

Analysis of Electronic-Based Government Systems (SPBE) Using the Six-Ware Cyber Security Framework (SWCSF) in West Sumatra Province

Muntalib Yudha Makatur^{1*}, Rudy A. G. Gultom², Achmad Farid Wadjidi³,
Dinifusya'ban⁴
Cyber Defense Engineering, Faculty of Science and Technology, Universitas
Pertahanan, Indonesia

Corresponding Author: Muntalib Yudha Makatur makatur8119@gmail.com

ARTICLE INFO

Keywords: E-Government,
Cybersecurity, SPBE, SWCSF

Received : 16, January

Revised : 30, January

Accepted: 24, February

©2025 Makatur, Gultom, Wadjidi,
Dinifusya'ban: This is an open-access
article distributed under the terms of
the [Creative Commons Atribusi 4.0
Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

Effective and secure e-government is a key factor in achieving good governance and high-quality public services. The Six-Ware Cyber Security Framework (SWCSF) was chosen for its strong focus on cybersecurity, a critical aspect in the implementation of Electronic-Based Government Systems (SPBE). This study employs a mixed-methods approach, combining qualitative and quantitative methods through interviews, observations, questionnaires, and descriptive data analysis. The research findings reveal varying levels of maturity across different security dimensions, with certain areas requiring further improvement to meet higher security standards in alignment with national policies for SPBE. Additionally, the study aims to provide a comprehensive overview of e-government maturity in West Sumatra, particularly from a cybersecurity perspective.

INTRODUCTION

The Electronic-Based Government System (SPBE) has become a crucial pillar in the digital transformation of government in Indonesia (Pemerintah Republik Indonesia, 2018). Indonesia holds significant potential in leveraging digital opportunities to enhance public services through information technology (Das et al., 2016). Through SPBE, the government aims to improve efficiency, transparency, and accountability in public services by utilizing information and communication technology (ICT) (Wuryantai, 2013; Yoserizal & Yudiatmaja, 2010). Presidential Regulation No. 95 of 2018 mandates the implementation of SPBE across all government institutions, with periodic evaluations of its maturity level (Pemerintah Republik Indonesia, 2018).

Since 2018, the National SPBE Index has continued to improve, and according to the 2022 E-Government survey by the United Nations, Indonesia's e-government index ranking reached 77 (United Nations, 2022). This result marks a significant improvement from its previous rank of 88 in 2020 (United Nations, 2022). This progress has been reflected across almost all institutions in Indonesia, including West Sumatra Province. This is evident from West Sumatra Province's inclusion among the nine provinces with the highest SPBE Index in Indonesia (Pemerintah Provinsi Sumatera Barat, 2023; Yoserizal & Yudiatmaja, 2010).

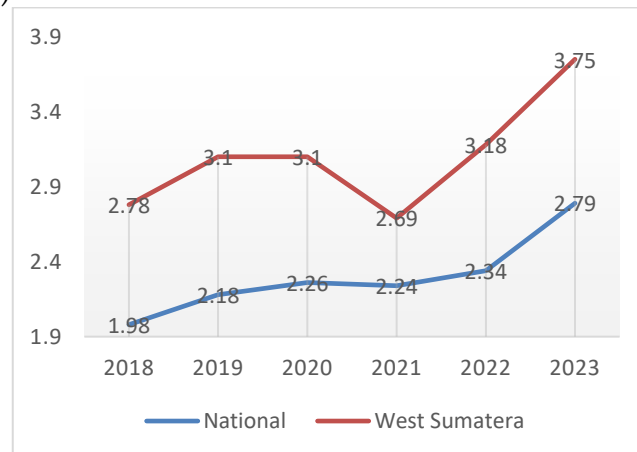


Figure 1. SPBE Index

The implementation of SPBE is not without significant cybersecurity challenges, which can be assessed using the Six-Ware Cyber Security Framework (SWCSF) (Gultom, 2019). The evolution of digital governance requires a robust framework to ensure its sustainability and successful implementation (Bakar et al., 2020). SWCSF emerges as a comprehensive solution to protect SPBE from various cyber threats. This framework, developed by Prof. Dr. Ir. Rudy Agus Gemilang Gultom, M.Sc., CEH., CIQaR, encompasses six key components: brainware, hardware, software, infrastructure-ware, firmware, and budgetware (Gultom et al., 2018). SWCSF focuses not only on technical aspects but also on human resources, infrastructure, and budget, offering comprehensive protection against potential cyberattacks (Gultom & Ahmad, 2022).

This study focuses on analyzing the maturity of digital security in SPBE within the West Sumatra Provincial Government based on the SWCSF (Pemerintah Provinsi Sumatera Barat, 2023). The research makes a significant contribution to the development of SPBE cybersecurity in West Sumatra by identifying areas that require further attention (Gultom et al., 2020). Measuring the cybersecurity maturity level in SPBE aims to provide an overview of how well organizations have developed and implemented effective security systems in terms of technology, governance, and human resources (Amali et al., 2020).

The results of this study are expected to provide valuable contributions to the provincial government in formulating appropriate strategies and policies to enhance SPBE cybersecurity, as well as to foster smarter and more secure governance (MENPANRB, 2020).

LITERATURE REVIEW

The Electronic-Based Government System (SPBE)

Cybersecurity generally refers to practices and technologies designed to protect systems, networks, and data from cyber threats, which can include attacks, unauthorized access, damage, or information theft (Lindgren et al., 2019). Cybersecurity encompasses various aspects, including physical security, network security, data encryption, identity management, and emergency response strategies for security incidents (Gultom et al., 2018). In the context of e-government, cybersecurity plays a crucial role as it involves protecting sensitive data belonging to the government and the public, as well as maintaining the integrity and availability of public services delivered digitally (Iannacci et al., 2019).

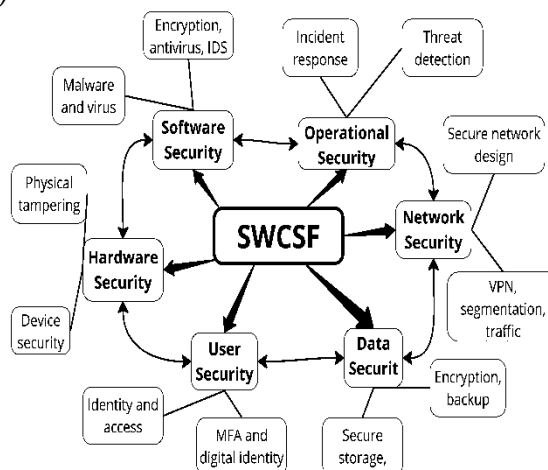


Figure 2. SPBE Cybersecurity Framework

The Electronic-Based Government System (SPBE) refers to the administration of government utilizing ICT to improve the quality of public services (Pemerintah Republik Indonesia, 2018). SPBE encompasses various aspects, including ICT infrastructure, applications, and data, as well as human resources and governance (Bakar et al., 2020). A digital transformation governance framework is necessary to ensure the effectiveness and efficiency of e-government implementation (Papavasiliou, 2020). Presidential Regulation No. 95 of 2018 mandates the implementation of SPBE across all government

institutions, aiming to create a government that is more transparent, accountable, efficient, and effective (Wuryantai, 2013).

Table 1. Domains and Aspects of SPBE

DOMAIN	ASPECT
Policy	• Internal Governance Policy
Governance	• Strategic Planing
	• ICT
	• Administrator
Management	• Management Implementation
	• ICT Audit
Services	• Administrative Services
	• Public Services

SPBE in West Sumatra Province aims to enhance bureaucratic efficiency through integrated, transparent, and innovative governance (Yoserizal & Yudiatmaja, 2010). The implementation of SPBE covers various domains and aspects with key achievements, such as improved information technology infrastructure, including integrated internet access in 51 Regional Government Organizations (OPDs) and 31 schools (Pemerintah Provinsi Sumatera Barat, 2023). Various public digital services have been provided, including licensing applications and complaint services (Pemerintah Provinsi Sumatera Barat, 2023). The level of transparency in e-government implementation affects public adoption and trust in government digital services (Sabani, 2021). Supporting regulations, such as Governor Regulation No. 59 of 2020 and various gubernatorial decrees, govern the architecture and internal audits of SPBE, ensuring sustainable and measurable implementation (Pemerintah Provinsi Sumatera Barat, 2020).

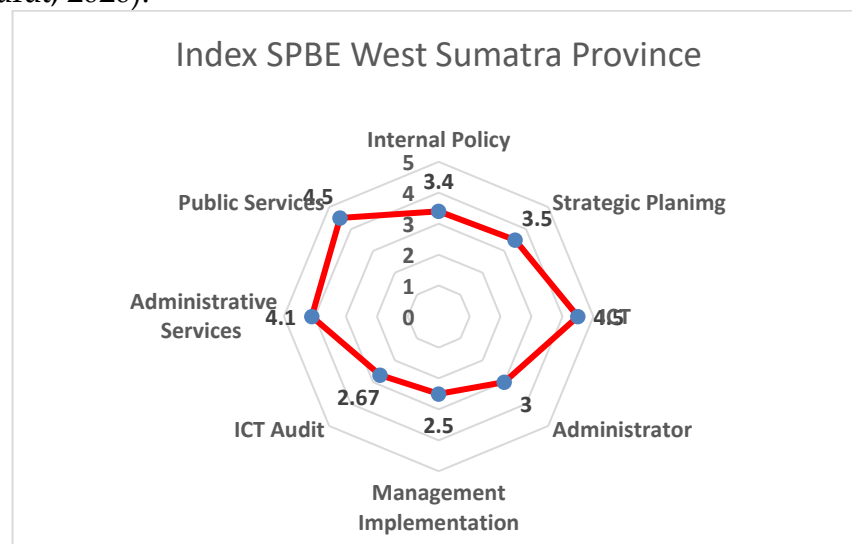


Figure 3. West Sumatera SPBE Index

The Six-Ware Cyber Security Framework

The Six-Ware Cyber Security Framework (SWCSF) is a cybersecurity framework developed to protect digital assets from various cyber threats. SWCSF consists of six main components: brainware, hardware, software, infrastructure-ware, firmware, and budgetware (Gultom et al., 2020). This framework is holistic, encompassing both technical and non-technical aspects, and can be applied to various types of organizations, including government institutions (Gultom & Ahmad, 2022). SWCSF has proven effective in enhancing an organization's preparedness and resilience against cyberattacks (Gultom et al., 2018).

Several previous studies have examined the application of SWCSF in the context of SPBE. Gultom et al. (2020) conducted research in Batam City, Indonesia, and found that SWCSF is suitable for application across various sectors, including local government, industry, and education (Gultom et al., 2020). This study shows that SWCSF can help organizations identify strengths and weaknesses in their cybersecurity and provide recommendations for improvement (Gultom et al., 2020).

Table 2. SWCSF Component

Component	Criteria
Brainware	The human factor is the primary and weakest aspect of network security
Hardware	Hardware plays a dominant role in addressing threats and vulnerabilities.
Software	Software protects applications such as email and websites from attacks
Infrastructure-Ware	This indicator plays a crucial role in facilitating secure networks.
Firmware	Includes security policy documents, SOPs, ISO standards, and operational and technical guidelines
Budgetware	Plays an important and strategic role as a facilitator for the implementation of all other indicators

Another study by Darmawan et al. (2021) applied SWCSF at the Palu Naval Base and found that this framework could help enhance Palu Naval Base's preparedness in facing cyber threats. The study also emphasized the importance of cross-sector collaboration and adequate resource allocation for cybersecurity (Darmawan et al., 2022). Meanwhile, Gultom and Wajdi (2022) applied the SWCSF at the Indonesian Ministry of Defense and found that this framework could help identify areas requiring improvement in the cyber defense system. The study also highlighted the importance of adequate budgets for cybersecurity (Gultom & Ahmad, 2022). Overall, previous research has demonstrated that SWCSF is an effective framework that can be applied in various contexts to enhance cybersecurity.

The e-government maturity model can be used to evaluate the success of SPBE implementation in different regions, including local governments (Sukarsa et al., 2020). This study will continue this tradition of research by focusing on evaluating SPBE cybersecurity in West Sumatra Province.

METHODOLOGY

A quantitative evaluation of the SWCSF implementation is conducted to measure and understand the success level of SPBE cybersecurity across various government institutions (Gultom & Ahmad, 2022). The quantitative research method is highly effective for measuring and analyzing data focused on the success rate of technology implementation (Sugiyono, 2018). This approach involves using questionnaires targeting SPBE service managers and users, with the results analyzed using data normalization, min-max, and aggregation methods to produce the SWCSF Index (Gultom et al., 2020). Measurement steps, index calculation methods, and guidelines for visualizing and interpreting the results are further detailed (Iannacci et al., 2019).

The initial stage of quantitative measurement for SWCSF implementation begins with identifying the goals and objectives to be achieved in enhancing SPBE cybersecurity (Gultom & Ahmad, 2022). These objectives may include improving literacy, system protection, or incident response (Gultom et al., 2020). Subsequently, a deep understanding of the six main components of SWCSF (Brainware, Hardware, Software, Infrastructureware, Firmware, and Budgetware) forms the foundation for designing accurate measurement instruments (Gultom et al., 2018).

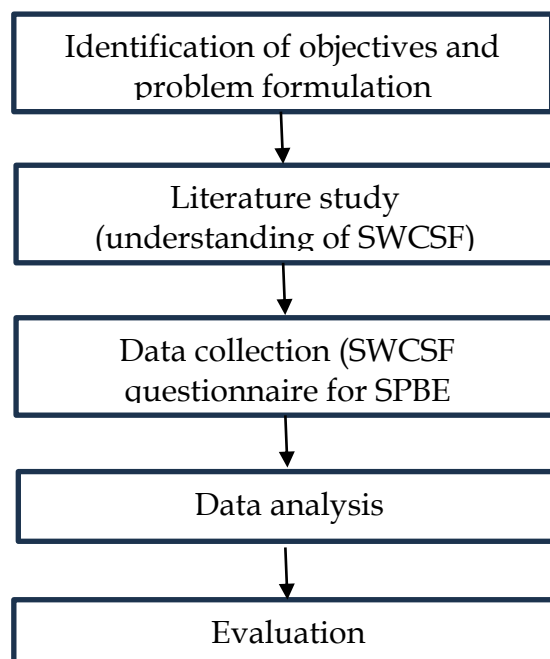


Figure 4. Research Flow

Formulating the questionnaire is a crucial step in data collection. The questionnaire is developed based on the six components of SWCSF and is aimed at SPBE administrators and service users. A Likert scale of 1-5 is used to

rate each question, providing a structured assessment range (Iannacci et al., 2019). Once the questionnaire is formulated, the next step is data collection by distributing the questionnaire to relevant respondents and gathering the responses (Gultom et al., 2020).

The next critical step is data normalization using the min-max method. This process ensures that all variables are on the same scale, enabling fair and accurate comparisons among the various SWCSF components (Iannacci et al., 2019). After normalization, the average score for each component is calculated and then aggregated to produce the total SWCSF Index. This index provides an overall picture of the cybersecurity effectiveness of SPBE in government institutions (Gultom et al., 2020).

Visualizing the measurement results using Radar Charts or Heatmaps simplifies interpretation and helps identify areas that require further improvement (Iannacci et al., 2019). The final stage in calculating the SWCSF Index is value aggregation. At this stage, the average values of the six SWCSF components are combined to produce a single index score. This score offers an overall overview of the cybersecurity effectiveness level of SPBE in the evaluated government institutions (Gultom & Ahmad, 2022).

RESEARCH RESULT

The interviews were conducted at the West Sumatra Provincial Communication and Information Agency (Dinas Kominfo Pemprov Sumbar), represented by the Head of Informatics and the Head of Cybersecurity, as well as SPBE users represented by the Secretary of the West Sumatra Provincial Communication and Information Agency. The results, as presented in Table 3, reveal perceptions regarding the main components of the SWCS framework. This table identifies gaps and priorities in achieving robust SPBE maturity in West Sumatra.

Table 3 Interview Result

SWSC	ADMINISTRATOR	USER
Brainware	4	3
Hardware	4	4
Software	4	3
Infrasware	3	2
Firmware	3	3
Budgetware	3	2

The survey results show that the hardware aspect received a high score (4), but brainware and infrastructure-ware need more attention, with lower scores (3 and 2). Budgetware is also an area that needs improvement, with the lowest score (2.88), indicating a need for increased funding to support the development and security of SPBE.

The SPBE Management Respondents consist of 30 Civil Servants (ASN) from various divisions of the Communication and Information Agency (Dinas Kominfo) related to SPBE. Respondent data can be seen in Figure 5.

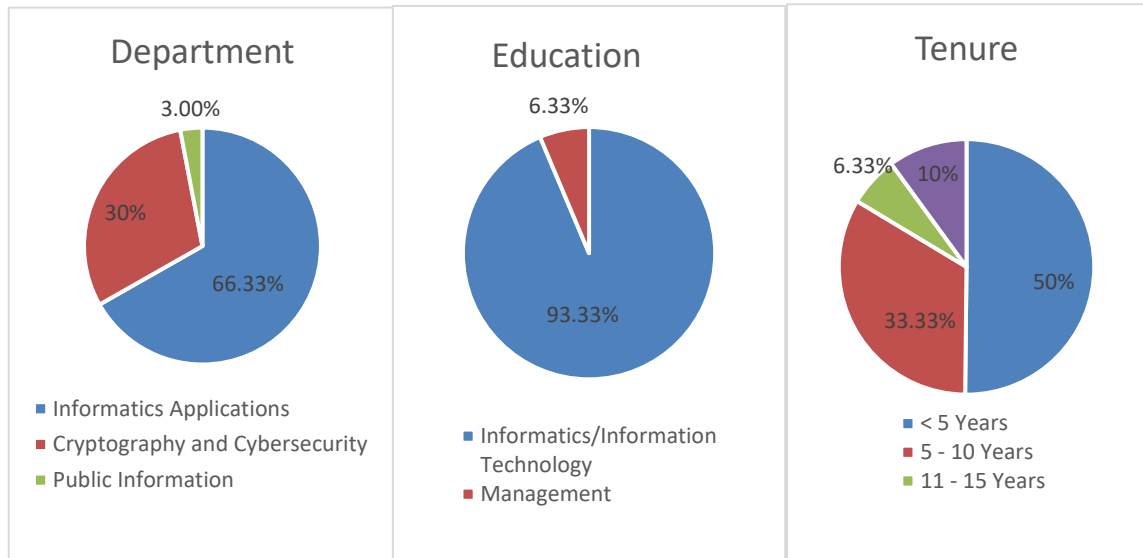


Figure 5. SPBE Administrator Respondents

Most SPBE administrators (66.33%) work in the application systems department, focusing on e-government systems, while 30% are in cybersecurity, highlighting data protection. Only 3.33% are in public information, showing its minor role. Nearly all administrators (93.33%) have backgrounds in informatics or IT, with just 6.33% in management, emphasizing technical expertise.

Regarding experience, 50% have less than 5 years, 33.33% have 5-10 years, and 16.66% have more than 10 years, suggesting a mix of adaptability and the need for knowledge transfer between newer and experienced staff to strengthen SPBE.

The SPBE User Respondents consist primarily of Civil Servants (ASN) representing Regional Government Organizations (OPD). Respondent data can be seen in Figure 6.

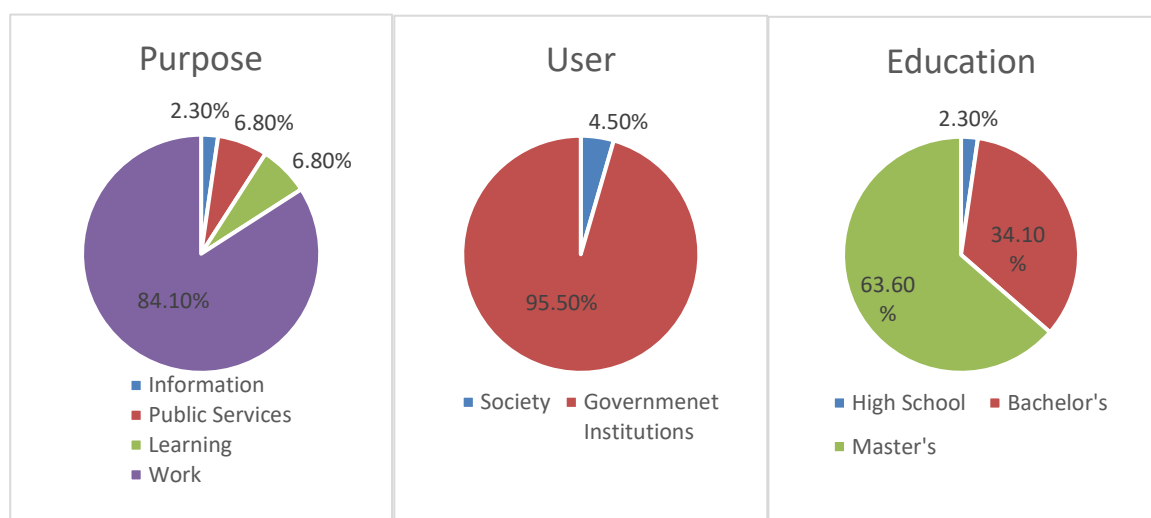


Figure 6. SPBE User Respondents

The data from SPBE user respondents reveals key insights: the first pie chart shows that 84.1% of users utilize SPBE for work purposes, while 6.8% use it for learning and another 6.8% for public services. The second chart indicates that 95% of the users are civil servants from West Sumatra. The third pie chart provides information on the educational background of the respondents, with 63% holding a Master's degree (S2) and 34.21% having a Bachelor's degree (S1). This suggests that the majority of users are highly educated and primarily use SPBE for professional purposes.

SPBE in West Sumatra has been implemented since 2018. In the questionnaire, open-ended questions were posed to users regarding the common challenges they face and areas requiring changes and improvements. Twenty-five percent of respondents suggested enhancing the reliability of data and network security. The complete results can be seen in Figure 7.

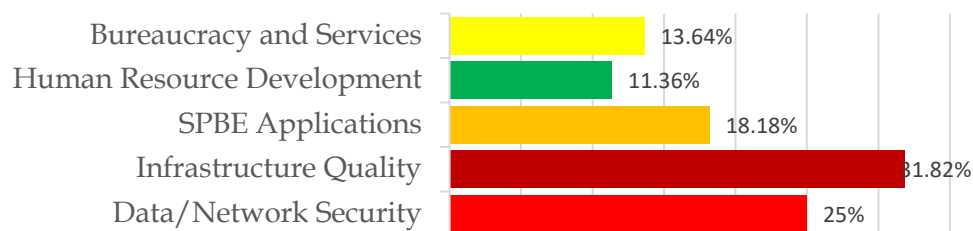


Figure 7. SPBE Improvement Suggestions

The data from SPBE user suggestions in West Sumatra reveals key areas for improvement: 31.82% of users emphasize the need to improve infrastructure quality, while 25% are focused on enhancing data and network security, highlighting concerns about protection from cyber threats. Additionally, 18.18% suggest improvements to the SPBE applications themselves, aiming for better functionality and performance. Human resource development (11.36%) is also seen as essential for strengthening the system, and 13.64% of users call for better bureaucratic efficiency and public services. Overall, users are seeking a more secure, efficient, and well-supported SPBE system.

In 2023, the West Sumatra Provincial Government's SPBE received an award from the Ministry of Administrative and Bureaucratic Reform (Menpanrb) as one of the top 10 provinces with the best SPBE index development. The public service and digital service indices consistently received high ratings (see Figure 3). Recognizing the importance of SPBE in the future, user respondents expressed the need for reliable digital services and mature cybersecurity, supported by high-quality infrastructure and well-integrated systems or applications (see Figure 8).

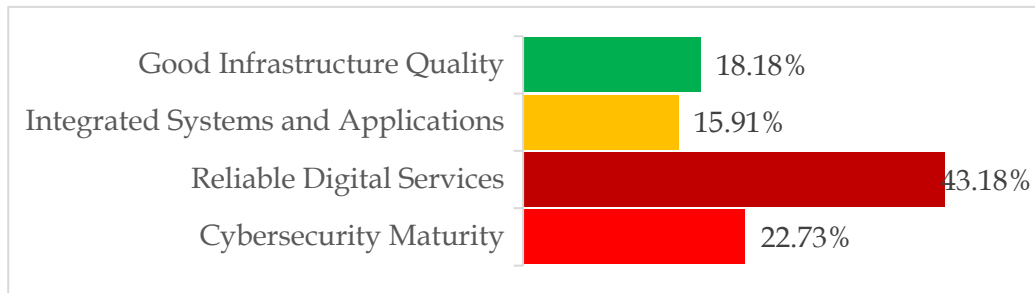


Figure 8. Future Expectations of SPBE

The data shows that SPBE users in West Sumatra have clear expectations for the future of the system. The majority (43.18%) prioritize reliable digital services, indicating that users value consistent and accessible services the most. Additionally, 22.73% of respondents emphasize the need for improved cybersecurity maturity, reflecting concerns about protecting sensitive data and systems from cyber threats. About 18.18% highlight the importance of good infrastructure quality, showing that robust and stable infrastructure is essential for the system's success. Lastly, 15.91% of users stress the need for better-integrated systems and applications, suggesting that seamless connectivity between different SPBE components is key to improving the overall user experience.

We can observe from Table 4 that the SWCS Index indicates the average values of six indicators reflecting the level of cybersecurity maturity in the Electronic-Based Government System (SPBE) in West Sumatra. The "Hardware" indicator has the highest value at 3.51, signifying strength in hardware management. Conversely, the "Budgetware" indicator has the lowest value at 2.88, highlighting the need for improvement in budget allocation to support cybersecurity. Overall, the SWCS Index demonstrates an average score of 3.21, indicating a fairly good level of cybersecurity.

This can also be seen in the radar chart in Figure 9, where significant improvements are needed in aspects such as budgeting, infrastructure, and policy documentation to achieve a more mature and holistic cybersecurity level.

Table 4. SWCS Index

INDIKATOR	INDEKS
Brainware	3,32
Hardware	3,51
Software	3,41
Infrasware	3,06
Firmware	3,12
Budgetware	2,88
SWCS	3,21

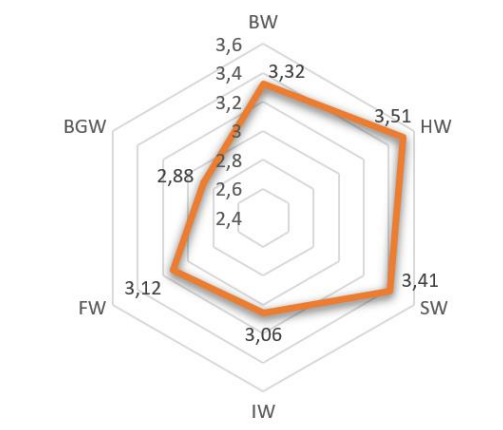


Table 4 presents the SWCS Index, reflecting the cybersecurity maturity of SPBE in West Sumatra. The highest score is in hardware (3.51), suggesting strong physical infrastructure, followed by software (3.41), indicating secure systems and applications. However, infrastructureware (3.06) and firmware (3.12) show areas that need improvement, particularly in network security and security policy enforcement. The brainware score (3.32) highlights moderate attention to human resources and cybersecurity awareness, while the lowest score is in budgetware (2.88), pointing to insufficient funding for cybersecurity and system development. Overall, the SWCS Index of 3.21 shows that while SPBE's cybersecurity is fairly mature, there is a need for improvement in funding, infrastructure, and policy implementation to strengthen the system further. Overall, the Spider Chart emphasizes that while hardware and software are well-managed, significant improvements are required in areas like budgeting, infrastructure, and policy documentation to achieve a more mature and robust cybersecurity environment for SPBE in West Sumatra.

DISCUSSION

The results of this study provide important insights into the current state of the Electronic-Based Government System (SPBE) in West Sumatra, especially regarding its cybersecurity readiness. The highest scores in the SWCS Index were in hardware (3.51) and software (3.41), showing that the physical infrastructure and software systems supporting SPBE are relatively strong and secure. These results reflect findings from previous studies that stress the importance of solid infrastructure for supporting effective e-government services (Gultom et al., 2020). However, lower scores in infrastructureware (3.06) and firmware (3.12) suggest that improvements are still needed in areas like network security and policy enforcement. This is consistent with research indicating the need for more resilient infrastructure to protect against evolving cyber threats (Darmawan et al., 2021).

The brainware score (3.32) suggests that while the human resources managing SPBE are adequately trained, there's still room to grow in terms of cybersecurity education and awareness. As the human element remains a key vulnerability in cybersecurity, further investment in training and development is essential (Gultom et al., 2020). Additionally, the budgetware score (2.88) highlights a critical issue: there's insufficient funding to fully support the ongoing development and enhancement of SPBE's security and technological systems. Adequate financial resources are necessary to ensure that SPBE keeps up with both technological advances and rising cyber threats (Gultom & Wajdi, 2022).

Looking ahead, users of SPBE in West Sumatra have clear expectations for its future development. Most respondents (43.18%) emphasized the importance of reliable digital services, suggesting that the primary focus should be on ensuring the system remains accessible and dependable. Moreover, 22.73% of users highlighted the need for cybersecurity maturity, underlining the growing concern for secure digital governance. These findings show that while SPBE has made significant strides, there are still challenges to address, particularly in

terms of infrastructure, cybersecurity, and human resource development, to meet the evolving needs of users and strengthen the system's overall security.

CONCLUSIONS AND RECOMMENDATIONS

In conclusion, the implementation of the Electronic-Based Government System (SPBE) in West Sumatra has made notable progress, particularly in terms of hardware and software security. However, the study highlights areas that still require attention, such as strengthening network infrastructure, improving security policies, and increasing funding for continued development. While the human resources managing SPBE are adequately trained, further investment in cybersecurity education is needed to ensure a well-rounded, secure system. The growing concerns over cybersecurity and the demand for reliable digital services suggest that the system must evolve to meet the increasing expectations of its users.

Based on the findings, it is recommended that the government of West Sumatra prioritize enhancing its cybersecurity framework by addressing the infrastructure and policy gaps identified in this study. Investments should be made to improve network security, formalize security policies, and ensure that all aspects of SPBE are well-integrated. Additionally, more financial resources need to be allocated to support the ongoing development and protection of the system. Finally, continuous professional development for SPBE administrators should be emphasized, focusing on improving cybersecurity literacy and keeping up with technological advancements to maintain the system's resilience in the face of evolving threats.

ADVANCED RESEARCH

While this study provides valuable insights into the cybersecurity maturity of SPBE in West Sumatra, further research is needed to explore the effectiveness of specific cybersecurity measures within the system. Future studies could examine the impact of real-world cyber threats on SPBE's performance and security, identifying vulnerabilities that may not be evident through internal assessments. Additionally, research could investigate the role of user behavior in maintaining the system's security, focusing on how user training and awareness programs could reduce human error. Comparative studies with other regions or countries implementing similar e-government systems could offer useful benchmarks for improving the SPBE framework and its resilience against cyber risks.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to all the individuals and institutions who contributed to the success of this research. Special thanks to the SPBE administrators and users in West Sumatra for their valuable time, insights, and cooperation during the data collection process. I also wish to acknowledge the support from the faculty and colleagues at the Republic of Indonesia Defense University, whose guidance and encouragement were essential in completing this study. Finally, I would like to thank my family and

friends for their continuous support and understanding throughout this research journey.

REFERENCES

- Amali, L. N., Katili, M. R., Suhada, S., & Hadjaratie, L. (2020). The measurement of maturity level of information technology service based on COBIT 5 framework. *Telkomnika (Telecommunication Computing Electronics and Control)*, 18(1), 133-139.
- Bakar, K. A., Ibrahim, R., & Yunus, Y. (2020). Digital government evolution and maturity models: A review. *Open International Journal of Informatics*, 8(2), 70. <https://www.researchgate.net/publication/362467584>
- Das, K., et al. (2016). Unlocking Indonesia's digital opportunity. *McKinsey Indonesia Office*, 11-12.
- Darmawan, N., Poniman, A., & Gultom, R. A. (2022). Konsep pembangunan teknologi pertahanan cyber security berbasis Six-Ware Framework di markas komando pangkalan Tentara Nasional Indonesia Angkatan Laut Palu. *Teknologi Penginderaan*, 3(2).
- Firdaus, I., Tursina, M., & Roziqin, A. (2021). Transformasi birokrasi digital di masa pandemi COVID-19 untuk mewujudkan digitalisasi pemerintahan Indonesia. *Kybernan: Jurnal Studi Pemerintahan*, 4(2), 226-239. <https://doi.org/10.35326/kybernan.v4i2.12>
- Gultom, R. A. G. (2019). *Cyber warfare: Sudah siapkah kita menghadapinya*. Bogor: UNHAN Press.
- Gultom, R. A. G., Midhio, W., Silitonga, T., & Pudjiatmoko, S. (2018). Introducing the six-ware cyber security framework concept to enhancing cyber security environment. *Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018)*, 262-271.
- Gultom, R. A. G., & Ahmad, F. W. (2022). Development of Six-Ware Cyber Defense Framework (SWCDF) design as a standardization of computer network protection state defense information system. *International Journal of Arts and Social Science*, 5(3).
- Gultom, R. A. G., Farid, A., Lestari, A. A., Lahallo, C. A. S., & Akbar, R. N. (2020). Cyber-based defense technology development of the Six-Ware Cyber Framework to enhance the implementation of the national defense system in the city of Batam. *International Journal of Advanced Science and Technology*, 29(7), 3431-3436.
- Iannacci, F., Seepma, A. P., Blok, C. de, & Resca, A. (2019). Reappraising maturity models in e-government research: The trajectory turning point theory. *Journal of Strategic Information Systems*, 28(3), 310-329. <https://doi.org/10.1016/j.jsis.2019.02.001>
- Lindgren, I., Madsen, C. Ø., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A research agenda for the digitalization of public services. *Government Information Quarterly*, 36(3), 427-436. <https://doi.org/10.1016/j.giq.2019.03.002>
- MENPANRB. (2020). *Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik*. Direktur

- Jenderal Peraturan Perundang-Undangan Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, 5(261), 1689–1699.
- MENPANRB. (2023). *Laporan Hasil Evaluasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Nasional Tahun 2023*. Jakarta: Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia.
- Mulyadi, M. (2019). Penelitian kuantitatif dan kualitatif serta pemikiran dasar menggabungkannya. *Jurnal Studi Komunikasi dan Media*, 15(1), 128.
- Muttaqin, M. H., & Susanto, T. D. (2019). The effect of website components on user trust in increasing the interest to use public administration service on e-government website. *2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)*, 30–36.
- Papavasiliou, S. (2020). A digital transformation governance framework for e-government: A systemic approach. *University of Adelaide Digital Library*. <https://digital.library.adelaide.edu.au/dspace/handle/2440/126968>
- Pemerintah Republik Indonesia. (2018). *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*.
- Pemerintah Provinsi Sumatera Barat. (2022). *Peraturan Gubernur Provinsi Sumatera Barat Nomor 09 Tahun 2022 tentang Tata Cara Pengelolaan Nama Domain dan Subdomain*.
- Pemerintah Provinsi Sumatera Barat. (2020). *Peraturan Gubernur Provinsi Sumatera Barat Nomor 59 Tahun 2020 tentang Rencana Induk SPBE*.
- Pemerintah Provinsi Sumatera Barat. (2023). *Laporan Hasil Evaluasi SPBE 2023 Pemerintah Provinsi Sumatera Barat*.
- Sabani, A. (2021). Investigating the influence of transparency on the adoption of e-government in Indonesia. *Journal of Science and Technology Policy Management*, 12(2), 236–255.
- Sugiyono. (2018). *Metode penelitian kuantitatif, kualitatif dan R&D*. Bandung: Alfabeta.
- Sukarsa, I. M., et al. (2020). Evaluation of e-government maturity models in sub-district public services in Indonesia using the SPBE framework. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 4(2), 243–253. <https://doi.org/10.29207/resti.v4i2.1825>
- United Nations, E.-G. S. (2020). *Digital Government in the Decade of Action for Sustainable Development: With addendum on COVID-19*, Vol. 1, No. 1. 2020.
- United Nations. (2022). *UN E-Government Survey 2022: The Future of Digital Government*. Department of Economic and Social Affairs, United Nations. Retrieved from <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022>
- Wuryantai, A. E. W. (2013). Digitalisasi masyarakat: Menilik kekuatan dan kelemahan dinamika era informasi digital dan masyarakat informasi. *Jurnal Ilmu Komunikasi*, 1(2). <https://doi.org/10.24002/jik.v1i2.163>
- Yoserizal, Y., & Yudiatmaja, W. E. (2010). Strategi pemerintah Provinsi Sumatera Barat dalam mengembangkan e-government sebagai upaya peningkatan kualitas pelayanan publik. *JIANA (Jurnal Ilmu Administrasi Negara)*, 10(1), 89–100).