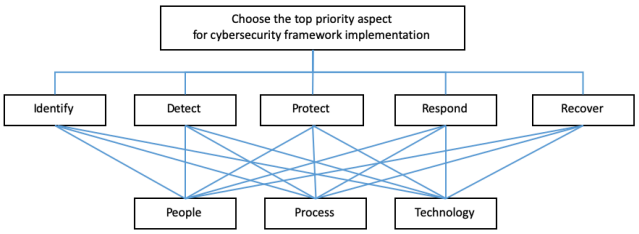

Fig. 2. Structure of decision hierarchy

TABLE II. INTENSITY OF IMPORTANCE (SAATY, 2008)

Intensity	Definition	Explanation
1	Equal importance	Two elements contribute equally to the objective
3	Moderate Importance	Experience and judgment slightly favor one aspect over another
5	Strong Importance	Experience and judgment strongly favor one element over another
7	Very strong Importance	One aspect is favored very strongly over another, its dominance is demonstrated in practice
9	Extreme Importance	The evidence favoring a element over another is of the highest possible order of affirmation
2,4,6,8 can be used to express intermediate values		

In the AHP questionnaire, 5 criteria and three alternatives require 25 pairwise comparisons. Then, we performed calculations of eigenvalue and eigenvector methods to obtain the relative weight of each criterion and alternative. The results of the AHP analysis will give the weight for each criterion and alternative, so it can be a consideration to decide what is the top priority among five core components and three aspects that most contribute to the implementation of cybersecurity frameworks in e-government.

After conducting the AHP analysis, we proceeded with a qualitative approach to gather expert opinions for the designing effectiveness and sustainability of cybersecurity framework strategy in e-government. We utilized closed-ended questions to elicit expert perspectives and open-ended questions to gather recommendations. Specifically, we sought insights from experts regarding the top priority among the three evaluated aspects for implementing a cybersecurity framework in e-government.

IV. Result Of Evaluation

After distributing the questionnaires, most responses were received in a completed state. There is no requirement for minimal additional clarifications regarding the completion process, pairwise comparison, or the AHP scale. It was observed that the background information and instructions provided were generally understandable to the participants, as evidenced by their accurate completion of the questionnaires.

The evaluation results show that identification has the highest priority in the e-government cybersecurity framework. This shows that an important step in maintaining system security is to understand the threats and identify vulnerabilities that can be exploited by unauthorized parties. In an e-government context, where systems must protect sensitive data and serve the public securely, effective identification is a top priority before implementing protection, detection, respond, and recovery. The result of the pairwise comparison in the core component of the cybersecurity framework is shown in Table III, and the weight is in Fig. 3.

TABLE III. Pairwise Comparison of Core Component Cybersecurity

	Identify	**Protect**	**Detect**	**Respond**	**Recover**
Identify	**1,000**	2,550	2,043	2,643	3,043
Protect	0,392	**1,000**	3,032	3,143	3,917
Detect	0,490	0,330	**1,000**	2,460	2,483
Respond	0,378	0,318	0,407	**1,000**	3,417
Recover	0,329	0,255	0,403	0,293	**1,000**

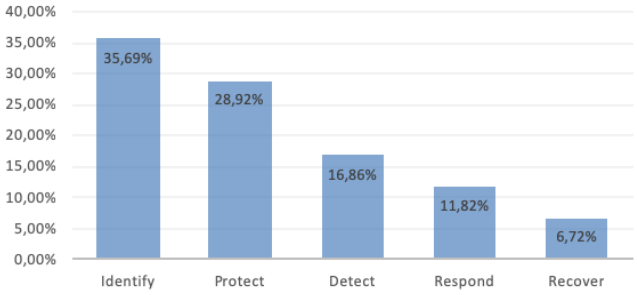

Fig. 3. The Weight for the Criteria

Using the equation 1 provided in the AHP Method, we calculated the Consistency Ratio (CR) with a result of 0.093. The decision is consistent if the CR is less than 0.1. So, it can be concluded that the weight for the criteria describes the priority of core component for implementing cybersecurity framework respectively identify (35.69%), protect (28,92%), detect (16.86%), respond (11.82%), and finally recover (6.72%). To obtain the final results, we calculated pairwise comparisons for each of the three aspects concerning the five core components. The final results of the evaluation are shown in Table IV and Fig. 4 below.

TABLE IV. Synthesizing To Obtain The Final Results

Criteria and Sub-criteria Weight	Identify	Protect	Detect	Respond	Recover	**Overall Priority**
	0,350	0,286	0,169	0,126	0,069	
People	0,682	0,665	0,634	0,694	0,585	**0,664**
Process	0,234	0,237	0,255	0,208	0,287	**0,239**
Technology	0,084	0,097	0,110	0,098	0,128	**0,097**

The final result shows that the highest priority weight is the people aspect, with a score of 66.39%. The second is the process aspect with a score of 23.89%, and lastly, the technology aspect with a score of 9.71%. The findings of this research further reinforce the notion that the people aspect or human factor holds the utmost significance in implementing a cybersecurity framework. However, these results do not address how the human factor can effectively and efficiently enhance cybersecurity measures to prevent cyberattacks, given that technology remains the applicable solution in the current context. Insights from experts who have completed the questionnaire can provide recommendations for answering the question.

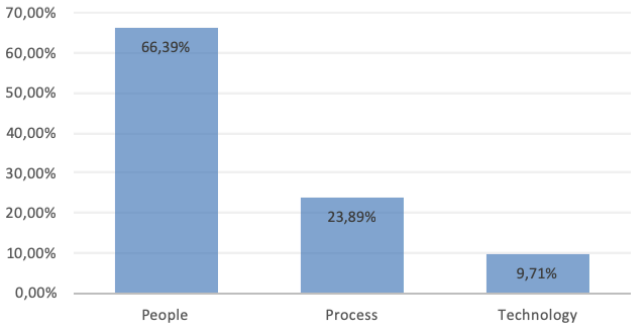

Fig. 4. The Prioritization of Global Weight

V. Recommendations

To gather expert recommendations, we presented closed and open-ended questions relating to the people, process, and technology aspects of implementing a cybersecurity framework. This approach is implemented to ensure the inclusion of all recommendations, thereby aligning them with the final result of this research, prioritizing the people aspect as the top priority.

Recommendations for the people aspect consist of developing or revising cybersecurity with a people aspect approach, enhancing compliance with cybersecurity practices, improving personnel competencies through education and training, and strengthening security awareness programs. The weight assigned to each recommendation varies depending on the number of experts who agree with the specific recommendations derived from the closed-ended questions, as shown in Fig. 5. Additional offers from the open-ended questions include promoting collaboration and synergy among different entities involved in cybersecurity and ensuring strong support from top management.

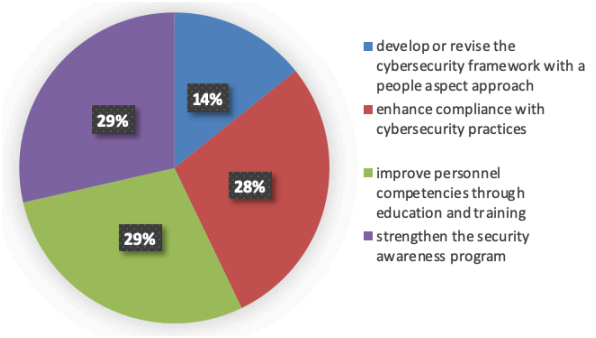

Fig. 5. Recommendation for People Aspect

Next, the recommendations of the process aspect are developing or revising the cybersecurity framework based on the process aspect approach, ensuring compliance and regularly updating required regulations and policies, enhancing the implementation of risk management practices, and conducting continuous security monitoring and regular audits. The weight of each recommendation on the process aspect is shown in Fig. 6. An additional recommendation from the open-ended questions is to emphasize periodic updating of procedures following referenced regulations and policies.

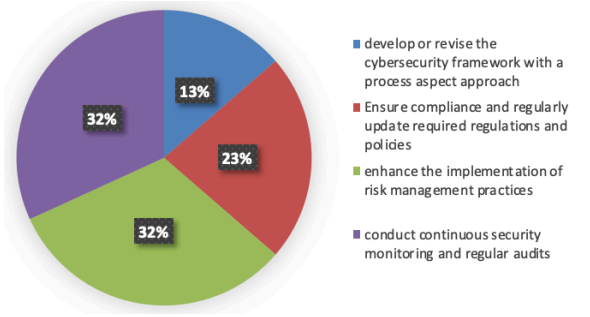

Fig. 6. Recommendation for Process Aspect

For the technology aspect, the recommendations are developing or revising the cybersecurity framework based on the technology aspect approach, fulfilling the necessary cybersecurity hardware and software requirements, updating outdated technology, and implementing robust cryptography technology based on data sensitivity levels. The weight of each recommendation is shown in Fig. 7. An additional recommendation from the open-ended questions is managing the data processing technology properly and precisely.

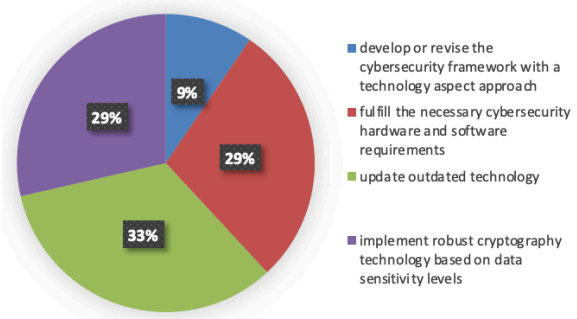

Fig. 7. Recommendation for Technology Aspect

VI. Conclusion

In summary, this research has evaluated the priority of five core components and three aspects for implementing a cybersecurity framework in e-government. This research used a mixed quantitative and qualitative approach by utilizing the AHP method to determine the priorities of all aspects and collecting expert's judgments to get recommendations based on the prioritized results. The findings show that the identify aspect is the top priority among the core components and emphasizes the importance of thorough preparation before implementing the other components. Additionally, the results reveal that the people aspect holds the highest priority among the three aspects, emphasizing the significance of effectively and sustainably implementing the cybersecurity framework.

Based on the prioritization results, several recommendations are proposed for managing the people aspect within the cybersecurity framework. These recommendations include enhancing compliance, improving competencies through education and training, implementing a robust security awareness program, developing or revising the cybersecurity framework focusing on the people aspect, fostering collaboration and synergy among entities, and obtaining strong support from management. These recommendations aim to enhance the role of individuals as people aspect and their contribution to the overall cybersecurity framework, ultimately improving the effectiveness and resilience of e-government systems.

Our suggestion for future research is to explore other alternative AHP methods to get more precise results or even strengthen this research. Additionally, involving more experts would increase the depth and breadth of insights gathered for generating comprehensive recommendations.

Acknowledgment

The authors acknowledge the support from the Educational Fund Management Institution, Ministry of Finance Indonesia (Lembaga Pengelola Dana Pendidikan/LPDP) for granting the scholarship. This research is also supported by the E-Government Laboratory, Faculty of Computer Science, University of Indonesia.

References

[1] W. Yeoh, S. Wang, A. Popovič, and N. H. Chowdhury, "A systematic synthesis of critical success factors for cybersecurity," *Computers & Security*, vol. 118, p. 102724, Jul. 2022, doi: 10.1016/j.cose.2022.102724.

[2] N. Gcaza and R. von Solms, "Cybersecurity Culture: An Ill-Defined Problem," in *Information Security Education for a Global Digital Society*, M. Bishop, L. Futcher, N. Miloslavskaya, and M. Theocharidou, Eds., in IFIP Advances in Information and Communication Technology, vol. 503. Cham: Springer International Publishing, 2017, pp. 98–109. doi: 10.1007/978-3-319-58553-6_9.

[3] Verizon, "2022 Data Breach Investigations Report." 2022. [Online]. Available: https://www.verizon.com/business/en-

gb/resources/2022-data-breach-investigations-report-dbir.pdf
[4] T. L. Saaty, “Decision making with the analytic hierarchy process,” *IJSSCI*, vol. 1, no. 1, p. 83, 2008, doi: 10.1504/IJSSCI.2008.017590.
[5] B. M. Mohsen, “Multi-Criteria Decision System for the Selection of A Freight Forwarder Using AHP,” *Procedia Computer Science*, vol. 220, pp. 135–144, 2023, doi: 10.1016/j.procs.2023.03.020.
[6] NIST, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
[7] H. Taherdoost, “Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview,” *Electronics*, vol. 11, no. 14, p. 2181, Jul. 2022, doi: 10.3390/electronics11142181.
[8] ISO IEC, “ISO IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems Requirements.” 2022.
[9] CIS, “CIS Controls v8 Guide.” Center for Internet Security, Inc. (CIS®)., 2021.
[10] S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, “COBIT as a Framework for Enterprise Governance of IT,” in *Enterprise Governance of Information Technology*, in Management for Professionals. Cham: Springer International Publishing, 2020, pp. 125–162. doi: 10.1007/978-3-030-25918-1_5.
[11] M. Parent and B. Cusack, “Cybersecurity in 2016: People, technology, and processes,” *Business Horizons*, vol. 59, no. 6, pp. 567–569, Nov. 2016, doi: 10.1016/j.bushor.2016.08.005.
[12] M.E. Whitman and H. J. Mattord, “Principles of Information Security.” 2012.
[13] B. Dave, E. Pikas, H. Kerosuo, and T. Mäki, “ViBR – Conceptualising a Virtual Big Room through the Framework of People, Processes and Technology,” *Procedia Economics and Finance*, vol. 21, pp. 586–593, 2015, doi: 10.1016/S2212-5671(15)00216-6.
[14] T. L. Saaty and M. S. Özdemir, “How Many Judges Should There Be in a Group ?,” *Ann. Data. Sci.*, vol. 1, no. 3–4, pp. 359–368, Dec. 2014, doi: 10.1007/s40745-014-0026-4.