RISK ASSESSMENT RELATED TO PRIVACY INFORMATION ON ELECTRONIC MONEY SERVER-BASED USING ISO 27001 ISO 27005, ISO 27701

SYIFAURACHMAN[1], ANTONI WIBOWO[2]

[1]Bina Nusantara University, Computer Science, Jakarta, Indonesia

[2] Bina Nusantara University, Computer Science, Jakarta, Indonesia

E-mail: [1]syifaurachman@binus.ac.id, [2]anwibowo@binus.edu

ABSTRACT

Electronic money server-based issuers are faced with the reality of the emergence of threats from information technology risks and insufficient knowledge of the impact of the risk of user data leakage on electronic systems used. However, on the other hand, the operator does not have an integrated method to identify and assess the risk to information technology security and user data privacy. This study focuses on the integration risk assessment of information security and user data privacy in electronic money server-based mobile applications using ISO 27001:2013, ISO 27005:2018, and ISO 27701:2019. The data was obtained from one of the providers in Indonesia through leadership interviews and observations of mobile applications with the scope of business processes for user registration, top up of balances, and acting as a Personally Identifiable Information Controller. The evaluation uses the KAMI Index version 4.1 for understanding the condition of the organization and the final results after the implementation of the risk assessment based on the three implemented standards. The results of the study explain that company XYZ has an electronic system category with a value of 26 (High), and the value of the application of information security and privacy increases from level I (initial condition) to II (basic framework). This study provides a comparative analysis and method of information technology risk assessment related to privacy information, so that the use of the three proposed standards can be a reference for any organization to expand the control of information technology security controls on user data privacy and compliance with regulations.

Keywords: *Risk Assessment, Information Security, Privacy Information, Electronic Money*

1. INTRODUCTION

Development of payment systems also known as electronics as transaction no cash has grown in Indonesia since the year 2009 with the rise of Bank Indonesia regulations in the form of regulation regarding electronic money. Bank Indonesia must do an effort to strengthen in Thing system payment electronic as an effort to enhance awareness of the Public for the use of non-cash transactions and make it happen ecosystem cashless society [1].

Technology and changes in people's lifestyles greatly affect the development of electronic money payment systems as micro-payment instruments. This is indicated by the increasing use of electronic money in Indonesia. Bank Indonesia data for the period 2015-2021 shows the number of electronic money instruments in circulation from 34 million units to 511 million units, nominal transactions from 5.28 trillion rupiahs to 132.05 trillion rupiahs. This is in line with the growth in the number of electronic money providers, until 2021 there have been 60 companies that have licenses.

The rapid growth of electronic money with the support of sophisticated systems makes the organizers faced with the reality that there will be a threat of information technology risk and insufficient knowledge of the impact of the risk of user data leakage on the electronic system used. However, on the other hand, the operator does not have an integrated method for conducting an information technology security risk assessment [2], moreover the protection or privacy of user data.

Payment transaction processing regulations related to the use of electronic money instruments require providers to fulfill consumer protection aspects to maintain user data privacy as a mitigation or prevention effort amid the threat of fraudulent transactions and cybercrimes. One of the main risks is the leakage of personal data as a result of threats to privacy along with the massive use of the internet and weak protection of data and information. Cyber portal site data states that throughout 2020 there have been 36 cases of data theft [3].

PT XYZ is a financial technology company that already has a license to operate electronic money with server-based electronic money storage media. The company is obliged to maintain the privacy of user data from threats of information security risks such as leakage of personal data on their electronic money mobile applications. Data privacy in question such as identity data contained in national population data, telephone number data, and email used as authentication parameters as well as other related data such as transaction data that can initiate user profiles. Therefore, companies must have an integrated method for conducting risk assessments as part of implementing risk management and mitigation of various information security risk threats. This study applies three standards, namely ISO 27001:2013 as an information security standard, ISO 27701:2019 as an information privacy standard, and ISO 27005:2018 which are linked to carrying out the information technology security risk management cycle and user data privacy on server-based electronic money mobile applications.

This study focuses on the integration risk assessment of information security and user data privacy in electronic money server-based mobile applications using ISO 27001:2013, ISO 27005:2018, and ISO 27701:2019, so provides a comparative analysis and method of information technology risk assessment related to privacy information acting as PII Controller, so that the use of the three proposed standards can be a reference for any organization to expand the control of information technology security controls on user data privacy. Organizations must have the ability to carry out information security risk management with appropriate and correct methods [4], therefore information security aims to protect the company's information assets against aspects of confidentiality (C), integrity (I), and availability (I).

2. RELATED WORKS

In research on information security, the ISO 27001 standard becomes a guide in the implementation of information security controls. Research [5] describes the handling of information security issues in government agencies determining security control objectives in the process of identifying information assets, risk assessment, risk control, and using the System Security Engineering Capability Maturity Model (SSE-CMM) method in the evaluation process to measure effectiveness standard application. The study by [6] conducted a risk assessment related to information security aimed at determining the risk of information assets and their impact on academic information systems and then calculating the value of assets and risks with CIA criteria such as the principles of the ISO 27001 standard. The study by [7], implementation of information security planning based on ISO 27001 using the Analytical Hierarchy Process (AHP) method at the stage of gap analysis in a government institution. On several other issues, the ISO 27001 standard is implemented by integrating it into other standards such as the implementation model of information technology service management using ISO 20000 to provide recommendations for security control on IPTV/VoIP services in telecommunication companies in Bosnia & Herzegovina [8]. The study by [9] provides suggestions from the results of the integration of ISO 20000, ITIL V3, and ISO 27001 to help organizations that implement information security standards and information technology management simultaneously.

Implementation of the ISO 27001 standard requires organizations to carry out information security risk assessment stages [10], which generally refers to its family standard, namely ISO 27005 as a standard for information security risk management techniques. The study by [11] proposes a practical guide to managing information technology risk in government institutions using the ISO 27005 standard. In research on the vulnerabilities and risks that arise in payment methods using contactless smart cards in the transportation system in Colombia, propose an evaluation risk based on the ISO 27005 standard by identifying threats, vulnerabilities, and inherent risks. The ISO 27005 standard is also used in research to answer problems in the maintenance and inspection information system in a telecommunications company that has not considered the risk assessment aspect in its use [12]. Some studies also combine the risk assessment process with other standards such as NIST 800-300 to support ISO 27005 in the stages of risk identification, risk analysis, and risk evaluation [13].

The ISO 27001 standard has not been designed in detail to control risks from privacy-related threats such as data leakage, data theft, or breaches of customer data, so expansion is needed to assist companies in mitigating privacy threats and risks [14]. The ISO 27701:2019 standard was published to address information security challenges and threats as an extension of ISO 27001:2013 to be implemented as an additional requirement of information security standards and applicable guidance for privacy or protection of personal data that could potentially affect PII. The ISO 27701:2019 privacy risk management approach follows the same cycle as the information security standard, generally referring to the ISO 27005:2018 risk management methodology [15]. Research [16] proposed the design of privacy information security controls in the electronic card business process for a Driving License (SIM) based on an analysis of ISO 27001:2013 and 27701:2019. Study by [17] evaluated compliance with privacy protection in e-government systems in West African countries using ISO/IEC 29100:2011.

Protection of information from various threats to ensure continuity effort, reduce risk business, and improve return investment and opportunity business. Information security is an effort for protection, at least three principles to do for ensuring the effective application of information security that is confidentiality (C), integrity (I), and availability (A). Besides that's, aspect information security consists of Authentication, Identification, Authorization, Privacy, and Accountability [18].

A standard that refers to used organizations for the implementation of information security is ISO 27001. This is standard international already used by various sectors of industry good private, government, and non-profit sectors. Standard used as guidelines and requirements of information security, started from initiation, implementation until maintenance security in the organization as part of control [19]. Standard this has 7 clauses requirement domain information security, 14 control information security contains 35 controls and 114 controls or called as Annex A [7].

Privacy information is the ability of an individual to control or have several influences on information personal, everything from related information direct to identity that can be identified. The use of information technology causes the potential risk to privacy information so that needs something framework proper work as effort protection to data or identifying identity or profile individual [16].

Research by [20], describes the mechanism for implementing information security controls to design, maintain, and improve protection aspects using ISO 27701:2019. This standard is an extension of ISO 27001 and ISO 27002 which are set to regulate the management of information privacy. The specific control of information privacy management based on ISO 27701:2019 is how the organization has adequate controls to manage and protect aspects of Personally Identifiable Controllers (PII). Privacy Information Management requires organizations to establish themselves as controllers and/or processors of user identity data that they manage, as the basis for protecting personal data and fulfilling privacy principles, which are oriented to the consent and choice of the owner of personal data, conveying the purpose of collecting personal data individually as specific, restrictions on personal data collection, minimal presentation of personal data, restrictions on use including data storage and disclosure, data accuracy and quality management, transparency, providing easy access for personal data owners, accountability, protection of personal data as control of information security, and compliance to the applicable laws.

This study will produce recommendations for information security control controls related to user data privacy based on the results of risk assessments and ensure that the risks inherent in server-based electronic money mobile applications can be identified, analyzed, and mitigated following company conditions and management expectations to improve information security maturity. The results of this study can provide comparative analysis and information technology risk assessment methods related to information privacy so that the use of the three proposed standards can be a reference for expanding information technology security controls related to user data privacy and compliance with regulations.

3. RESEARCH METHOD

The analysis of this study conducted a review of each standard of ISO 27001 and ISO 27701. The method approach carried out in this study used a qualitative method where the study was carried out by analyzing the content of each standard of information security and information privacy by reviewing and finding links to each other both from clauses and annex controls.

We formulate information security controls related to user data privacy at PT XYZ electronic money issuer, identify problems, and explore the company's condition on potential risks to information security and information privacy. The data used in this study were obtained from interviews with leadership and observations on the user registration business process, electronic money balance replenishment, and mobile applications and information technology used as part of the company's information assets, in addition, we conducted interviews with stakeholders, namely the head in charge of information technology security and the head of risk management.

The results of the analysis of the review of ISO 27001 and ISO 27701 standards will then become the basis for later controlling information security and information privacy, then the analysis is carried out by comparing similarities and differences which will produce an integration matrix. In the next stage, we run a series of risk assessment processes based on the ISO 27005 standard which we mapped with the information privacy risk assessment requirements as required by the ISO 27701 standard so that at this stage we initiated the new information security and information privacy risk assessment terms (New Infosec & Privacy Risk Assessment). **Figure 1.** Show pictures of the study process that we do.

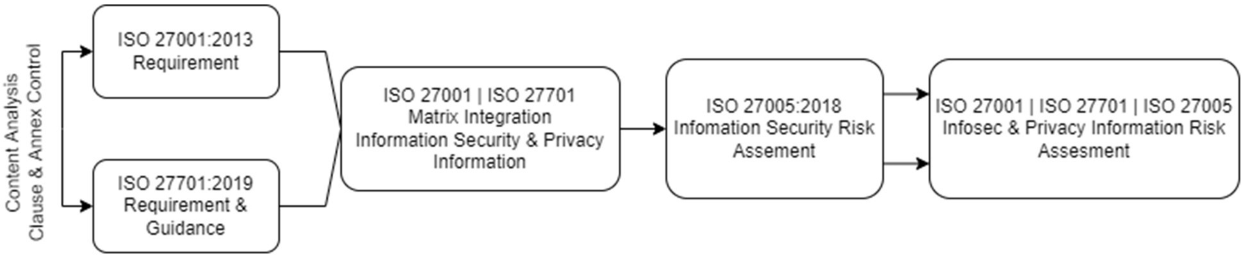

Figure 1. Information Security & Information Privacy Risk Assessment Methodology

In Table 1, describes the mapping between the information privacy requirements of the ISO 27701:2019 standard which is linked to the ISO 27001:2013 information security standard in terms of the implementation of controls.

Table 1. Mapping of ISO/IEC 27001:2013 against ISO 27701:2019

Clause Number ISO 27001:2013	Title	Clause Number ISO 27701:2019	Information
4	Organizational Context	5.2	Additional requirements special for privacy
5	Leadership	5.3	Not required addition requirements
6	Planning	5.4	Additional requirements special for privacy
7	Support	5.5	Not required addition requirements
8	Operation	5.6	Not required addition requirements
9	Performance evaluation	5.7	Not required addition requirements
10	Enhancement	5.8	Not required addition requirements

Content analysis in the clauses of ISO 27001:2013 and ISO 27701:2019 contains similarities in Context Organization and Planning. In context organization, the company in requirements implementation privacy information need add and define the role act as PII-Controller, requirements addition about the needs and expectations of the parties related with the organization, include mechanism PII processing in determine scope, as well as ensure consistency determination and implementation PDCA cycle with requirements of ISO 27001:2013 described in Clause 5 of the ISO 27701:2019 standard.

4. RESULT AND DISCUSSION

4.1 Content Analysis

In stages early, we study the respective contents of the ISO /IEC 27001:2013 and ISO/IEC 27701:2019 standards with destination get results comparison similarities and differences between the two standards and generate matrix integration as recommendation control among information security and privacy information that will be used for could be chosen as appropriate controls on the privacy of user data on electronic money issuers based on PT XYZ server. The analysis result is shown in Table 2.

Table 1. Recommended Integration Matrix Results Control Between Information security and Privacy Information

Clause-Annex	ISO/IEC 27001:2013	clause	ISO/IEC 27701:2019
CL.4	Context of the organization	CL.5.2	Context of organization
CL.6	Planning	CL.5.4	Planning: with additional conducting additional privacy risk assessment
A.5.1	Management direction for information security	CL.6.2.1	Management direction for additional information security with additional privacy guidance
A.6.1	Internal organization	CL.6.3.1	Internal organization with additional privacy guidance
A.6.2	Mobile devices and teleworking	CL.6.3.2	Mobile device and teleworking with additional privacy guidance
A.7.2	During employment	CL.6.4.2	During employment with additional privacy guidance
A.8.2	Information classification	CL.6.5.2	Information classification with additional privacy guidance
A.8.3	Media Handling	CL.6.5.3	Media handling with additional privacy guidance
A.9.2	User access management	CL.6.6.2	User access management with additional privacy guidance
A.9.4	System and application access control	CL.6.6.4	System and application access control with additional privacy guidance
A.10.1	Cryptographic control	CL.6.7.1	Cryptographic control with additional privacy guidance
A.11.2	Equipment	CL.6.8.2	Equipment with additional privacy guidance
A.12.3	Backup	CL.6.9.3	Backup with additional privacy guidance
A.12.4	Logging and monitoring	CL.6.9.4	Logging and monitoring with additional privacy guidance
A.13.2	Information transfer	CL.6.10.2	Information transfer with additional privacy guidance
A.14.1	Security requirements of information system	CL.6.11.1	Security requirements of information system with additional privacy guidance
A.14.2	Security in development and support processes	CL.6.11.2	Security in development and support processes with additional privacy guidance
A.14.3	Test data	CL.6.11.3	Test data with additional privacy guidance
A.15.1	Information security in supplier relationship	CL.6.12.1	Information security in supplier relationship with additional privacy guidance
A.16.1	Management of information security incidents and improvements	CL.6.13.1	Management of information security incidents and improvements with additional privacy guidance
A.18.1	Compliance legal and contractual requirements	CL.6.15.1	Compliance legal and contractual requirements with additional privacy guidance
A.18.2	Information security reviews	CL.6.15.2	Information security reviews with additional privacy guidance

In implementation studies, this needs attention main about a clause in ISO/IEC 27701:2019 PII Controller for planning control related privacy of user data on electronic money issuers server based which is not Specific set in standard ISO/IEC 27001:2013 [20]. Control as PII Controller is described in **Table 3**

Table 3. Control Privacy Act as PII Controller

Clause ISO 27701:2019 Control as PII Controller
7.2 Conditions for collection and processing
7.3 Bonds to PII Principals
7.4 Privacy by design and privacy by default
7.5 PII sharing, transfer, and disclosure

4.2 Privacy Risk Management

Process management risk-related privacy information was carried out in the study this is in line with the principle applied to the cycle evaluation risk information security that uses ISO /IEC 27005:2018 standard. Application evaluation risk is shown in Table 4, as mapping, every stage evaluation risk information security with privacy information.

In terms of privacy, rating risk is also called the term privacy impact assessment. Steps are identification risk, analysis risk, and evaluation risk as well as handler risk. Evaluation risk privacy information expects certainty to the organization for having adequacy in control from potency loss aspect confidentiality (C), integrity (I), and availability (A) related to the processing of Personally Identifiable Information (PII) in scope privacy information management.

Table 2. Information security related to Privacy Risk

clause	ISO 27001:2013	clause	ISO 27701:2019	clause	ISO 27005:2018
CL.6.1.2	Information Security Risk Assessment	CL.5.4.1.2	Information Security and Privacy Risk Assessment: • Privacy risk identification • Privacy risk analysis • Privacy risk evaluation	CL.8	Risk Assessment: • risk identification • risk analysis • Risk Evaluation
CL.6.1.3	Information Security Risk Assessment	CL.5.4.1.3	Information Security and Privacy Risk Treatment	CL.9	Risk Treatment

4.3 Risk Assessment Privacy Information

4.3.1 Determination Context Organization

That the management process risks privacy on study this is done in line with framework work described in ISO/IEC 27005:2018 which includes including the process of understanding context organization, appraisal risk, handling risks and criteria reception risk. Stages evaluation risk follow term as already _ described in Table 4 in implement clause 5.4 is information security and privacy risk assessment. A series of assessment processes risk in the study this only in the scope of 2 business processes as described in registration account and top up balance electronic money.

4.3.2 Privacy Risk Identification

Stage this includes doing identification to information assets, identification threat, identification vulnerability, identification on the existing control that has been related with privacy data on electronic money issuers with scope 2 business processes. We have identified 11 assets of PT XYZ which consist of categories of data, software, and hardware and sources are triggering the threat problem of privacy that has been happened.

4.3.3 Privacy Risk Analysis

The purpose of the privacy risk analysis stage is to get results from appraisal of risk-related data privacy based on the impact and likelihood of every identified risk. As for the criteria evaluation to the likelihood for justifying frequency incident possible risks occur in a year, while criteria impact assessment is based on several categories like possible risks impact to reputation organization, distraction operational, potential loss financial, and potential risk law. In phase, this was implemented to 14 potential risk that has been successfully identified with the result of 7 risks is high, 4 risks is medium, and 3 risks is low. Formulation results score risk obtained based on multiplication between likelihood and impact on every potency the risk that has been identified, next results calculation whole risk will be evaluated. Table 5 is matrix risk as a reference after each potential risk identified assessed and produced score level risk low (1-2), medium (3-4), or high (6-9).

Formula to define risk score is

Risk Score = Likelihood × Consequence (1)

Tables 5. Likelihood and Impact Risk Matrix

Likelihood X Consequence	Low (1)	Medium (2)	High (3)
High (3)	Medium (3)	High (6)	High (9)
Medium (2)	Low (2)	Medium (4)	High (6)
Low (1)	Low (1)	Low (2)	Medium (3)

4.3.4 Privacy Risk Evaluation

From the result evaluation risk will obtain level risk based on evaluation independently conducted by subject matter experts in the organization. After the whole potency identified risks so mapped to matrix criteria from appetite risks defined by the organization. Criteria reception risk will take effect to mechanism handling risk like add control or evaluate control moment this for getting score risk at acceptance level i.e., low level to medium. For risk level currently too tall already should organization to do control mitigation. Figure 2 shows the assessment and evaluation of the results of the risks we have carried out in the study.

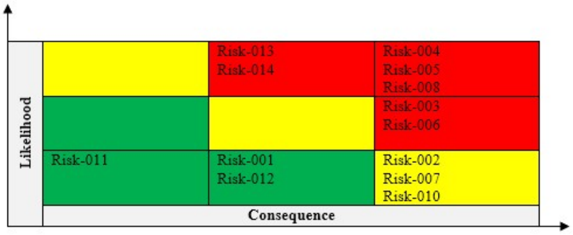

Figure 2. Privacy Risk Evaluation

Table 6. Risk Evaluation with Privacy Control Recommendation

Code	Risk Level	Control Existing	Control Recommedation From ISO 27001 | ISO 27701
Risk-001	**Low**	IAM, HTTPS/SSL Encypted Data Processing	Risk Accepted
Risk-002	**Medium**	IAM	CL.6.6.2: User access management with additional privacy guidance CL.6.6.4: System and application access control with additional privacy guidance
Risk-003	**High**	-	CL.6.10.2 Information transfer with additional privacy guidance 7.4 Privacy by design and privacy by default 7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosed to third parties
Risk-004	**High**	Password (Hash), PIN, 2-Factor Authentication	CL.6.11.1 Security requirements of information system with additional privacy guidance CL.6.11.2 Security in development and support processes with additional privacy guidance
Risk-005	**High**	-	CL.6.11.1 Security requirements of information system with additional privacy guidance CL.6.11.2 Security in development and support processes with additional privacy guidance
Risk-006	**High**	User Access Matrix	CL.6.6.2: User access management with additional privacy guidance CL.6.6.4: System and application access control with additional privacy guidance
Risk-007	**Medium**	-	CL.6.10.2 Information transfer with additional privacy guidance 7.4 Privacy by design and privacy by default

Code	Risk Level	Control Existing	Control Recommedation From ISO 27001 | ISO 27701
			7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosed to third parties
Risk-008	**High**		CL.6.11.1 Security requirements of information system with additional privacy guidance
Risk-009	**Medium**		CL.6.10.2 Information transfer with additional privacy guidance 7.4 Privacy by design and privacy by default 7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosed to third parties
Risk-010	**Medium**		CL.6.10.2 Information transfer with additional privacy guidance 7.4 Privacy by design and privacy by default 7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosed to third parties
Risk-011	**Low**	GCP Autoscaling	Risk Accepted
Risk-012	**Low**	Load balancer, VPC Network	Risk Accepted
Risk-013	**High**	-	CL.5.2 Context of organization CL.6.10.2 Information transfer with additional privacy guidance 7.2 Condition for collection and processing 7.3 Obligations to PII Principals 7.4 Privacy by design and privacy by default 7.4 Privacy by design and privacy by default 7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosed to third parties
Risk-014	**High**	-	CL.5.2 Context of organization CL.6.10.2 Information transfer with additional privacy guidance 7.2 Condition for collection and processing 7.3 Obligations to PII Principals 7.4 Privacy by design and privacy by default 7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosed to third parties

4.3.5 Evaluation

Studies apply recommendations for control-related data privacy based on results from stages evaluation risk, calculate score index related data privacy, and assessment by subject matter experts in organizations. Assessment results in level application data privacy using tool help in the form of KAMI Index version 4.1 which we focus on calculation aspect personal data protection with repair results from value 56% (analysis initial) to 70% (after evaluation risk). That the process of electronic money services server-based is category system electronic character tall with value 26, while on analysis beginning total value obtained index application information security and privacy experience enhancement from value 316 become 420. From 7 aspects as evaluation parameter has shown results at implementation level application framework work basic, specifically on aspects management risk and data privacy experienced repair significant though still there is a gap that does not fit properly with hope management. Table 7 explains the results evaluation of application information security and data privacy.

Evaluation calculation formula each aspect is

$$\text{Evaluation } indeks\ score = \sum_{i=1}^{n} ev \ (2)$$

$$\text{evs} = (wa + wb + wc) + (xa + xb + xc) + (ya + yb + yc) + (za + zb + zc)$$

evs = evaluation score each aspect
w, x, y, z = Total of answer from each question
a, b, c = Weight for control 1, 2, and 3

Table 3. Result gap evaluation of information security related to privacy information

Aspect	Target	Before	After	Gap
1. Governance	II+	I+	II	1
2. Risk Management	II+	I+	II	1
3. Framework	II+	I+	II	1
4. Asset Management	II+	II	II	1
5. Technology	II+	II	II	1
6. Vendor Management	85%	78%	80%	5%
7. Privacy Information - Supplement	75%	56%	70%	5%

That the current research provides additional in terms of risk assessment of information security and information privacy, to what has been proposed in previous studies regarding the design of information security control designs related to privacy, in previous researcher's aspects of data privacy have not been comprehensively discussed in the implementation of information security, besides that there is no evaluation in measuring the level of implementation effectiveness, so the current research proposed KAMI Index mechanism to help calculate each aspect for evaluation information security and privacy.

5. CONCLUSION AND FUTURE WORKS

Analysis result of information security and privacy information on electronic money issuers server- based show there is harmony between ISO/IEC 27001:2013 and ISO/IEC 27701:2019, there are 2 clauses and 20 security annex controls information with addition for recommendation guide implementation to the privacy information and 4 clauses main as recommendation control privacy because of organization in scope this only Act as PII Controller. Assessment results risk from scope business registration process user and charging electronic money balance there is 30 potential the risk that has been successfully identified with result 3 risks high, 12 risk medium, 12 risk low. The results of the evaluation carried out use tool help US index version 4.1 gets results at implementation level application framework work base with level II increased after implementation evaluation risk from score start I or show condition start, evaluate aspect personal data protection increase from 56% to 70%, though still there is a gap that needs strive for conducted future improvement come for getting appropriate value with hope management.

Studies this expected capable give analysis comparative and method evaluation risk technology information related privacy information, so that use third proposed standard could become the reference for organization anywhere for expanding control information security technology on user data privacy as well as fulfillment compliance to regulation.

Suggestions for development studies next could be conducted with add criteria organization in action as a PII Processor or PII Join Controller and additional framework work management risk information security and privacy information other for strengthening recommendation control related specifically with personal data security.

6. ACKNOWLEDGMENT

The publication is supported by Bina Nusantara University, we would like to say thank you to all parties to help and involve in this study.

REFERENCES:

[1] H. Kartika, Y. A. Fatimah, and S. H. Supangkat, “Secure Cashless Payment Governance in Indonesia: A Systematic Literature Review,” *2018 International Conference on ICT for Smart Society (ICISS)*. IEEE, 2018, doi: 10.1109/ictss.2018.8549980.

[2] S. Alfarisi and N. Surantha, “Risk assessment in fleet management system using OCTAVE allegro,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 1, pp. 530–540, 2022, doi: 10.11591/eei.v11i1.3241.

[3] F. L. Gaol, A. D. Budiansa, Y. P. Weniko, and T. Matsuo, “Cyber crime risk control in non-banking organizations,” *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 5, pp. 1219–1231, 2021.

[4] W. Al-Ahmad and B. Mohammed, “A code of practice for effective information security risk management using COBIT 5,” *2015 Second International Conference on Information Security and Cyber Forensics*

(InfoSec). IEEE, 2015, doi: 10.1109/infosec.2015.7435520.

[5] Nurbojatmiko, A. Susanto, and E. Shobariah, “Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO Depok City,” *2016 4th International Conference on Cyber and IT Service Management*. IEEE, 2016, doi: 10.1109/citsm.2016.7577471.

[6] Angraini, Megawati, and L. Haris, “Risk Assessment on Information Asset an academic Application Using ISO 27001,” *2018 6th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2018, doi: 10.1109/citsm.2018.8674294.

[7] O. C. Briliyant, J. Widhi Candra, and S. Rebeca Tamba, “ISMS Planning Based On ISO / IEC 27001 : 2013 Using Analytical Hierarchy Process at Gap Analysis Phase (Case Study : XYZ Institute),” *1th Int. Conf. Telecommun. Syst. Serv. Appl.*, vol. 4, no. 4, pp. 4–9, 2016.

[8] A. Tanovic and I. S. Marjanovic, “Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard,” *2019 42nd Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2019 - Proc.*, pp. 1503–1508, 2019, doi: 10.23919/MIPRO.2019.8756843.

[9] B. Al Faruq, “Integration of ITIL V3, ISO 20000 &amp; ISO 27001:2013forIT Services and Security Management System,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 3, pp. 3514–3531, 2020, doi: 10.30534/ijatcse/2020/157932020.

[10] International Organization for Standardization, *Internasional Standard ISO/IEC 27001:2013*, vol. 2014, no. ISO/IEC 27001:2013. 2013.

[11] S. Patino, E. F. Solis, S. G. Yoo, and R. Arroyo, “ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005,” *2018 5th Int. Conf. eDemocracy eGovernment, ICEDEG 2018*, no. April, pp. 75–82, 2018, doi: 10.1109/ICEDEG.2018.8372361.

[12] M. S. Ivan Felipe, L. V. Sergio Andres, and B. G. Raul, “Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp D.C Colombia,” *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)*. IEEE, 2019, doi: 10.1109/coniiti48476.2019.8960881.

[13] S. Jaya Putra, M. Nur Gunawan, A. Falach Sobri, J. M. Muslimin, Amilin, and D. Saepudin, “Information Security Risk Management Analysis Using ISO 27005: 2011 for the Telecommunication Company,” *2020 8th Int. Conf. Cyber IT Serv. Manag. CITSM 2020*, 2020, doi: 10.1109/CITSM50537.2020.9268845.

[14] A. R. Putra, Fandi Aditya; Setiawan, H; Pradana, “Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Application of XYZ Institute,” in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2017, pp. 251–256.

[15] L. C. Hamit, H. Md. Sarkan, N. F. Mohd Azmi, M. N. Mahrin, S. Chuprat, and Y. Yahya, “Adopting ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients Data Theft,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 3, p. 914, 2020, doi: 10.18517/ijaseit.10.3.10172.

[16] M. I. Fadhil and F. Hidayat, “Control Design of Information Security Related to Privacy in The Smart SIM Business Process,” *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)*. IEEE, 2021, doi: 10.1109/eiconcit50028.2021.9431861.

[17] A. C. Nwaeze, P. Zavarsky, and R. Ruhl, “Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011,” *2017 Twelfth International Conference on Digital Information Management (ICDIM)*. IEEE, 2017, doi: 10.1109/icdim.2017.8244644.

[18] D. Kouns, Jake; Minoli, *Information Technology Risk Management In Enterprise Environments*. Canada: John Wiley & Sons, Inc., Hoboken, New Jersey, 2010.

[19] H. J. Whitman, Michael E.; Mattord, *Principles of Information Security, Fourth Edition*. Boston, USA: Course Technology, Cengage Learning, 2012.

[20] M. I. Fadhil and F. Hidayat, “Control Design of Information Security Related to Privacy in the Smart SIM Business Process,” *3rd 2021 East Indones. Conf. Comput. Inf. Technol. EIConCIT 2021*, pp. 66–72, 2021, doi:

10.1109/EIConCIT50028.2021.9431861.

[21] G. Wangen, C. Hallstensen, and E. Snekkenes, “A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF,” *Int. J. Inf. Secur.*, vol. 17, no. 6, pp. 681–699, 2018, doi: 10.1007/s10207-017-0382-0.

[22] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, “Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency,” *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.

[23] H. Setiawan, F. A. Putra, and A. R. Pradana, “Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute,” *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*. IEEE, 2017, doi: 10.1109/icitsi.2017.8267952.