Jurnal Informatika Ekonomi Bisnis

http://www.infeb.org

2024 Vol. 6 Iss. 4 Hal: 815-821 e-ISSN: 2714-8491

Risk Management Design and Analysis on Agile Development Project using ISO 31000 Integrated with ISO 27005: A Case Study of SiREV Application

Redry Maynard Ananda Sinulingga[1]✉, Teguh Raharjo[2], Ni Wayan Trisnawaty[3]

[1,2,3]Universitas Indonesia

redry.maynard21@ui.ac.id

Abstract

Implementing e-government in Indonesia, one example of technology adoption in the government sector is the digitalization of business processes within government agencies. SiREV application is an information system used by auditor XYZ Agency in carrying out business processes in the field of supervision. In developing this application, the agile method was chosen to accommodate several reasons starting from requirements that could not be determined at the beginning of the work implementation and changes to the application in the future that needed to be made to adapt to needs. Several obstacles are encountered in its implementation which are the familiarity of using agile methods and the security of the information while developing it. To conduct this research, we use ISO 31000:2018 and ISO 27005:2018 framework to assess the risks. This study aims to assess risk in agile project with ISO 31000 and ISO 27005 so that XYZ Agency has a design of risk management related to agile implementation in project development and information security. The results of this research showed that 24 risks were identified, consisting of 11 risks related to agile implementation and 13 risks related to information security. After doing risk evaluation from these 24 risks, 13 risks need to be handled because they are outside the organization's risk appetite, while the other 11 risks do not need to be handled because they are within the organization's risk appetite.

Keywords: Agile Method, Information Security, Risk Management, ISO 31000:2018, ISO 27005:2018.

1. Introduction

Implementing e-government in Indonesia, there are several infrastructures that can be used to support this and technology adoption. According to Presidential Regulation No. 95 of 2018, One example of technology adoption in the government sector is the digitalization of business processes within government agencies [1]. In current conditions, there are several ministries and institutions that already have implement this, one of those who have implemented this is XYZ Agency.

In the implementation of digitalization of business process, one example of technology adoption in the government sector is the digitalization of business processes in the field of supervision. In this paper, we use a case of SiREV application. This application is an information system used by Inspectorate General of XYZ Agency in carrying out business processes in the field of supervision.

In developing this application, the agile method was chosen to accommodate several reasons starting from requirements that could not be determined at the beginning of the work implementation and changes to the application in the future that needed to be made to adapt to needs. However, in using the agile method there are obstacles encountered in its implementation. In this organization, the waterfall method is the most frequently used method. This results in using the agile method, there will be many risks that will be encountered which can result in not achieving the objectives of developing this application. To solve the problems, good project management is needed to ensure that the project is executed according to the predetermined time, budget, and quality. One way to ensure and maintain the quality of the project in line with the established targets is to implement risk management during the project execution [2], [3].

Risk management reduces uncertainty and enhances success. In Agile software development, it's integrated into the process implicitly. This implicit approach can cause problems and may miss some risks. Effective risk management is also essential for Agile development, with a need for some explicit technique [4]. According to the authors in certain research, the implicit approach to risk management can result in various new risks [5]. To manage risks effectively in Agile software development, conscious and careful effort is needed. Based on previous research also mentioned that risk management is essential and must be clearly defined for project development [6]. It consists of the phases of Assessment and Controlling, each with its own hierarchical structure.

Another risk that needs to be considered in terms of risk management related to application development is information security because there are several critical pieces of information that need to be secure while developing this application. While numerous structured

Accepted: 04-12-2024 | Revision: 10-12-2024 | Publication: 31-12-2024 | doi: 10.37034/infeb.v6i4.1053

risk management strategies have been suggested for Agile development, cyber-related security threats have received little attention. According to studies, Agile teams rarely outsource the specialized skills and expertise necessary to manage cybersecurity threats. Security specialists were frequently scarce, and their functions were unclear. In Agile projects, this could result in engineers handling cybersecurity issues without sufficient prior knowledge [7].

In managing risk, there are several frameworks that we can use. One of global standard that we can use is standard from International Organization for Standardization (ISO). There are several references regarding risk management from ISO and in this study, we will focus on ISO 31000 which is standard for risk management and ISO 27005 on guidance on managing information security risk [8]. The standard from ISO have already known and widely uses in XYZ Agency and guidelines for preparing risk management at XYZ Agency are based on ISO 31000. These are the reasons why we chose this standard in this study [9].

According to a previous study on agile software development risk management, the biggest problem with Agile methods is that they implicitly manage risk by reducing it through sprints. The practices within each sprint target reducing negative outcomes and thus lowering risk, which has been enough for software developers and the industry to support decision-making efforts. Therefore, Agile lacks a specific strategy for managing risk without deliberate risk management [10]. Furthermore, other authors have recommended hybrid solutions that integrate conventional risk management tools with an agile approach to assess risk in agile project. However, between traditional risk methods, compatibility challenges with agile methods occur because they interpret critical project variables differently. Aspects like adaptability, documentation, added value, processes, team composition, project management, delivery scope, collaboration, communication, transparency, and leadership are viewed through different lenses in each method, limiting the effectiveness of hybrid approaches [2], [10].

Other study related to cybersecurity risk in agile software projects identified two methods to implement risk management which area integrating risk management system or adopting agile technologies for addressing risk, but this study has not yet carried out risk assessment using either these methods [7]. However, from previous studies, there have been no further explanations regarding the suitable risk management approaches to implement in assessment in agile project. This study aims to assess risk in agile project with ISO 31000 integrated ISO 27005 as one of international standard in risk management with study case in one of application that are going to be developed in XYZ Agency which is SiREV application and will be the new things in risk assessment in project development.

This paper presents the following research question:

RQ: What is the design of risk management in SiREV application using ISO 31000 integrated with ISO 27005?

The results of this research will propose the risk management that are related to agile implementation and information security.

2. Research Method

This section explains the research methodology that is carried out during research and explains methods also instruments to collect and process data. The research methodology adopted in this study is based on the ISO 31000 process in conducting risk assessment [11]. The research methodology is carried out by literature study, interviewing people in charge that related to software development and information security and gathering important data that author needs. After that, analysis was held to assess all risks that related agile implementation in project and information security from the information systems that organization going to build as follows ISO 27005 [12].

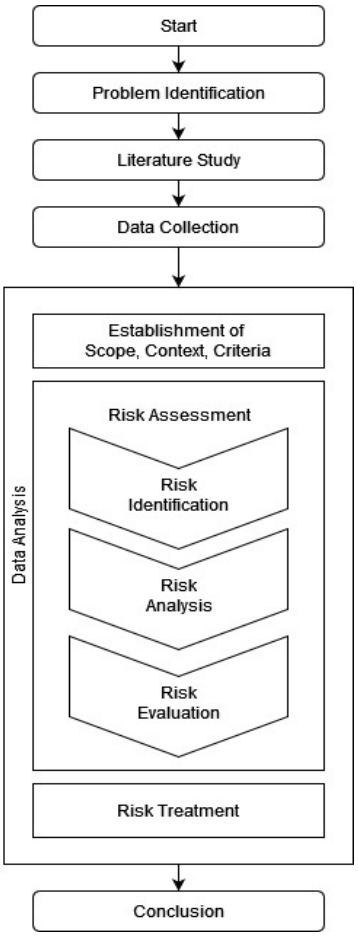

Figure 1. Research Methodology

The research methodology as depicted in Figure 1 can be described as follows:

2.1. Problem Identification

Problem Identification in this study was obtained from interview and observation within organization regarding agile implementation in project development as well as lack of risk management in terms of information security in organization, especially in the phase of project development. Based on the results of the interview, it was found that the implementation of the agile method in software development at XYZ Agency is something new and several risks must be mapped out that could hinder the completion of the project in accordance with what has been determined.

2.2. Literature Study

This section explains a literature study using some theory that is already used in the common professional world. The literature study focuses on agile implementation theory, risk or hazard in agile implementation, the theory of risk management, risk in managing information security, previous research, and related regulations.

2.3. Data Gathering

Qualitative data gathering methods were used in this study. These methods focus on analyzing and describing phenomena or research subjects through individuals' or groups' social activities, attitudes, and perceptions. The study utilized both primary and secondary data. Primary data was collected directly from sources, by doing interview with the person in charge, then doing some observations in the organization, and by making questionnaires that need to fill in by person who really know about the topics [13]. In interviews, there are some methods that we can use. Doing one-on-one or by gathering groups are some alternatives. Then after we choose what method of interviews that we are going to use, we can do it in person or by conference call through conference application. To collect secondary data, alternatives that we can use are by study from previous research, internal organization policies and theoretical books [13].

2.4. Data Analysis

Data, which was previously gathered, were analyzed using ISO 31000:2018 guidelines and ISO 27005:2018. The analysis begins with setting the risk management context, including setting the basic criteria and providing the necessary scope and context related to project development risk management in XYZ Agency. A risk assessment is then performed by identifying, measuring, and prioritizing risks according to the set of criteria for evaluation. After that, the next step is to do risk analysis through impact assessment, probability assessment, determination of the magnitude risk and ranking the risks. Finally, controls are implemented to reduce, maintain, avoid, or transfer the identified risks. These controls are determined based on ISO 31000 and ISO 27005 [14].

2.5. Conclusion

The last step in this research is to make conclusions regarding risk management in SiREV application. In this section, it will present the result of risk assessment on SiREV application that is related to agile implementation and risk on information security as well as the recommendation of control to all those risks.

3. Result and Discussion

This chapter covers the process of implementing risk management. This study's analysis focuses on implementing risk strategies through the ISO 31000 dan ISO 27005 framework and provides recommendations based on the identified risks. There are several activities that need to be done following the framework of ISO 31000 and ISO 27005. Although there are similarities between them, there are also differences which is ISO 31000 is more general in the risk and ISO 27005 is more specific in information security risk [9], [15]. Several steps that were concluded will be explained in this chapter.

3.1. Establishment of Scope, Context and Criteria

The initial step in risk management procedures is to determine the context for all the risk process. It includes setting targets for risk implementation and establishing risk criteria, such as risk evaluation criteria, criteria of impact, criteria of likelihood, and criteria of risk acceptance, that will serve as a reference during the risk assessment. In terms of scope, context and criteria, because the research location is in XYZ Agency, there are already internal regulations from XYZ Agency related to risk management, namely XYZ Agency Regulation No. 6 year 2017. In this regulation, XYZ Agency already defines impact and likelihood criteria as can be seen in Table 1 and Table 2, risk matrix in Table 3 and risk acceptance criteria in Table 4.

Table 1. Criteria of Impact

Level	Criteria of Impact		
	Finance	Performance	Operational
Very low - 1	up to IDR 5 million in losses	Interference one - two days	Minor disturbance
Low - 2	5 million to 10 million IDR losses	delay of up to a week	Performance declines by 20-40%.
Moderate - 3	10 million to 25 million IDR losses	Interference one - two weeks	Performance declines by 40-60%.
High - 4	25 million to 50 million IDR losses	delay of up to a month	Performance declines by 60-80%.
Very high - 5	Losses > IDR 50 million	Interferens > 1 month	Performance declines by more than 80%

Table 2. Criteria of Likelihood

Level	Criteria of likelihood	
	Occurrence Frequency	Possible Potential Occurrence
Very low - 1	Very rare. Only occurs in extremely abnormal circumstances or once every three years	This occurs only occasionally. likely to occur for a considerable amount of time (over five years)
Low - 2	Rarely occurs. Occurs irregularly or outside of normal circumstances within three years	It only occurs in routine circumstances; the likelihood of it occurring is low. Happens over a significant stretch (under 5 years)
Moderate - 3	Quite often. Under normal circumstances, events occur frequently.	likely to occur under a variety of circumstances. occurs every one to three years
High - 4	Often. Under normal circumstances, the occurrences occur anywhere from six to fifteen times per year, making them quite frequent.	Most likely to occur under a variety of typical circumstances. Occurs within a predetermined time frame (three to twelve months)
Very high - 5	Very often. Between three and five times per month, it always occurs in every incident.	It must always occur under various normal circumstances. Occurs quickly for unusual circumstances (less than three months)

Table 3. Matrix of Risk Assessment

Risk Matrix	Level of Impact				
	1	2	3	4	5
5	M	M	H	VH	VH
4	L	M	H	H	VH
3	L	M	M	H	H
2	VL	L	M	M	M
1	VL	VL	L	L	M

Where VH is very high, H is high, M is moderate, L is low and VL is very low.

Table 4. Risk Acceptance

Likelihood	Impact				
	Very Low	Low	Moderate	High	Very High
Very High	M	M	M	M	M
High	A	M	M	M	M
Moderate	A	M	M	M	M
Low	A	A	M	M	M
Very low	A	A	A	A	M

Where M means mitigate and A means accept.

3.2. Risk Assessment

At this stage of risk assessment, the ISO 31000:2018 guidelines are used, adapted to include the ISO 27005:2018 process.Identification Related to Agile Implementation

First step in risk assessment in risk identification. Based on previous study, the authors identified several risks in terms of agile hazards that can affect project development. Moreover, the author in certain study also identified several risks in some categories that can affect projects [2]. After we conclude all possibilities risks that are related to agile implementation then we confirm which risk is suitable and have already happened in the organization. Table 5 will show all the risks that have been identified related to agile implementation.

Table 5. Risk Related to Agile Implementation

Categories	Issues (Code)
Human resources	Team formation without consideration of required skill level. (R1) Not assigning responsibility clearly (R2) Developers not grasping agile software development (R3) Lack of responsibility, supervision and control (R4)
Development process	Scrum activities taking too long (R5)
Environmental	Low customer involvement (R6) Unclear requirements (R7)
Communication	Communication lag between members (R8)
Agile hazard	Scope creep (R9) Unrealistic expectations (R10) Lack of cooperation (R11)

3.2.2. Risk Identification Related to Information Security

After we identified risks that are related to agile implementation, next we will identify risks that related to information security while developing this application. Based on ISO 27005 and we conduct the same step as the previous section which is we confirm which of that risk that suitable and already happened in the organization. Table 6 will show all the risks related to information security

Table 6. Information Security Risk

Asset	Threats (Code)
Hardware	Unauthorized access from external threat (R12) Damage to the device (R13)
Software	DoS/DDOS attack (R14) Social engineering attack (R15) Unauthorized access (R16) Mistake on segregation of access rights (R17) Failure of system (R18)
Network	Network sniffing (R19)
Information and Data	Data theft from internal parties (R20) Data theft from external parties (R21) Data modification (R22)
Network	Network disruption (R23)
Location	Blackout (R24)

3.2.3. Risk Analysis

After we conduct risk identification in the previous step, then we do risk analysis. In risk analysis, from all the risks that have already been identified, we give score based on the criteria of likelihood and criteria of impact. In this step, to get more accurate information about the likelihood and impact, we conduct interviews with people in the organization that have responsibilities in this field. Table 7 summarize the risk assessment that have done.

Table 7. Risk Assessment

Code	Likelihood	Impact	Risk Level	
R1	1	4	8	Low
R2	1	3	5	Low
R3	2	3	12	Moderate
R4	1	4	8	Low
R5	1	3	5	Low
R6	4	3	18	High
R7	4	3	18	High
R8	1	3	5	Low
R9	2	5	17	Moderate
R10	3	3	15	Moderate
R11	1	3	5	Low
R12	1	4	8	Low
R13	3	4	19	High
R14	4	3	18	High
R15	3	4	19	High
R16	2	3	12	Moderate
R17	1	4	8	Low
R18	1	4	8	Low
R19	2	4	14	Moderate
R20	2	5	17	Moderate
R21	3	5	21	Very high
R22	2	5	17	Moderate
R23	1	4	8	Low
R24	1	3	5	Low

3.2.4. Risk Evaluation

This stage involves evaluating and prioritizing risks based on the previously established criteria. The evaluation process compares the amount of risk identified in the analysis with the risk acceptance criteria defined in the context, in line with XYZ Agency Guidelines Number 6 of 2017, as detailed below.

a. Risks of a very low or very low level are acceptable, and risk mitigation is unnecessary.

b. Risks with moderate level until very high-level risks must be handled to reduce the risk level until the level of risk appetite.

Table 8 shows the evaluation of the risk related to agile implementation and Table 9 shows the evaluation of the risk related to information security.

3.3. Risk Treatment

The results of the risk analysis and evaluation stages showed that 24 risks were identified, consisting of 11 risks related to agile implementation and 13 risks related to information security. According to the results of the risk evaluation of these 24 risks, 13 risks need to be handled because they are outside the organization's risk appetite, while the other 11 risks do not need to be handled because they are within the organization's risk appetite. These risks consist of 5 risks related to agile implementation and 8 risks related to information security.Risk Treatment for Agile Implementation Risks

To determine the handling of the risks that have been selected, the control recommendations for handling risks in this research related to agile implementation are based on several sources. Table 10 summarizes all recommendations regarding risks of agile implementation.

3.3.2. Risk Treatment for Information Security

Next, to determine the handling of the risks that related to information security are based on the information security control standard ISO/IEC 27002:2018. Table 11. Summarizes all recommendations regarding risks of information security.

3.4. Discussion

SiREV will be a crucial asset for XYZ Agency, making it essential to implement risk management to ensure its development using agile methods and its information security. This study used the ISO 31000 and ISO 27005 framework, which outlines the steps for conducting risk management in general and information security risk management process in detail. Based on a study, risk assessment in agile project starts before the beginning of project and before sprint start and later after sprint is executed or during iteration, the activity of risk management is updating risk register that already made in the beginning of the project therefore in this study, the scope of task that author do is made a risk register and do assessment regarding it [16]. The reason for this is because the project has not yet started and that makes the next process regarding updating the risk register during iteration cannot be done.

Table 8. Risk Evaluation Related to Agile Implementation

Code	Risk Level		Risk Appetite
R6	18	High	Mitigate
R7	18	High	Mitigate
R9	17	Moderate	Mitigate
R10	15	Moderate	Mitigate
R3	12	Moderate	Mitigate
R1	8	Low	Accept
R4	8	Low	Accept
R2	5	Low	Accept
R5	5	Low	Accept
R8	5	Low	Accept
R11	5	Low	Accept

Table 9. Risk Evaluation Related to Information Security

Code	Risk Level		Risk Appetite
R21	21	Very high	Mitigate
R13	19	High	Mitigate
R15	19	High	Mitigate
R14	18	High	Mitigate
R20	17	Moderate	Mitigate
R22	17	Moderate	Mitigate
R19	14	Moderate	Mitigate
R16	12	Moderate	Mitigate
R12	8	Low	8
R17	8	Low	8
R18	8	Low	8
R23	8	Low	8
R24	5	Low	5

Table 10. Control Related to Agile Implementation

Code	Risk Level	Recommendation
R6	18	Without the SPO's approval of the selected user stories, project work should not begin. Acceptance criteria should be established for each User Story. During each Run/Emphasis there is a Run Demo/Survey where the work that has been finished is introduced to the client for acknowledgment. [17]
R7	18	User stories are chosen to be included in each Sprint Planning session. The Sprint Backlog ought to be frozen when Sprint Planning is finished. The Product Backlog should contain any modifications made during the Sprint/Iteration. To keep breaking down user stories for the upcoming sprints, regular backlog grooming should be done during a project [17].
R9	17	A type of User Story known as an Epic is typically regarded as high-level, intricate, or incompletely described. During Backlog Grooming or Release Planning sessions, epics should be refined until they are sufficiently detailed to estimate. Before being chosen in a Sprint Planning session, all user stories (requirements) should be estimated and include a Definition of Done. Criteria for an acceptable user story should be included in the Definition of Done by the project team [10], [17].
R10	15	Preceding beginning work, a team estimating game or planning Poker ought to be utilized to gauge the high-need client stories from the Item Build-up to figure out what can be important for the impending run; this will assist with grasping the intricacy and cost of prerequisites [10], [17].
R3	12	During release planning, when the colleagues start to comprehend the extension and content of the Delivery, preparation required for colleagues ought to be distinguished and considered during arranging [17].

Table 11. Control Related to Information Security

Code	Risk Level	Recommendation
R21	21	Implement regular password change procedures and password quality regulations [12]
R13	19	Routine device maintenance and testing of primary and backup devices [12]
R15	19	Improving the implementation of Threat and Vulnerability Management (TVM) such as Monitoring the condition and performance of servers including database servers, application servers using monitoring applications [12]
R14	18	Routine maintenance of firewall devices, IDPS and other network devices and conducting periodic surveys to ensure that newly discovered vulnerabilities are addressed quickly [12]
R20	17	Carrying outreach regarding the dangers of insider threats, such as detecting and preventing insider activities that are suspicious or could endanger information security [12]
R22	17	Restrict access permissions to log files by configuring permissions on log files to append-only so that existing files cannot be modified (immutable) and only new files can be added [12]
R19	14	Strengthening monitoring of network service usage. Network service usage policies need to be consistent with the organization's access control policies [12]
R16	12	Implement regular password change procedures and password quality regulations and Force users to change the default password upon first log-on to the system [12]

The results of risk management showed that 24 risks were identified, consisting of 11 risks related to agile implementation and 13 risks related to information security. According to the results of the risk evaluation of these 24 risks, 13 risks need to be handled because they are outside the organization's risk appetite, while the other 11 risks do not need to be handled because they are within the organization's risk appetite. These risks consist of 5 risks related to agile implementation and 8 risks related to information security. Implementing risk control recommendations is crucial to mitigating risks. Organizations can lessen the impact or decrease the likelihood of an incident by addressing the identified risk scenarios. Table 10 provides an in-depth description of the study's 13 control recommendations and treatment plans. Furthermore, Table 11. which associations can use to address existing dangers

4. Conclusion

SiREV needs risk management in agile implementation to ensure the successful development of this application as well as risk management in information security to ensure the security of its information during development process. As indicated by the most common way of distinguishing and surveying the risks of SIREV, we can infer that 24 risks were recognized, comprising 11 risks connected with agile implementation and 13 risks connected with information security. The results of the risk assessment of these 24 risks indicate that 13 of them must be handled because they are outside the organization's risk appetite, while the remaining 11 risks are within the organization's risk appetite and need not be handled. In future work, it is possible to carry out further research including updating risks throughout the sprint or iteration implementation period, apart from also trying to use other frameworks or standards in implementing risk management using the agile method.

References

[1] Presiden Republik Indonesia. (2018). *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.*

[2] Buganová, K., & Šimíčková, J. (2019). Risk management in traditional and agile project management. *Transportation Research Procedia*, *40*, 986-993. https://doi.org/10.1016/j.trpro.2019.07.138

[3] Lunesu, M. I., Tonelli, R., Marchesi, L., & Marchesi, M. (2021). Assessing the risk of software development in agile methodologies using simulation. *IEEE Access*, *9*, 134240-134258. https://doi.org/10.1109/ACCESS.2021.3115941

[4] Tavares, B. G., da Silva, C. E. S., & de Souza, A. D. (2019). Risk management analysis in Scrum software projects. *International Transactions in Operational Research*, *26*(5), 1884-1905. https://doi.org/10.1111/itor.12401

[5] Elbanna, A., & Sarker, S. (2015). The risks of agile software development: learning from adopters. *IEEE Software*, *33*(5), 72-79. https://doi.org/10.1109/MS.2015.150

[6] Andrat, H., & Jaswal, S. (2015, December). An alternative approach for risk assessment in Scrum. In *2015 International Conference on Computing and Network Communications (CoCoNet)* (pp. 535-539). IEEE. https://doi.org/10.1109/CoCoNet.2015.7411239

[7] Khurana, S. K., & Wassay, M. A. (2023, April). Towards Challenges Faced in Agile Risk Management Practices. In *2023 International Conference on Inventive Computation Technologies (ICICT)* (pp. 937-942). IEEE. https://doi.org/10.1109/ICICT57646.2023.10134188

[8] Rampini, G. H. S., Takia, H., & Berssaneti, F. T. (2019). Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. *Procedia Manufacturing*, *39*, 894-903. https://doi.org/10.1016/j.promfg.2020.01.400

[9] Syihabuddin, A., Suryanto, Y., & Salman, M. (2019). Risk Management in Data Centers Using ISO 31000 Case Study: XYZ Agency. *The 1st STEEEM 2019*, *1*(1), 341-352.

[10] Anes, V., Abreu, A., & Santos, R. (2020, July). A new risk assessment approach for agile projects. In *2020 International Young Engineers Forum (YEF-ECE)* (pp. 67-72). IEEE. https://doi.org/10.1109/YEF-ECE49388.2020.9171808

[11] Peciña, K., Estremera, R., Bilbao, A., & Bilbao, E. (2011, October). Physical and Logical Security management organization model based on ISO 31000 and ISO 27001. In *2011 Carnahan conference on security technology* (pp. 1-5). IEEE. https://doi.org/10.1109/CCST.2011.6095894

[12] SNI ISO_IEC 27005: 2022. (2023).

[13] Recker, J. (2021). *Scientific research in information systems: a beginner's guide*. Springer Nature.

[14] Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). 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 Computer Science*, *161*, 1206-1215. https://doi.org/10.1016/j.procs.2019.11.234

[15] Putra, I. M. M., & Mutijarsa, K. (2021). Designing information security risk management on bali regional police command center based on ISO 27005. In *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)* (pp. 14-19). IEEE. https://doi.org/10.1109/EIConCIT50028.2021.9431865

[16] Zahedi, M. H., Kashanaki, A. R., & Farahani, E. (2023). Risk management framework in Agile software development methodology. *International Journal of Electrical & Computer Engineering (2088-8708)*, *13*(4). https://doi.org/10.11591/ijece.v13i4.pp4379-4387

[17] CMMI Product Team. (2016). A Guide to Scrum and CMMI®: Improving Agile Performance with CMMI. *CMMI Institute*.