International Journal of Cyber and IT Service Management (IJCITSM) p-ISSN: 2797-1325
Vol. 3 No. 2 October 2023 e-ISSN: 2808-554X

Transforming PT Pertamina with Cybersecurity, File Security, and Essential Items

Rama Azhari[1], Agita Nisa Salsabila[2]
Departement of Engineering Business Management, Singapore Institute of Management
461 Clementi Rd, Singapore 599491
Singapore
e-mail: ramaazhari25@yahoo.com[1], agitanisasalsabila@gmail.com[2]

Author Notification
13 October 2023
Final Revised
29 October 2023
Published
31 October 2023

To cite this document:
Azhari, R. ., & Salsabila, A. N. (2023). Transforming PT Pertamina with Cybersecurity, File Security, and Essential Items. *International Journal of Cyber and IT Service Management, 3(2), 160–167. Retrieved from https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/140*

DOI:
https://doi.org/10.34306/ijcitsm.v3i2.140

Abstract

Considering the threat posed by cyberattacks, terrorist acts, and security breaches, it is imperative to implement an effective security policy to safeguard important items. Cybersecurity is yet another important topic covered in this study. PT Pertamina is a company that relies heavily on computer networks and information technology. Cyberattack defense and computer system security are critical components of PT Pertamina's operating performance. Consequently, to stop cyberattacks, data theft, and the leakage of private information, an efficient cyber security plan must be put into place. This paper also focuses on file security. Financial data, customer information, and contract agreements are just a few of the crucial items that PT Pertamina maintains and keeps track of. It is essential to protect these files to stop illegal access, data theft, and other threats to the business's operations. This essay will examine many tactics and approaches that PT Pertamina might use to implement file security, cyber security, and vital objects. It is hoped that this paper will act as a guide for PT Pertamina and other similar businesses in safeguarding their valuable assets against security-related internal and external threats.

Keywords*: Cybersecurity, Transforming, File Security, Essential Items*

1. Introduction

The national energy company of Indonesia, PT Pertamina, is involved in the discovery, production, and distribution of energy resources [1]. Being one of the biggest sectors in Indonesia, Pertamina has a significant obligation to safeguard the long-term viability of its business, safeguard confidential data, and combat security risks that persist in the current digital world [2]. Although the development of data and communications technology benefits businesses such as Pertamina, it also poses new security challenges [3]. PT Pertamina faces genuine dangers from cyber security threats like sabotage, information theft, and hacker assaults [4]. Industrial operations rely heavily on Pertamina's essential assets, including data systems, network infrastructure, and production facilities [5].

This essential object's destruction or obstruction might have a major impact on the nation's economy, the ability to run its industries, and the continuity of its energy supply [6]. Furthermore, PT Pertamina possesses important data and information that needs to be appropriately safeguarded [7]. Confidential information on production processes, energy reserves, the financial sector, and personal employee information needs to be shielded from

prying eyes. For PT Pertamina to overcome this obstacle, putting in place effective file security and cyber security is crucial. To safeguard data systems, critical industrial information, and IT infrastructure, comprehensive plans and actions must be implemented [8]. Strict security regulations, the application of cutting-edge security technologies, and security awareness and training for all involved staff members are some of these measures [9]. PT Pertamina (Persero) stated in relation to the strike plan filed by the United Pertamina Workers Union Forum (FSPBB) that providing residents with services and fuel and LPG needs will always be the industry's top priority [10]. "All employees who are in charge of carrying out the government's responsibility to guarantee national energy security are included in Pertamina as a BUMN. Employees are also at the forefront of meeting the demands of the public and completing government assignments to supply LPG and fuel in remote 3T areas so that people can go about their daily lives as usual [11].

Additionally "We need to keep pushing the wheels of the national economy forward because Indonesia is currently struggling to recover from the Covid-19 pandemic," VP of Corporate Communication Pertamina Fajriyah Usman said [12]. Both those who live close to the PT Pertamina Refinery and all Indramayu inhabitants would undoubtedly benefit from the establishment of the Balongan Refinery. The oil refinery owned by Pertamina is a strategically important source of national income in addition to being a critical national asset that serves the interests of the nation and the lives of many people [13]. Information technology (IT)-related industries consider the security of electronic data to be critical infrastructure. thus data or information is a valuable resource for the sector. PERTAMINA is focused on implementing a best-in-class Security Management System based on risk management in order to achieve security and energy sovereignty [14]. PERTAMINA Security Risk Management is the foundation for security management attempts. The purpose of this study is to examine and evaluate PT Pertamina's use of vital objects, file security, and cyber security [15]. The role of crucial items in preserving Pertamina's operations, cyber security difficulties encountered, and actions and tactics that may be put in place to reduce security threats and safeguard industrial information and data systems will all be covered in this study. In addition to offering pertinent recommendations for boosting security and industrial resilience against security risks that are only going to get worse in the digital age, it is intended that this article will be able to give PT Pertamina a thorough explanation of what file security and cyber security entail [16].

2. Research Method

This study falls under the category of qualitative research and library studies. examining ideas and connections to or affects on variables using books and journals, either online using Mendeley, Google Scholar, and other online resources, or offline at the Park Library [17]. It is anticipated that a qualitative method will yield a comprehensive account of speech, writing, and behavior that is appealing to people, groups in the community, and a specific organization within a certain context that is examined from every viewpoint [18].

2.1 Literature Review

Organizations, especially those in vital sectors like energy and petroleum, are increasingly vulnerable to cyberattacks in today's digitally connected world [19]. The importance of PT Pertamina, the state-owned oil and gas firm in Indonesia, to the nation's economic stability makes extensive cybersecurity measures imperative. This review of the literature explores the crucial elements of integrating cybersecurity, file security, and necessities into PT Pertamina [20].

a. The Cybersecurity Imperative

It is vital to safeguard PT Pertamina's sensitive data and vital infrastructure. Given the always changing threat landscape, cybersecurity needs to be resilient, proactive, and flexible. Protecting against sophisticated cyber threats requires utilizing state-of-the-art technologies like firewalls, intrusion detection systems, and threat intelligence exchange [21].

b. File Security and Data Governance

PT Pertamina needs to give these two areas top priority because it has access to a lot of sensitive data. Strict access controls, encryption methods, and data classification guidelines ensure that only individuals with the proper authorization can access sensitive data, lowering the possibility of data breaches [22].

c. Supply Chain Resilience

PT Pertamina's primary responsibilities include the distribution and acquisition of necessities, such as oil and gas products. It is crucial to make sure that the supply chain is resilient, especially during emergencies or other disruptive events. Adopting cutting-edge technology like blockchain and Internet of Things sensors can improve supply chain security, traceability, and transparency [23].

d. Human Factors and Training

Human factor plays an equally important role in cybersecurity as does technology. Workers at PT Pertamina must be knowledgeable about industry best practices and conscious of the dangers posed by online attacks. Frequent awareness and training campaigns can greatly strengthen the organization's defenses [24].

e. Adherence to Regulations

For PT Pertamina to undergo a change, compliance with pertinent cybersecurity and data protection standards is essential. For legal and reputational reasons, compliance with frameworks such as NIST, ISO 27001, and local requirements in Indonesia is imperative [25].

f. Working together and exchanging information

Staying ahead of developing cyber dangers can be achieved by exchanging threat intelligence and working together with government agencies and industry peers. PT Pertamina and the energy industry as a whole stand to gain from forming alliances within the sector that can result in collective defensive mechanisms [26].

This assessment of the literature highlights the diverse strategy required to make PT Pertamina a secure and resilient organization. PT Pertamina can enhance the security of its important operations and sustain its crucial position in the Indonesian economy by adopting state-of-the-art cybersecurity techniques, putting in place strong file security measures, and guaranteeing the integrity of its supply chain for essential commodities [27].

3. Findings

3.1 Essential Items

According to Presidential Decree No. 63 of 2004, essential objects A national is a region, position, building, installation, and/or business that affects a large number of people's livelihoods, the national interest, and/or a vital source of state revenue [28]. Recall that because of its highly strategic function, protecting important national assets necessitates a system that is both stricter and more robust than the current one, with tight security standards to reduce risks and security consequences brought on by threats and security limitations. A military strategist named Carl (1801) claims that crucial objects are targets with great strategic importance that, if successfully comprehended by the adversary, might yield substantial strategic advantages [29]. This can include vital infrastructure, command and control facilities, strategic locations, renewable energy sources, and so forth. Targets that a nation needs to defend to maintain its integrity, sovereignty, and existence are known as vital objects, according to the National Security Doctrine. In this perspective, border regions, strategically important military installations, vital infrastructure (e.g., power plants and telecommunications hubs), energy sources, and so on, can all be considered vital objects [30].

3.2 File Security

Information security, in the words of G.J. Simons, is the means by which we may prevent fraud (cheating) in data-based systems where the data itself lacks physical meaning, or at the very least, identify that fraud exists. Gollmann (1999) asserts that self-deterrence and the identification of disruptive acts that the computer system is unable to detect are related to file security. File security, according to Mulyana (2016), is the process of thwarting attacks by users' careless network access or files.

3.3 Internet Safety

From a political standpoint, cyber security is a response to contemporary hazards and threats faced by the worldwide data technology infrastructure, commonly referred to as "the internet" (Stevens, 2016). Prabuningtyas (2018) claims that cyber security is a type of modified security that pertains to anything that is owned and needs to be secured in cyberspace. Alan (2020) asserts that cyber security is a subset of data security and shares similarities with data security. While data security adopts a universal strategy, cyber security concentrates on adopting a specific approach to electronic data, including the physical aspects of data maintenance.

3.4 Vital Objects Implementation at PT. Pertamina

Taken from Presidential Decree Number 63 of 2004 (Kepres). The object of national vitality (Obvitnas) that Pertamina operates in is the energy infrastructure, and it must be free from dangers and impediments. The Pertamina Balongan Refinery in Indramayu Regency has a highly crucial position towards the wheel of the Indonesian economy because it is a National Vital Object (Obvitnas). This is because the Balongan Refinery supplies the majority of the fuel oil (BBM) required by Bunda City (Jakarta) and its environs, including West Java and Banten. Not only does its location matter on a national scale, but the Balongan Refinery's presence Naturally will also have a favorable effect on people who live in Indramayu generally and in close proximity to PT Kilang Pertamina. Harry views Pertamina's oil refinery as a strategically important source of state revenue and a critical national asset for meeting the requirements of many people and the nation's interests. Pertamina also owns and operates oil refineries, which it uses to supply petroleum to Indonesian nationals. There's little doubt that the Balongan Refinery's presence will benefit all Indramayu locals as well as those who live close to PT. The Pertamina International (KPI) Refinery Unit VI Balongan refinery is the most significant in terms of the economic impact multiplier. Because of this, everyone in society needs to defend the Balongan refinery's existence to fulfill their obligations. The nation's electricity supply is still being carried out without any issues or roadblocks.

3.5 PT. Pertamina's Cybersecurity

PERTAMINA concentrates on implementing best-in-class Security Management System based risk management in order to achieve energy security and sovereignty. The foundation of security management is PERTAMINA Security Risk Management (PSRM). PRSM manages the processes involved in creating risk profiles, keeping an eye on security threats, mitigating implementation risks, and updating the security risk register. Decisions made by PSRM in all PERTAMINA organizational domains are founded on risk management concepts. PERTAMINA pledged to continuously enhance transaction security, cyber security, and other digital security in keeping with the digital transformation. When it comes to the use of electronic signatures, PERTAMINA and two universities have partnered with Electronic Certificate Organizers (PSE). This application is limited to the issue of invoices from Holding's core ERP system or the electronic document signing of external correspondence by paraworkers at PERTAMINA. Given the significance of the data and infrastructure they manage, cyber security is an important concern for organizations such as PT Pertamina. PT Pertamina may encounter the following issues with cyber security:

1. Attack Threat: A variety of entities, including hackers, criminal organizations, and even foreign nations, may launch attacks against PT Pertamina. Malware, DDoS (Distributed Denial of Service) assaults, phishing attacks, and other attacks with the intent to steal

data or compromise the system are all considered forms of attacks.

2. Limited Resources: A substantial investment in infrastructure, technology, and human resources is needed for cyber security. Building and keeping a skilled security team may prove to be difficult for PT Pertamina due to a lack of internal resources. Object Implementation...., Soesanto et al., IJM: Indonesian Journal of Multidisciplinary Volume 1 Number 1 Year 2023 101 put in place the technology required to protect their systems and networks.
3. Vulnerable Supply Chain: PT Pertamina's supply chains may be subject to intrusions. Attacks on suppliers or business partners could give PT Pertamina's systems illegal access, necessitating careful security oversight throughout their whole supply chain.
4. Data and Information Security: Vital data and information, including customer details, technological blueprints, and financial data, are stored by PT Pertamina. It is critical to safeguard sensitive data from cyber threats in order to uphold consumer confidence, stop data breaches, and prevent monetary losses.
5. Non-Compliance with Safety Standards: PT Pertamina Possible is obliged to abide by a number of security standards, including ISO 27001, which are established by the government and business community.

Failure to adhere to these guidelines may lead to penalties, a decline in customer trust, or breaches of personal information. PT Pertamina may use the subsequent strategy to get around This issue arises:

1. Make a Security Team Investment: Hire and develop a solid security staff with the knowledge and expertise to recognize, stop, and handle cyberattacks.
2. Put in Place a Robust Security System: To defend networks and systems from threats, install and maintain system security measures including firewalls, antivirus software, antispyware, and intrusion detection systems (IDS/IPS).
3. User Awareness: Provide PT Pertamina staff with frequent cyber security training so they can identify and report phishing scams and other hacking attempts.
4. Active Security Monitoring: To enable prompt action, engage in ongoing active security monitoring to identify intrusions or questionable activities.
5. Creating Backups and Restores

3.6 Data Protection at PT. Pertamamina

Security of electronic data is crucial for businesses who employ IT facilities and consider them essential infrastructure. Since information or data is a valuable resource for the business. The following are PERTAMINA's information system security controls:

1. The purpose of the security policy, often known as the "security police," is to guide content and mission management in order to preserve the integrity of critical firm data and ensure the organization's continuity.
2. Access control for the system (System Access Control). The authority to restrict or regulate user access to information, including telenetworking and mobile computing. Control protocols for resource and information access Existing power encompasses a number of elements, including:
    a. Access control business requirements.
    b. User access control, sometimes known as UAC.
    c. Awareness of information security (user responsibilities).
    d. Use network access control (NAC) to manage network access.
    e. Use Operating System Access Control to restrict access to the operating system.
    f. Application Access Management (Application Access).
    g. Monitoring System Access and Use (Supervision of System Access and Use). Telenetworking and mobile computing
    h. System development and maintenance, making sure that the system functions and that, via validation and verification, newly implemented applications can work together harmoniously.

3. Physical and environmental security, which guards against data loss or damage brought on by natural disasters and other physical environmental factors, as well as declines in data held on storage media or in other information storage facilities.
4. Adjustment, making sure that, through routine system audits, security policy implementation complies with all relevant laws, rules, and agreements, including contracts.
5. Security for HR or personnel. attempts to lessen the possibility of misuse of power and function as a result of user error, data manipulation in operations and applications. Activities included information awareness training, which enables all users to preserve the confidentiality of data and information in the workplace for one another.
6. Security organizations, which uphold an agency's or organization's worldwide information security, preserve and safeguard the accuracy of system information processed by outside parties, including control over such processing.

For a business, like PT Pertamina, file security is crucial to safeguarding critical information and sensitive data. There are several issues that could come up with PT Pertamina file security and Among the options for solutions are the following:

1. Unauthorized access: Unauthorized parties gaining access to files is a typical issue related to file security. Subject: This may occur due to inadequate security measures, easily cracked passwords, or improper device security by users. Strict security guidelines, such as the requirement for strong passwords and frequent password changes, should be put into place as a solution. makes use of two-factor authentication (2FA) to protect system and file access. Keep an eye on file usage and access on a regular basis to spot unusual activities.
2. Malware assaults: The PT Pertamina system and file integrity may be jeopardized by malware attacks like viruses, ransomware, or other dangerous software. Using software with cutting-edge security, constant updating, and malware assault monitoring is the answer. Update software and the system on a regular basis to address vulnerabilities that are discovered. Provide Pertamina, the PT staff, with security training so they can identify and stay away from malware dangers like phishing and dubious connections.
3. Device theft or loss: If the device has PT files on it The loss or theft of Pertamina could expose private firm information to unapproved access. Solution a: Encrypt files and devices that hold private data. a. Turn on the compatible device's remote tracking and wiping capabilities. c. Inform staff members on physical security procedures, like watching over their device and not leaving it unattended for extended periods of time.
4. Limited accessibility and collaboration: Although file security is crucial, there are occasions when it can impede accessibility and teamwork at PT Pertamina. Using a security system that enables flexible file permission and access level setting is the solution. Put in place secure collaboration tools that let users who have been properly authorized share files. The effectiveness of the team is not hampered by the security rules and procedures used at PT Pertamina. It's crucial to keep in mind that every business has different file security requirements. Consequently, it is vital to conduct a risk assessment and confer with IT security specialists in order to devise and execute security tactics that align with PT Pertamina's requirements.

4. Conclusion

This article's goal is to examine and critique PT Pertamina's implementation of critical objects, cyber security, and file security in this context. The importance of key components to Pertamina's operations, the difficulties facing cyber security, and the actions and tactics that can be used to reduce security risks and safeguard the information and data systems sector are all covered in this paper. Maintaining the sustainability of business operations and security at PT Pertamina requires the implementation of critical objects, cyber security, and file security. Strong cyber prevention measures, efficient file and data protection, and effective security policies will

all work to shield PT Pertamina from outside dangers that could harm the business and its clients. PT Pertamina can increase confidence among community stakeholders and deal with potential security issues down the road. It is hoped that this article will provide a detailed explanation of what cyber security and file security mean to PT Pertamina, as well as pertinent recommendations to strengthen security and increase industrial resistance to security risks that are only going to get worse in the digital age.

References

[1] B. P. K. Bintoro, N. Lutfiani, and D. Julianingsih, “Analysis of the Effect of Service Quality on Company Reputation on Purchase Decisions for Professional Recruitment Services,” *APTISI Trans. Manag.*, vol. 7, no. 1, pp. 35–41, 2023.

[2] U. Rahardja, “Meningkatkan Kualitas Sumber Daya Manusia Dengan Sistem Pengembangan Fundamental Agile,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 63–68, 2022.

[3] D. Apriani, T. Ramadhan, and E. Astriyani, “Kerja Lapangan Berbasis Website Untuk Sistem Informasi Manajemen Praktek (Studi Sistem Informasi Program Studi Kasus Merdeka Belajar Kampus Merdeka (MBKM) Universitas Raharja,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 24–29, 2022.

[4] K. D. Nusandari, R. Widayanti, Y. F. Achmad, A. H. Azizah, and N. A. Santoso, “Analisis Kesuksesan Pengguna Tangerang Live menggunakan Information System Success Model (ISSM),” *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 77–88, 2022.

[5] N. Sari, W. A. Gunawan, P. K. Sari, I. Zikri, and A. Syahputra, “Analisis Algoritma Bubble Sort Secara Ascending Dan Descending Serta Implementasinya Dengan Menggunakan Bahasa Pemrograman Java,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 16–23, 2022.

[6] C. S. Bangun and N. A. Santoso, “Inovasi Pengembangan Kartu Ujian Online pada Web Portal dengan Metode Waterfall,” *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 1–8, 2022.

[7] S. Kosasi, U. Rahardja, N. Lutfiani, E. P. Harahap, and S. N. Sari, “Blockchain technology-emerging research themes opportunities in higher education,” in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–8.

[8] H. R. Widarti, N. C. E. Habiddin, A. B. Parlan, A. Ardyansyah, and D. A. Rokhim, “Development website of planning, writing, and publication of scientific articles based on Classroom Action Research (CAR) to increase teacher’s pedagogical competence,” *Improv. Assess. Eval. Strateg. Online Learn.*, pp. 37–43, 2022.

[9] M. Budiarto, S. Maesaroh, M. Hardini, and A. Djajadi, “Future energy using blockchain systems,” in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–9.

[10] U. Rahardja, M. A. Ngad, S. Millah, E. P. Harahap, and Q. Aini, “Blockchain Application in Educational Certificates and Verification Compliant with General Data Protection Regulations,” in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*, 2022, pp. 1–7.

[11] S. Azizah *et al.*, “Quantum Computing and AI: Impacts & Possibilities,” *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 121–138, 2022.

[12] P. Hendriyati, F. Agustin, U. Rahardja, and T. Ramadhan, “Management Information Systems on Integrated Student and Lecturer Data,” *APTISI Trans. Manag.*, vol. 6, no. 1, pp. 1–9, 2022.

[13] M. Wahyudi, V. Meilinda, and A. Khoirunisa, “The Digital Economy ’ s Use of Big Data Technologies and Data Science,” vol. 1, no. 1, pp. 62–70, 2022.

[14] A. S. Bist, B. Rawat, U. Rahardja, Q. Aini, and A. G. Prawiyogi, “An Exhaustive Analysis of Stress on Faculty Members Engaged in Higher Education,” *IAIC Trans. Sustain. Digit. Innov.*, vol. 3, no. 2, pp. 126–135, 2022.

[15] B. Rawat, N. Mehra, A. S. Bist, M. Yusup, and Y. P. A. Sanjaya, “Quantum Computing and AI: Impacts & Possibilities,” *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 202–207, 2022.

[16] D. Rustiana, J. D. Pratama, T. Mudabbir, and M. A. Fahmi, “Adoption Computerized

Certificate Transparency And Confidentiality," *Int. J. Cyber IT Serv. Manag.*, vol. 2, no. 1, pp. 1–10, 2022.

[17] R. Widhawati, A. Khoirunisa, N. P. L. Santoso, and D. Apriliasari, "Secure System Medical Record with Blockchain System: Recchain Framework," in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–8.

[18] M. Saraswati, N. Lutfiani, and T. Ramadhan, "Kolaborasi Integrasi Inkubator Bersama Perguruan Tinggi Sebagai Bentuk Pengabdian Terhadap Masyarakat Dalam Perkembangan Iptek," *ADI Pengabdi. Kpd. Masy.*, vol. 1, no. 2, pp. 23–31, 2021.

[19] D. Zarasky and N. Septiani, "Analisis Faktor Kepuasan dan Minat Penggunaan E-Money Flazz BCA di Kota Tangerang," *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 89–99, 2022.

[20] L. A. Faza, P. M. Agustini, S. Maesaroh, A. C. Purnomo, and E. A. Nabila, "Motives For Purchase of Skin Care Product Users (Phenomenology Study on Women in DKI Jakarta)," *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 139–152, 2022.

[21] E. Retnaningtyas, E. Kartikawati, and D. Nilawati, "erma UPAYA PENINGKATAN PENGETAHUAN IBU HAMIL MELALUI EDUKASI MENGENAI KEBUTUHAN NUTRISI IBU HAMIL," *ADI Pengabdi. Kpd. Masy.*, vol. 2, no. 2, pp. 19–24, 2022.

[22] E. S. Pramono, D. Rudianto, F. Siboro, M. P. A. Baqi, and D. Julianingsih, "Analysis Investor Index Indonesia with Capital Asset Pricing Model (CAPM)," *Aptisi Trans. Technopreneursh.*, vol. 4, no. 1, pp. 36–47, 2022.

[23] D. Apriliasari and B. A. P. Seno, "Inovasi Pemanfaatan Blockchain dalam Meningkatkan Keamanan Kekayaan Intelektual Pendidikan," *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 68–76, 2022.

[24] F. P. Oganda, N. Lutfiani, Q. Aini, U. Rahardja, and A. Faturahman, "Blockchain education smart courses of massive online open course using business model canvas," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–6.

[25] T. Ramadhan, Q. Aini, S. Santoso, A. Badrianto, and R. Supriati, "Analysis of the potential context of Blockchain on the usability of Gamification with Game-Based Learning," *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 1, pp. 84–100, 2021.

[26] F. P. Oganda, "PEMANFAATAN SISTEM IJC (iLearning Journal Center) SEBAGAI MEDIA E-JOURNAL PADA PERGURUAN TINGGI DAN ASOSIASI," *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 11, no. 1, pp. 23–33, 2020.

[27] R. Widayanti, Q. Aini, H. Haryani, N. Lutfiani, and D. Apriliasari, "Decentralized Electronic Vote Based on Blockchain P2P," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.

[28] R. Widayanti, U. Rahardja, F. P. Oganda, M. Hardini, and V. T. Devana, "Students Formative Assessment Framework (Faus) Using the Blockchain," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2021, pp. 1–6.

[29] S. Purnama, U. Rahardja, Q. Aini, A. Khoirunisa, and R. A. Toyibah, "Approaching the Anonymous Deployment of Blockchain-Based Fair Advertising on Vehicle Networks," *3rd Int. Conf. Cybern. Intell. Syst. ICORIS 2021*, 2021, doi: 10.1109/ICORIS52787.2021.9649600.

[30] P. Edastama, N. Lutfiani, U. Rahardja, S. Avionita, and P. A. Sunarya, "Overview of Business Innovation and Research Probability on Blockchain and Introduction to its Exclusive Version," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2021, pp. 1–7.