Information Technology Security Audit at the YDSF National Zakat Institution Using the ISO 27001 Framework

Mustafa Kamal [1*], Muhamad Nasrullah [2], Yupit Sudianto [3], Rully Rosadi [4], Muhammad Arkan Fauzan [5], Yuvens Anggito [6], Wahid Yasin [7], Hendrik Hermawan [8]

Information Technology and Business Faculty [1], [2], [3], [4], [5], [6], [7], [8]
Institut Teknologi Telkom Surabaya, Surabaya, Indonesia
mustafakamal@ittelkom-sby.ac.id [1*], emnasrul@ittelkom-sby.ac.id [2], yupit@ittelkom-sby.ac.id [3], rosadirully5@gmail.com [4], arkanfauzan84@gmail.com [5], yuvens112@gmail.com [6], wahid.yasin45@gmail.com [7], hendrikprima97@gmail.com [8]

***Abstract*— In this era of cyber crimes, data security is an important aspect that needs special attention from an organization. This is reinforced by the ratification of Law Number 27 of 2022 on personal data security. The National Zakat Amil Institute (LAZNAS) Yayasan Dana Sosial al Falah (YDSF) as an institution with a legal entity and having data on more than 100,000 donors and partners, it also has an obligation to protect the personal data of donors and partners. The focus of this research is to evaluate and audit information technology at the LAZNAS YDSF, especially regarding the security aspect of information technology. Evaluations and audits were carried out using the ISO 27001 framework as a standardization of information technology security at the international level. In this study, information technology audits were conducted using quantitative methods. The assessment was carried out on seven main clauses that are priorities for the LAZNAS YDSF based on management priorities: compliance clauses, risk management, policies, assets, physical and environmental management, access control, and incident management. Data were collected using a questionnaire distributed to all the LAZNAS YDSF managers and employees. Fifty-five respondents, ranging from management to staff, were involved in filling out the questionnaire, ranging from management to staff. Based on the recapitulation of answers from respondents, it was found that the risk management and access control clauses had good results, with scores of 2,727 and 2,796. The compliance and incident management clauses have scores of 2.381 and 2.53, respectively; therefore, improvement efforts need to be made. By evaluating and auditing information technology that refers to the ISO 27001 standard, it is hoped that LAZNAS YDSF can protect and maintain the confidentiality, integrity, and availability of information, and manage and control information security risks.**

Keywords*— *Data Security, Information Technology Audit, Information Technologi Governance, ISO 27001, National Zakat Amil Institute

I. INTRODUCTION

Industrial revolution 4.0 is an era that combines cyber technology and automation technology. In the era of Industry 4.0, there has been an increase in the use of information technology in various fields. An increase in the use of information technology is accompanied by an increase in the number of cybercrime cases. Cybercrime can attack anyone on the Internet, without exception. Information security evaluations and audits are very necessary in order to be able to provide measurements and evaluations of the readiness of an organization and institution in aspects of information technology security [1]. An overview of information technology security readiness is useful for mapping the conditions of information technology and the information systems of an organization and institution. Organizations and institutions that already have a complete picture of technology and information readiness will be able to organize and manage information technology better because, according to Saleh et al. An information technology service can work optimally only if it has reliable infrastructure [2].

Good information technology management and information systems will be a strong foundation for dealing with various types of security threats to an organization's information assets [3]. The information assets in the LAZNAS YDSF include more than 100,000 donors and partners. The security of donor and partner data concerning personal data security is strengthened by Law Number 27 of 2022 [4]. Donor and partner data are a very important responsibility for LAZNAS because they influence aspects of donor trust. A high level of security can make donors feel more secure about the assets entrusted with LAZNAS.

The ISO 27001 standard is a framework standard used to measure or audit the level of information security (cybersecurity) [5]. This standard helps an organization secure organizational assets and protects its information security management system [6]. An organization that is connected to the Internet will definitely be affected by the Industrial Revolution 4.0; therefore, in protecting systems and networks in the organization, it is best to implement cyber security hardening or strengthen the security of networks and systems in the organization [7]. Network security is strengthened by the rise of cyber attacks, recorded in Indonesia at the end of 2020, and there were 495 million cyber attacks [8].

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v13i1.1987, Copyright ©2024
Submitted : October 13, 2023, Revised : December 20, 2023, Accepted : January 5, 2024, Published : February 15, 2024

LAZNAS YDSF has never conducted an audit or evaluation of its information system or information technology, therefore the research team intends to conduct an audit or evaluation of the information system owned by LAZNAS because of this information technology audit and evaluation research.

II. LITERATURE REVIEW

ISO 27001 is an international standard in the field of information technology that provides a framework for managing information security in an organization. This standard identifies various requirements that an organization must meet to maintain the confidentiality, integrity, and availability of the information they manage. ISO 27001 also provides guidance on how to identify information security risks, implement appropriate controls, and monitor and review the existing information security systems. By adopting ISO 27001, organizations can increase their level of information security and minimize the risk of information loss or misuse.

The ISO 27001 standard has three principles of information security, also known as the CIA triad: confidentiality, information integrity, and data availability. Confidentiality means that only the right people can access the information held by the organization. Information integrity means that the data an organization uses to run its business or stores safely for others are stored reliably and are not deleted or damaged. Data availability means that organizations and their clients can access information whenever needed to meet business goals and customer expectations. Organizations and institutions with an information security management system that meets the requirements of ISO 27001 will maintain the confidentiality, integrity, and availability of information by implementing various risk management processes and providing confidence to interested parties that risks will be adequately managed [9]. The confidentiality, integrity, and availability of information security depicted in a triangle in Figure 1.

FIGURE 1. CIA TRIAD OF INFORMATION SECURITY

Previous research on audits using the ISO 27001 framework is unique. In [10], the aim was to audit security in e-cash applications using several clauses proposed by ISO. The selection of clauses is based on the problems found during problem identification; therefore, not all clauses were used in this research. The assessment in this research uses maturity levels from level 0, namely "None," to level 5, namely "Optimized." The depiction of the results of data analysis using maturity levels for the answers to this questionnaire can be said to be good enough to be sufficient to draw appropriate conclusions and suggestions; this research was conducted at a relatively large company, namely, one of the private banks located in Indonesia [11].

Another study contains information system security audits at the xyz service in Lampung province using the ISO/IEC 27001:2013 standard. This study [11] aims to audit LAZNAS YDSF services using the 13 clauses proposed by ISO 27001. This research also carries out a Strength, Weakness, Opportunity, Threat (SWOT) analysis, which aims to find out more deeply about the systematic factors in company/related services. The assessment of the results of respondents in this study used a maturity level on a scale of 0–5. The assessment of this company/department results in some aspects having weaknesses, and some aspects having more strengths; therefore, at the end of this journal, the author provides recommendations for aspects that are felt less than expectations, namely a scale of 5 [11].

Other studies have several techniques that can be used, namely the use of maturity levels, which are useful as a solution to ensure the level of reliability of internal auditors in achieving success with company performance, one of which is measured by its performance [12]. The maturity level used may be different in terms of scale because we did not want to have a relatively neutral scale of 3, so we used a scale of 1-4. This use is adjusted to the company through an interview process to obtain correct audit results [10].

An information security management system that meets the requirements of ISO 27001 maintains the confidentiality, integrity, and availability of information by implementing a risk management process and providing confidence to interested parties that risks are being managed adequately. In the ISO 20071 standardization, there are twelve components: risk management, policy, organization, asset management, HR security, physical environment, communication and operational management, access control, software development, incident management, business continuity, and compliance. The 12 clauses in ISO 27001 are illustrated in Figure 2 [9].

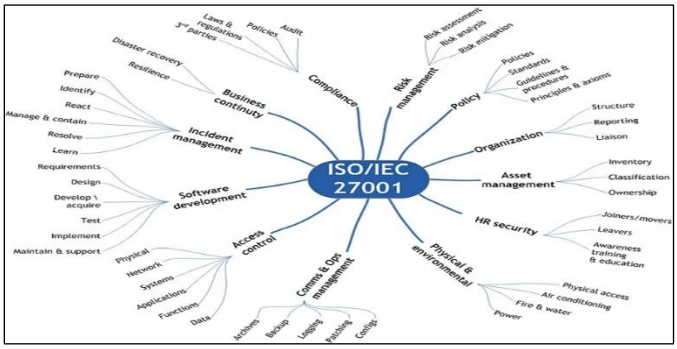

FIGURE 2. ISO 27001:2013 CLAUSES

This study used several clauses provided in the ISO 27001

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v13i1.1987, Copyright ©2024
Submitted : October 13, 2023, Revised : December 20, 2023, Accepted : January 5, 2024, Published : February 15, 2024

standard. Based on observations of analysis funds, as well as the strategies and priorities of LAZNAS YDSF management, this research focuses on seven main clauses. The seven clauses included compliance clauses, risk management clauses, policy clauses, asset management clauses, physical and environmental clauses, access control clauses, and incident management clauses. The clauses proposed in this study were obtained from the process of identifying problems with partners. The proposed clauses are listed in Table 1.

TABLE 1 RESEARCH CLAUSES

No	Description
1	Compliance
2	Risk Management
3	Policy
4	Asset Management
5	Physical and environment
6	Access Control
7	Incident Management

III. RESEARCH METHOD

This research was carried out in several stages, starting from a literature study, problem identification, selection of research aspects/clauses, creation of research tools, data collection, data analysis, evaluation, and recommendations for information security governance. The problem identification stage and selection of research aspects/clauses were carried out by conducting discussions and observations with LAZNAS YDSF management. The selection of research aspects/clauses is based on aspects that are the management's main priority regarding the institution's information technology governance. The complete research stages of the research method flow diagram are shown in Figure 3.

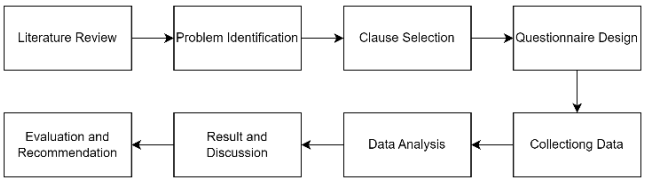

FIGURE 3. RESEARCH METHOD FLOW DIAGRAM

The data collection and analysis method used in this research is a quantitative method that aims to obtain data to assess the maturity level of the LAZNAS YDSF in its information security management [13].

Data were collected using a questionnaire. A questionnaire collects data or information through forms containing questions that will be filled in by several respondents to obtain responses that will be analyzed [14]. The questionnaire was prepared based on the clauses used, while one of the response category scales was shown on a Likert scale with values from one to four. This Likert category scale describes the responses to the questions given to the respondents, as shown in Table 2.

TABLE 2. RESEARCH RESPONDENT COMPLETION SCALE

Scale	Description
1.	Are not done
2.	In planning
3.	Partially implemented
4.	Implemented thoroughly

IV. RESULTS AND DISCUSSION

This information technology security audit research resulted in several assessments, such as the data obtained using a questionnaire, resulting in patterns that can be used as a basis for how information security is managed at LAZNAS YDSF information considered good in access control and risk management clauses. Meanwhile, the clause with the lowest score, which means that information security governance is deemed to need improvement, is in compliance with incident management clauses. The clauses with the highest evaluation score results in more detail are shown in table 3 and table 4, and the clauses with evaluation score results that need to be improved are in Table 5 and Table 6.

TABLE 3. ACCESS CONTROL EVALUATION RESULT

Clause	Attribute	Question	Score	Total Score
Access Control	Physical	Has the Institution implemented security for physical facilities in accordance with the interests of information assets in layers and can deter unauthorized parties?	2.6	2.796
	Network	Does the Institution have a mechanism to verify and validate users who enter the internal network?	2.909	
	Systems	How effective is the use of authentication and authorization systems to control user access to the system in accordance with established policies?	2.836	
	Applications	How effectively is the application monitoring and	2.727	

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v13i1.1987, Copyright ©2024
Submitted : October 13, 2023, Revised : December 20, 2023, Accepted : January 5, 2024, Published : February 15, 2024

		logging system implemented to ensure that all user activity on the application can be tracked and monitored?		
	Functions	Does your organization have appropriate access controls in place to manage and limit user access to the Institution's IT system functions?	2.872	
	Data	Does the Institution have appropriate access controls in place to manage and limit user access to sensitive data?	2.836	

The access control aspect has an average value of 2.8, which indicates that there are attributes AC1 (physical) with a value of 2.6, and AC4 (applications) with a value of 2.7, which still do not meet the average value stated. The access control aspect has, for attributes AC2 (network), AC3 (system), AC5 (functions), and AC6 (data), which is quite good but can be improved again. The results of the access control are shown in the spider chart in Figure. 4.

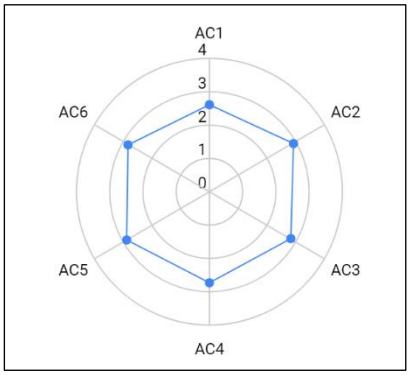

FIGURE 4. ACCESS CONTROL ASPECT RESULTS SPIDER CHART

TABLE 4. RISK MANAGEMENT EVALUATION RESULT

Clause	Attribute	Question	Score	Total Score
Risk Management	Risk Assesment	Does the Institution know the risks that may occur in information security?	2.763	2.727
	Risk Analysis	Has the Institution carried out a proper analysis to understand threats and vulnerabilities in the information security aspect?	2.69	
	Risk Mitigations	How effective are the risk mitigation steps taken by the IT department in reducing the impact of information security threats, such as data backup, disaster recovery, and network security monitoring?	2.727	

The risk management aspect with risk management (RM1) obtains a value above the average, followed by risk mitigation (RM3), which is in line with the average. The risk analysis value (RM2) is below average. The three attributes above still require quality improvement so that the resulting value is better. The results of risk management are depicted in the spider chart in Figure 5.

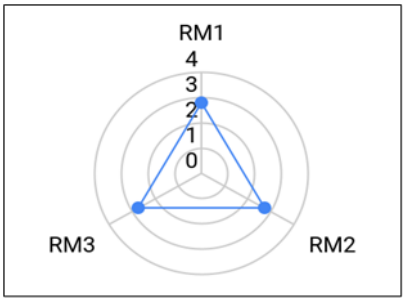

FIGURE 5. RISK MANAGEMENT ASPECT RESULTS SPIDER CHART

TABLE 5. COMPLIANCE EVALUATION RESULT

Clause	Attribute	Question	Score	Total Score
Compliance	Audit	Does the Institution have clear and documented Information Technology (IT) Audit procedures in its activities?	2.272	2.381
	Policies	Is there an information security policy, approved by	2.418	

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v13i1.1987, Copyright ©2024
Submitted : October 13, 2023, Revised : December 20, 2023, Accepted : January 5, 2024, Published : February 15, 2024

		management, published and properly communicated to all employees.		
	Laws & Regulations	Has the Institution implemented appropriate sanctions if employees violate established regulations and policies?	2.363	
	3rd Parties	Are there steps to ensure that IT security controls, description of IT services, and achievement of IT objectives, are implemented, operated, and maintained by third parties (vendors).	2.472	

The compliance aspect with the results of the policy (P1) and 3rd parties (P4) attributes is quite good because it is above the average compliance point aspect of 2.381. However, several aspects are still lacking and need to be improved, namely audit (P1) and laws and regulations (P3), because these two aspects are still below the average for compliance. The compliance results are depicted in the spider chart diagram in Figure 6.

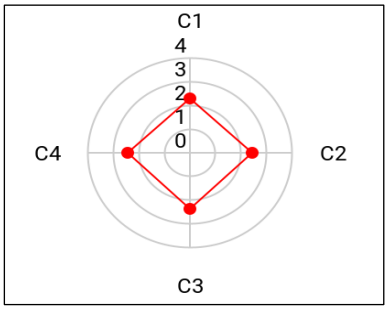

FIGURE 6. COMPLIANCE ASPECT RESULTS SPIDER CHART

TABLE 6. INCIDENT MANAGEMENT EVALUATION RESULT

Clause	Attribute	Question	Score	Total Score
Incident Management	Prepare	How often is the IT incident/problem handling plan updated to ensure consistency and readiness in dealing with IT incidents/problems that may occur?	2.418	2.53
	Identify	Does the Institution have standards to detect that something can be said to be an incident/problem?	2.436	
	React	Has the institution prepared an emergency response system for its employees regarding incidents?	2.636	
	Manage & Contain	Does the Agency limit or isolate incidents to prevent their spread?	2.636	
	Resolve	Does the Institution have procedures for system recovery related to incidents that occur?	2.8	
	Learn	How often are the results of security incidents/issues studied and shared with the IT staff and users involved?	2.254	

The incident management aspect had an average value of 2.5, and there were attributes IM1 (prepare) with a value of 2.4, IM2 (identify) with a value of 2.4, and IM6 (learn) with a value of 2.2. These values are below the Incident Management aspect value for the IM3 (react), IM4 (manage and contain), and IM5 (resolve) attributes, which are good but can be improved again. The results of incident management are depicted in the spider chart in Figure 7.

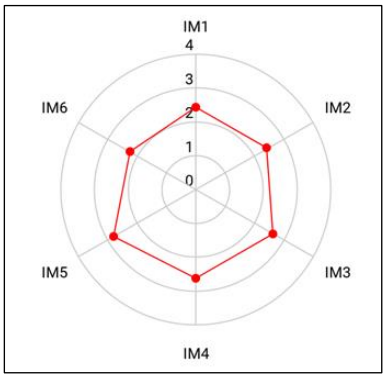

FIGURE 7. INCIDENT MANAGEMENT ASPECT RESULTS SPIDER CHART

Furthermore, from the evaluation results of each clause, the results are mapped and analyzed in the form of a spider chart, namely, a spider-shaped or hexagonal chart. The Spider Chart determines the strengths and weaknesses that can be observed from the evaluation results of each research clause [15]. This mapping makes it easier to observe the weaknesses and shortcomings of the sectors in the LAZNAS YDSF. The mapping results in the form of a spider chart are shown in Figure 8.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v13i1.1987, Copyright ©2024
Submitted : October 13, 2023, Revised : December 20, 2023, Accepted : January 5, 2024, Published : February 15, 2024

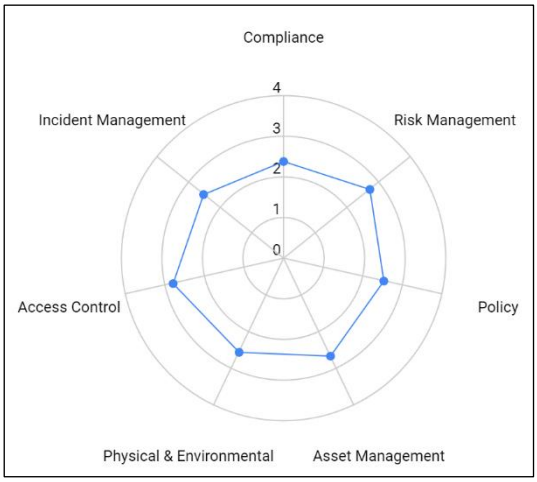

FIGURE 8. OVERALL EVALUATION RESULTS SPIDER CHART

V. CONLUSION

IT/SI Audit research on LAZNAS YDSF illustrates that on the LAZNAS YDSF scale, LAZNAS and the clause that needs improvement are the compliance clause and incident management clause. This lack of achievement in the compliance clause is due to a lack of compliance with LAZNAS. The compliance clause poses the threat of data breach and business continuity [16], which will affect business continuity if this is not addressed immediately. Therefore, enhancing employee training and awareness programs for information security, and improving incident response and recovery procedures are recommended. Updating and maintaining the documentation of information security policies and procedures.

ACKNOWLEDGEMENT

In this community service activity, we received significant help from various parties. We thank the Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) for their support in this community service activity, and the executive director of LAZNAS YDSF, who has given permission, to the management and employees of LAZNAS who directly or indirectly contribute to community service activities.

REFERENCES

[1] T. Rochmadi and Ike Yunia Pasa, "PENGUKURAN RISIKO DAN EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI DI BKD XYZ BERDASARKAN ISO 27001 / SNI," Cyber Security dan Forensik Digital, vol. 4, no. 1, pp. 38–43, Jun. 2021, doi: 10.14421/csecurity.2021.4.1.2439.

[2] M. Saleh, I. Yusuf, and H. Sujaini, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," Jurnal Edukasi dan Penelitian Informatika (JEPIN), vol. 7, no. 2, 2021, doi: 10.26418/jp.v7i2.48228.

[3] A. Saputra and Y. G. Sucahyo, "Rancangan Tata Kelola Organisasi Sistem Manajemen Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten Bekasi Organization Governance Design of Information Security Management System Bekasi Communications and Information Technology Agency," 2018.

[4] CSA Teddy Lesmana, E. Elis, and S. Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia, vol. 3, no. 2, 2022, doi: 10.52005/rechten.v3i2.78.

[5] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," International Journal on Informatics Visualization, vol. 4, no. 4, 2020, doi: 10.30630/joiv.4.4.482.

[6] P. Edo Rizky, Suprapto, and A.. Perdanakusuma, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 2, no. 11, pp. 5911–5920, 2018, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465

[7] S. Syafie, "Kesiapan Teknologi Informasi Perbankan hadapi Revolusi Industri era 4.0," JATISI (Jurnal Teknik Informatika dan Sistem Informasi), vol. 9, no. 1, 2022, doi: 10.35957/jatisi.v9i1.1540.

[8] "BSSN: Malware Trojan Dominasi Serangan Siber di 2020 -Tempo.co."

[9] R. Sheikhpour and N. Modiri, "An approach to map COBIT processes to ISO/IEC 27001 information security management controls," International Journal of Security and its Applications, vol. 6, no. 2, 2012.

[10] P. Paradise, K. Kusrini, and A. Nasiri, "Audit Keamanan Aplikasi E-Cash Menggunakan Iso 27001," Creative Information Technology Journal, vol. 5, no. 4, 2020, doi: 10.24076/citec.2018v5i4.209.

[11] A. Meyliana, T. Tristiyanto, and R. Prabowo, "AUDIT KEAMANAN SISTEM INFORMASI DI DINAS XYZ PROVINSI LAMPUNG MENGGUNAKAN STANDAR ISO/IEC 27001:2013," Jurnal Pepadun, vol. 1, no. 1, 2020, doi: 10.23960/pepadun.v1i1.16.

[12] Monang Nixon Haposan Tampubolon, "Manajemen Risiko, Internal Kontrol, Tata Kelola Perusahaan dan Kinerja Keuangan BUMN dengan Maturity Level Departemen Audit Internal sebagai Pemoderasi," Jurnal Riset Akuntansi & Perpajakan (JRAP), vol. 6, no. 02, 2019, doi: 10.35838/jrap.v6i02.1247.

[13] Pitrawati and I. Agus, "Audit Sistem Informasi pada AMIK Dian Cipta Cendekia Bandar Lampung," Jurnal Jupiter, vol. 10, no. Snati, pp. 83–92, 2018.

[14] K. N. Cahyo, Martini, and E. Riana, "Perancangan Sistem Informasi Pengelolaan Kuesioner Pelatihan pada PT Brainmatics Cipta Informatika," Journal of Information System Research (JOSH), vol. 1, no. 1, 2019.

[15] F. Rosique, P. J. Navarro, C. Fernández, A. Padilla, "A systematic review of perception system and simulators for autonomous vehicles research," Sensors (Switzerland), vol. 19, no. 3. 2019. doi: 10.3390/s19030648.

[16] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, "Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools," Risks, vol. 10, no. 8, 2022, doi: 10.3390/risks10080165.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v13i1.1987, Copyright ©2024
Submitted : October 13, 2023, Revised : December 20, 2023, Accepted : January 5, 2024, Published : February 15, 2024