

Cybersecurity Supply Chain Risk Management Using NIST SP 800-161r1

Rahmi Aulia Astri^{1*}, Muhammad Jazman², Syaifullah³, Eki Saputra⁴

Fakultas Sains dan Teknologi, Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia

Email: ¹rahmiaulia16@gmail.com, ²jazman@uin-suska.ac.id, ³syaifullah@uin-suska.ac.id, ⁴eki.saputra@uin-suska.ac.id

Email Penulis Korespondensi: rahmiaulia16@gmail.com

Abstract—Supply chain security issues were related to the product life cycle in an information system so it can harm the success of a company. Nowadays, there has been a paucity of analytical and decision-support tools used to analyze security supply chains. The purpose of this research was to determine the maturity level of supply chain risk management so that the research results can provide mitigation and optimize decision support to minimize supply chain risk in a company. The stages of this research started with a literature study, identification of the problem, data collection, and data analysis. Data collection was carried out using a questionnaire with a Likert scale referring to NIST SP 800-161r1. Data analysis was performed using descriptive statistics to describe the maturity level of cybersecurity supply chain risk management. The results showed that the level of maturity in cybersecurity supply chain risk management using NIST SP 800-161 was at level 3, namely the Defined level. These findings provide recommendations for companies to improve the contingency plan aspect because it had a score with the lowest gap, especially in every product change activity carried out in the system.

Keywords: Security; NIST SP 800-161r1; Supply Chain; Risk.

1. INTRODUCTION

The last few decades have seen rapid advances in technology, which are associated with an increase in the global economy. This has also led to intense competition, thereby driving innovation and technological progress[1]. As a result, supply chain risk decision making is more complicated than ever. It is very important to ensure the security of the data exchanged because the risks that may occur are data loss, organizational reputation, and even data theft[2],[3]. To maintain the security of supply chain data, information technology governance is needed to align with strategy, regulate, and control everything related to digital technology to achieve goals with a level of risk that can be measured and mitigated [4].

Looking at the current development of global supply chains, it is very difficult to fully understand the vulnerabilities of supply chains due to the complex structure of enterprises and distribution networks[5]. Component complexity such as too many unique components, supplier complexity such as too many sub-suppliers, then process complexity such as too many steps, and service complexity such as too many outsourced services. Supply chain vulnerabilities pose a threat, namely quality problems such as data falsification and others.

To illustrate the seriousness of the supply chain issue, Department of Defense (DoD) Senators Carl Levin and Senator John McCain reported to an Armed Services committee that there had been infiltration of counterfeit electronic components. Then in 2004 to 2005 there was a supply chain attack in Greece 100 cellphones were illegally tapped [6].

Without effective security processes and practices throughout the system life cycle, intentional or unintentional vulnerabilities can be introduced into the system. The system can then be exploited by an attacker who injects malicious content, retrieves data and gains other benefits. These risks can affect confidentiality, integrity, insertion of counterfeit goods, unauthorized production, tampering, theft, insertion of malicious software and hardware [7].

Various reports acknowledge that supply chain problems pose a real threat[8]. There has been little research done to address supply chain risks. These reports are primarily in the field of information and communication technology (ICT) including the Information Assurance Technology Analysis Center (IATAC) State-of-the-art Report (SOAR) in 2010, and a series of NIST guidelines, namely NIST SP 800-161, NIST 800- 53r4, and NIST IR 7622. The DoD acquisitions office also provides guidance for developing a Program Protection Plan (PPP) and managing supply chain risk throughout the program life cycle[1], [9], [10].

John Boyens (2022) released a NIST publication 800-161r1 to provide guidance to organizations for identifying, assessing, and minimizing supply chain risks. This guide is focused on increasing organizational visibility and control over the practices and procedures used to protect systems throughout their life cycle [11].

NIST publishes several guidelines that address supply chain risk. The high level supply chain risk mitigation measures suggested in their guidelines include due diligence review of suppliers such as software hardware, firmware, services, using trusted shipping and warehousing and using independent analysis and penetration testing.

Research conducted by Andhyka (2022) [12] used the Cobit framework to mitigate risk in the supply chain (supply chain risk management) which found that by conducting this research a maturity result value was obtained which became a scale for developing and improving the performance of the information technology sector in information technology change management. Other research measures supply chain maturity at PT. X using the maturity model to obtain maturity results for each dimension, which will later be used as input to improve the supply chain maturity of the company [13]. Likewise, in the research on maturity level analysis in the application of the audit process using ISO 27001:20113, the results obtained were a low percentage value of 71.12% [14]. Previous research has not been as thoroughly explained as the NIST. NIST has a number of processes for managing organizational security, asset security and protection, physical and environmental protection, a very detailed description of each control is a strength of the NIST 800-161 framework.

The purpose of this study was to determine the maturity level of cybersecurity supply chain risk management. In this study, a problem limitation will be carried out that only focuses on assessing the maturity level of supply chain risk

management. Risk mitigation will be applied after a maturity level analysis is carried out. Maturity level is a process that can illustrate the process flow, stages and steps that are currently underway which are then used as a basis for improving the maturity level, if the maturity value is higher, the more mature and better the supply chain process in the company.

2. RESEARCH METHODOLOGY

2.1 Research Approach

The methodology in this study uses a survey-based quantitative approach. According to Sugiyono (2018) a quantitative approach is a research methodology where data analysis uses numbers, and data collection uses a closed scale. This study used a questionnaire with a Likert scale. The Likert scale is an alternative answer provided in a questionnaire with several ratings/perspectives. The survey was conducted by distributing questionnaires to PT. X in Pelalawan District.

2.2 Research Stages

The stages in this study consisted of the initial stage, the data collection stage, the analysis stage and the completion stage. The flowchart in this study is shown in Figure 1.

a. Initial Stage - Problem Identification

Identification of the problem is the initial stage of the research conducted. Problem identification is carried out to find out the problems that will be analyzed through the methods that will be used. So that the research results are by the research objectives.

1. Literature review

This section seeks relevant references, such as papers, articles, and books that discuss and relate to cybersecurity supply chain risk management using NIST SP 800-161.

2. Field Study

Field studies are carried out by analyzing the conditions of the companies under study and collecting data to be studied.

3. Research Development

Research development was carried out to see the results of supply chain risk management maturity levels in the company.

b. Data Collection Stage - Determination of Maturity Indicators

The determination of maturity indicators is used by companies to evaluate the supply chain using a maturity level of 5 points (0 - 5).

1. Determination of Indicators

The NIST SP 800-161r1 approach is used as a reference guide for the process of measuring the level of supply chain cybersecurity maturity.

2. Questionnaire Preparation

Preparation of the questionnaire is part of the data collection stage by administering the questionnaire. Questionnaires were administered to obtain supply chain risk management cybersecurity analysis.

3. Observation

Observations are made to obtain information and data related to research objects. Observations were made directly to company X to verify data related to the company's general description, company activities, and IT human resources in the company.

4. Interview

The interview process was obtained by directly interviewing IT parties related to cybersecurity supply chain risk management. By conducting interviews, information and data will be obtained regarding the cybersecurity supply chain that exists in the company and problems that may occur will be identified.

c. Analysis Stage

1. Data Processing Using Maturity Level

Questionnaires are used to collect data for measuring maturity levels, and each measurement will have an index value that can be calculated using the formula below.

$$\text{Index} = \frac{\sum (\text{Sum of Answer Value})}{\sum (\text{Questionnaire Question})} \quad (1)$$

Djarmiko's research (2007) shows that the indexing scale and maturity level of the model have a mapping that can be seen in table 1.

Table 1. Maturity Assessment Category

Value Range	Maturity Value	maturity level	Description
0.00 – 0.49	0	Non-Existent	Complete lack of any known processes. The organization doesn't know when a problem occurs.

0.50- 1.49	1	<i>Initial/Ad Hoc</i>	There is evidence that the company recognizes a problem that needs to be solved. An ad hoc method based on individual examples is used to deal with the problem. No formal process management exists. Each procedure is carried out independently of the standard.
1.50 – 2.49	2	<i>Repeatable</i>	To accomplish the task, the same technique has been devised. These conventional practices are not taught or communicated.
2.50 – 3.49	3	<i>defined</i>	procedures have been standardized, collected and communicated through training. However, implementation is left to each individual, so it is very unlikely that irregularities will be detected. Procedures are developed as a form of formulation of existing practices. Processes are created as a way of formalizing techniques that are already in use.
3.50 – 4.49	4	<i>managed</i>	It is possible to test and monitor procedure compliance and take corrective action when processes are not functioning properly. Continuous improvement procedures are carried out. Great job on process implementation. Total automation and simple equipment.
4.50 – 5.00	5	<i>Optimized</i>	The implementation of the procedure has been completed. This is the result of continuous process improvement and measurement of maturity levels within the company. Workflow and information technology are intertwined, and the latter acts as a tool to increase efficiency and effectiveness. The organizational ability to react quickly to market competition has increased.

d. Completion Stage

This stage is carried out by analyzing the supply chain maturity level in the company. And after that, the level of maturity level values that exist in the company will be determined. Maturity level (maturity) is useful to determine the maturity value of the company at what level. So by obtaining a risk mitigation maturity value it will be easy to apply.

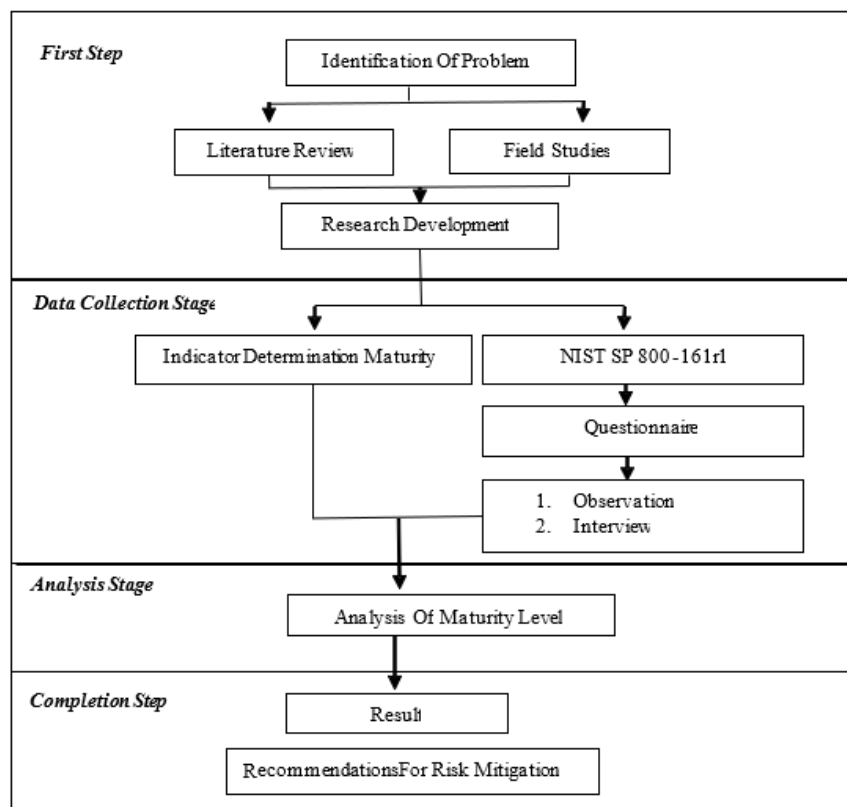


Figure 1. Research methodology

2.3 Cybersecurity Supply Chain Risk Management NIST SP 800-161r1

Information security aims to protect information data from unauthorized access, use, destruction, alteration or destruction to provide confidentiality, integrity and availability. Careful application of information security controls is essential to protect an organization's information assets and its reputation, legal standing, personnel, and other tangible or intangible assets.[15],[16].

A supply chain can be defined specifically in the form of a set of actions involving tools, data, and planning for the transportation and distribution of commodities and services from producers to consumers.[17]. Obtaining raw materials and components, manufacturing, warehousing, inventory recording, documentation, management, ordering,

distribution, communication, transportation and inventory control. Information systems are also needed to ensure that all processes run smoothly, all of which are included in supply chain activities [11].

The act of detecting, measuring and determining hazards, and creating plans to manage them. Risk management in these situations requires procedures, tactics and approaches that assist the project manager in maximizing the likelihood and impact of unfavorable events[18],[19].

NIST (National Institute of Standards and Technology) provides several special publications to provide guidance in conducting system and supply chain risk assessments in organizations [11]. Each stage of the risk assessment process, including planning the assessment, implementing it, delivering results and managing the assessment, is contained in the NIST SP 800-161r1 publication document[20]. NIST SP 800-161 provided a public draft. This draft provides guidance on supply chain management practices for identifying, assessing, and mitigating ICT supply chain risks for federal information systems and organizations. The report proposes a four-stage process in SCRM viz.

1. Sets the context for risk-based decisions and the current state of the supply chain system or environment.
2. Assess, review and interpret threats, vulnerabilities and related information.
3. Respond, select and adapt and apply mitigation controls.
4. Continuously monitor changes to the information system or supply chain environment using organizational communications and feedback for improvement

To address the complexity of supply chain issues the report suggests a three-level risk management approach. The first level starts at the organizational level to set broad strategic objectives. The second level is the business that affects program requirements such as cost, schedule, performance and other utilities[21]. The third level occurs at the information system level which affects system level details such as requirements, design, architecture, development, delivery, installation, integration and maintenance. The “frame” step helps establish assumptions, risk tolerance limits and priority exchanges. The “assess” step gathers available data to carry out a risk assessment[22]. At the assessment stage, criticality analysis, vulnerability analysis, and threats are carried out.

In the context of this report, a vulnerability assessment is performed on a system or component to identify exploitable design, development, production, or operating flaws. In the response step, actionable mitigation control options (based on the assessment step) are implemented to mitigate supply chain risks. Decision makers are provided with alternatives so that the assumptions, constraints, and trade-off tolerances are met as specified in the organizational level analysis. Finally, the "monitor" step allows programs and projects to be regularly evaluated to maintain or adjust risk posture[23].

3. RESULTS AND DISCUSSION

In the product analysis system (SAP) at PT. XYZ collected data, population and general description of respondents, survey assessments, calculation of data table results, and mapping results at the maturity level which became the source of the findings of this study.

3.1 Overview of Respondents

Table 2. Overview of Respondents from IT at PT. X

Based on Position			
No	Position	F	%
1	Chairman	1	16.7
2	Member	5	83.8
Total		6	100.0
Based on Education Level			
1	SMA/SLTA	4	66.7
2	S1	2	33.3
Total		6	100.0
Based on experience			
1	>1 Year	1	16.7
2	15 years	2	33.3
3	>5 Years	3	50.0
Total		6	100.0

Based on table 2, explains that the IT party in company X, totaling 6 people, the majority served as members (83.6%), graduated from high school/secondary school (66.7%), and had experience > 5 years (50.0%). Meanwhile, respondents who came from users had the following characteristics:

Table 3. Overview of Respondents Users at PT. X

Based on Position			
No	Position	F	%
1	Chairman	3	33.3

2	Member	6	66,7
Total		9	100.0
Based on Education Level			
1	SMA/SLTA	4	44,4
2	S1	5	55,6
Total		9	100.0
Based on experience			
1	>1 Year	2	22,2
2	15 years	2	22,2
3	>5 Years	5	55,6
Total		9	100.0

3.2 Questionnaire Assessment

The Likert scale was used to evaluate each respondent's rating, which corresponds to the distribution of answers 1, 2, 3, and 4. In addition, information was collected by distributing questionnaires and scoring using a Likert scale. The following table shows the Likert scale.

Table 4. Likert Scale in Questionnaire

Description	Score
Very Not Good	1
Not good	2
Good	3
Very good	4

3.3 Questionnaire Value Calculation

Table 5. Maturity Level

Process	Σquestion		Σrespondent		Σquestion * respondentΣ		Σscore	Σend	Index
	IT	Users	IT	Users	IT	Users			
AC1	6	5	6	9	36	45	81	210	2.59
AC2	3	5	6	9	18	45	63	150	2.38
AC3	6	2	6	9	36	18	54	151	2.80
AT3	2	5	6	9	12	45	57	160	2.81
AT4	3	3	6	9	18	27	45	119	2.64
AU1	5	5	6	9	30	45	75	192	2.56
CA1	3	5	6	9	18	45	63	152	2.41
CM3	5	4	6	9	30	36	66	196	2.97
CP2	2	4	6	9	12	36	48	128	2.67
IA1	6	10	6	9	36	90	126	327	2.60
IR5	5	10	6	9	30	90	120	276	2.30
MA2	5	8	6	9	30	72	102	257	2.52
PE6	4	5	6	9	24	45	69	183	2.65
PL2	3	5	6	9	18	45	63	151	2.40
PS1	5	5	6	9	30	45	75	176	2.35
RA5	5	5	6	9	30	45	75	217	2.89
Total									41.53
Average index									2.60

From table 5, the results obtained with a maturity value of 2.60 are at the defined level. at this level the implementation is left to each individual, so it is very unlikely that irregularities will be detected. Procedures are developed as a form of formulation of existing practices. Processes are created as a way of formalizing techniques that are already in use.

Table 6. Maturity Comparison with the Target set.

Process	Maturity Level				
	Now	Category	Target	Category	GAP
AC1 <i>Access Control Policies and Procedures</i>	2.59	<i>defined</i>	3.46	<i>defined</i>	0.86
AC2 <i>Account Management</i>	2.38	<i>repeatable</i>	3.73	<i>managed</i>	1.35
AC3 <i>Access Enforcement</i>	2.80	<i>defined</i>	3.48	<i>defined</i>	0.69
AT3 <i>Role-Based Training</i>	2.81	<i>defined</i>	4.84	<i>optimistic</i>	2.04
AT4 <i>Training Records</i>	2.64	<i>defined</i>	4,16	<i>managed</i>	1.51
AU1 <i>Audit and Accountability Policy and Procedures</i>	2.56	<i>defined</i>	3,47	<i>defined</i>	0.91

	Process	Maturity Level				
		Now	Category	Target	Category	GAP
CA1	Assessment and Authorization Policies and Procedures	2,41	repeatable	5,00	optimistic	2.59
CM3	Configuration Change Control	2.97	defined	3.00	defined	0.03
CP2	Contingency Plans	2.67	defined	5,42	optimistic	2.75
IA1	Identification and Authentication Policies and Procedures	2.60	defined	2.66	defined	0.06
IR5	Incident Monitoring	2.30	repeatable	2.68	defined	0.38
MA2	Controlled Maintenance	2.52	defined	3,28	defined	0.76
PE6	Monitoring Physical Access	2.65	defined	3,04	defined	0.39
PL2	System Security and Privacy Plans	2.40	repeatable	3,41	defined	1.02
PS1	Personnel Security Policy and Procedures	2.35	repeatable	3.00	defined	0.65
RA5	Vulnerability Monitoring and Scanning	2.89	defined	4,27	managed	1.37
Total		41.53		58,89		17,36
Average Index		2.60		4		0.40

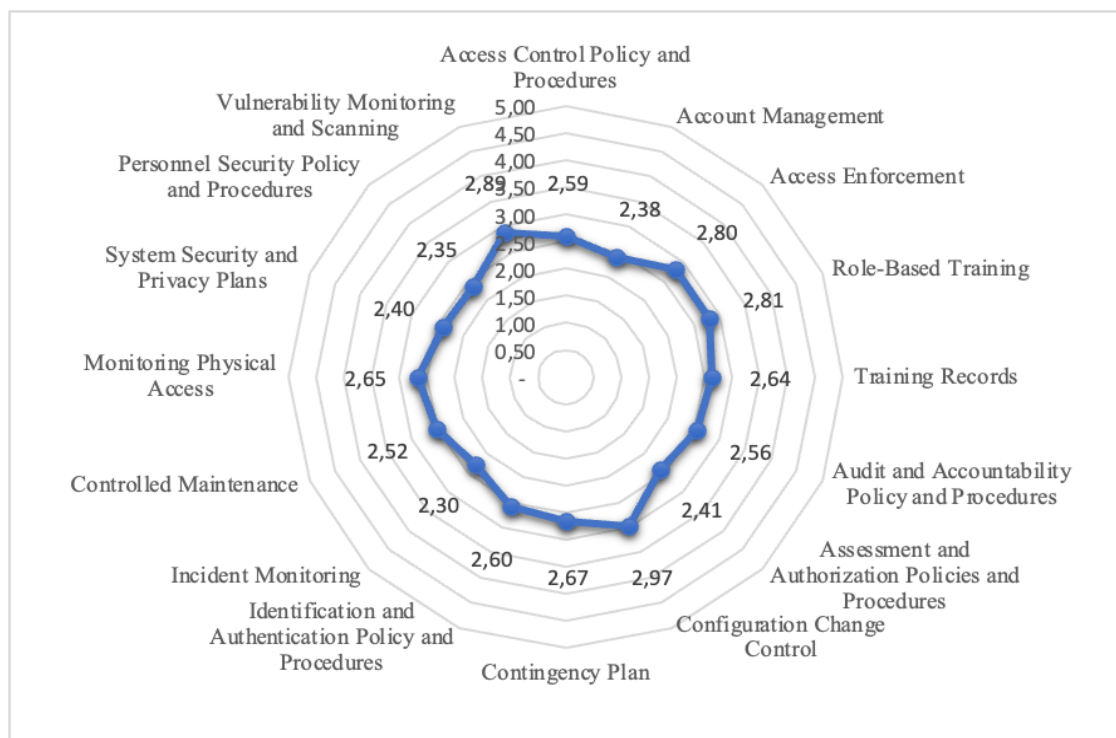


Figure 2. GAP Maturity Based on NIST SP 800-161

Information system at PT. XYZ has a maturity level of 2.60 which is at a defined level, which is lower than the maturity level desired by the organization, namely at managed level 4. as shown in the table above. A GAP of 0.40 can be calculated from this comparison. This can mean that the desired maturity level has not been achieved as expected. The aspect that has the highest gap is in the contingency plan with a score of 2.75 and the lowest gap results in the configuration change control with a score of 0.03 which is an aspect that controls if there are changes in each activity such as approving and tracking if changes occur in the product process. This aspect shows that PT. XYZ has problems with configuration changes in the product process. Configuration change control is usually used to ensure and evaluate changes before proceeding to the next stage. According to Jon Boyens, this aspect shows control of activity configuration changes to manage products to ensure the latest products have been approved and change documentation to control the risk of supplier configuration errors[11].

4. CONCLUSION

From the research results, the maturity value obtained by using NIST SP 800-161 is at level 3, namely the Defined level. Organizations need to consider the features of supply chain security management. This method can be extended to any level of detail available or desired. This representation can be used for visualization using plots (difficulties, consequences). This is suitable for input to the constrained optimizer to determine the most appropriate set of mitigations to apply. This approach can be applied to any supply chain. More generally, this framework can be applied to the analysis of other types of problems by making appropriate modifications to adversary and defender actions and system representations.

REFERENCES

- [1] G.Kaoet *et al.*, "Supply chain lifecycle decision analytics," in 2014 International Carnahan Conference on Security Technology (ICCST), IEEE, 2014, p. 1–7.
- [2] E. McDaniel, M. Albert, B. Cohen, and CJ Ortiz, "Making Smart Decisions About Supply Chain Security in the Age of Globalization," 2017.
- [3] T. Sianturi and K. Ramli, "A Security Framework for Secure Host-to-Host Environments," *J. RESTI System Engineering. And Technol. inf.*, vol. 6, no. 3, p. 380–386, 2022.
- [4] C. Topping, O. Michalec, and A. Rashid, "Contrasting global approaches for identifying and managing cybersecurity risks in supply chains," *ArXiv Prepr. ArXiv220802244*, 2022.
- [5] N. Guangnan, C. Xiaohua, S. Yanmin, W. Hailong, and X. Kefu, "Research on International ICT Supply Chain Security Management with Suggestions," *Strategy. Study Chin. Acad. Eng.*, vol. 18, no. 6, p. 104–109, 2016.
- [6] S. Tweneboah-Koduah and WJ Buchanan, "Security risk assessment of critical infrastructure systems: A comparative study," *Comput. J.*, vol. 61, no. 9, p. 1389–1406, 2018.
- [7] J. Boyens, C. Paulsen, L. Feldman, and G. Witte, "ITL BULLETIN FOR JUNE 2015 INCREASING VISIBILITY AND CONTROL OF YOUR ICT SUPPLY CHAINS".
- [8] "Huawei-ZTE Investigative Report (FINAL).pdf."
- [9] AM Ribbon, "Real-World Cyber Security Challenges in Rail Systems." 2020.
- [10] J. Boyens, C. Paulsen, R. Moorthy, N. Bartol, and SA Shankles, "Supply chain risk management practices for federal information systems and organizations," *NIST Spec. Publ.*, vol. 800, no. 161, p. 32, 2015.
- [11] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," National Institute of Standards and Technology, Oct 2021. doi: 10.6028/NIST.SP.800-161r1-draft2.
- [12] A. Ramadhan, "Analysis of Maturity Level Calculations Using COBIT 2019 Domain BAI06," *FTI*, 2022.
- [13] HN Izzati, I. Baihaqi, and DS Ardiantono, "Measurement of Supply Chain Maturity at PT X," *J.Tek. ITS*, vol. 10, no. 2, p. F197–F202, Dec 2021, doi: 10.12962/j23373539.v10i2.70324.
- [14] E. Riana, MES Sulistyawati, and OP Putra, "Analysis of Maturity Level and PDCA in the Implementation of an Information Security Management System Audit at PT Indonesia Game Using ISO 27001: 2013," *inform. educ. Prof. J. Inform.*, vol. 7, no. 1, p. 39–50, 2022.
- [15] N. Fitrianti Fahrudin, A. Nugraha S, and K. Ramadhan Putra, "Assessment of Employee Data Security Risks in Information Systems Using the Nist Sp 800-30 Framework at PT. A B C," *J. Ilm. Technol. Applied Information.*, vol. 8, no. 3, Aug 2022, doi: 10.33197/jitter.vol8.iss3.2022.900.
- [16] A. Salsabila, "RISK ASSESSMENT TO RECOMMEND SECURITY CONTROL OF ACADEMIC INFORMATION SYSTEMS (SIKAD) CLOUD SERVICE PROVIDER WITH NIST SP 800-30," PhD Thesis, UPN Veteran "Yogyakarta, 2022.
- [17] Y. You, S. Bae, SJ Kim, and DH Kim, "A Study on the Supplementation of the Korea's National Information Security Manual from the Perspective of Cyber Supply Chain Security," *J.Korea Inst. inf. Secur. Cryptol.*, vol. 32, no. 2, p. 309–327, 2022.
- [18] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sep 2020. doi: 10.6028/NIST.SP.800-53r5.
- [19] IPS Syahindra, CH Primasari, and ABP Iriantor, "XYZ PROVINCE DISCOMMINFO INFORMATION RISK EVALUATION USING OUR INDEX AND ISO 27005: 2011," *J. Teknoinfo*, vol. 16, no. 2, Art. no. 2, Jul 2022, doi: 10.33365/jti.v16i2.1246.
- [20] MJ Cotteleer *et al.*, "Cybersecurity Requirements for AM Systems: New Enforcement in DoD Environments, and Resources for Implementation," in the Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, 2021, p. 49–60.
- [21] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013," *NIST Spec. Publ.*, vol. 800, no. 53, p. 10.
- [22] M. Abrams, "Applying NIST SP 800-53 to Industrial Control Systems".
- [23] J. Martínez and JM Durán, "Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study," *int. J. Saf. Secur. Eng. Vol.*, vol. 11, no. 5, p. 537–545, 2021.