CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT MENGGUNAKAN *NIST SP 800-161R1*

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

RAHMI AULIA ASTRI
11950324994

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2023

LEMBAR PERSETUJUAN

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT MENGGUNAKAN *NIST SP 800-161R1*

TUGAS AKHIR

Oleh:

RAHMI AULIA ASTRI
11950324994

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 26 Juni 2023

Ketua Program Studi	Pembimbing
Eki Saputra, S.Kom., M.Kom.	Muhammad Jazman, S.Kom., M.Infosys.
NIP. 198307162011011008	NIP. 198206042015031004

LEMBAR PENGESAHAN

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT MENGGUNAKAN *NIST SP 800-161R1*

TUGAS AKHIR

Oleh:

RAHMI AULIA ASTRI
11950324994

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 20 Juni 2023

Pekanbaru, 20 Juni 2023
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Hartono, M.Pd.	Eki Saputra, S.Kom., M.Kom.
NIP. 196403011992031003	NIP. 198307162011011008

DEWAN PENGUJI:

Ketua : **T. Khairil Ahsyar, S.Kom., M.Kom.**

Sekretaris : **Muhammad Jazman, S.Kom., M.Infosys.**

Anggota 1 : **Syaifullah, SE., M.Sc.**

Anggota 2 : **Eki Saputra, S.Kom., M.Kom.**

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 20 Juni 2023

Yang membuat pernyataan,

RAHMI AULIA ASTRI

NIM. 11950324994

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Assalamu'alaikum Warahmatullahi Wabarakaatuh

Alhamdulillahi Rabbil 'Alamin, segala puji bagi Allah *Subhanahu Wa Ta'ala* sebagai bentuk rasa syukur atas segala nikmat yang telah diberikan tanpa ada kekurangan sedikitpun. Shalawat beserta salam tidak lupa pula kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'ala Sayyidina Muhammad Wa'ala Ali Sayyidina Muhammad*. Semoga kita semua selalu senantiasa mendapat syafa'at-Nya di dunia maupun di akhirat, *Aamiin Ya Rabbal'alaamiin*. Kupersembahkan hadiah istimewa karya kecil ini sebagai salah satu bentuk bakti, rasa terimakasih, dan hormatku kepada orang tuaku tercinta, Ayah dan Ibu.

Ayah dan Ibuku tersayang, terimakasih untuk setiap perjuangan yang kalian usahakan, doa yang selalu kalian berikan disetiap sujud panjangmu, membimbing, mendorong saya dalam kebaikan, dan selalu ada saat keadaan tersulit sekalipun. Terimakasih untuk segala pengorbanan yang kalian lakukan. Sampai kapanpun tiada rasa dan tiada cara yang dapat membalas semua yang telah kalian lakukan. Untuk itu saya anakmu ini selalu mendoakan yang terbaik untuk Ayah dan Ibu agar bahagia dunia dan akhirat, serta diberikan tempat istimewa di sisi-Nya kelak sehingga kita bisa berkumpul kembali bersama-sama di Jannah-Nya.

Terimakasih juga saya ucapkan kepada kakak dan adik yang sangat saya cintai. Terimakasih untuk segala waktu berharga yang telah dilalui bersama, doa, dan dukungan yang tiada hentinya. Terimakasih juga saya ucapkan kepada Bapak dan Ibu Dosen Program Studi Sistem Informasi yang selama ini sudah mewariskan ilmu, motivasi, dan arahan untuk menyelesaikan studi di Program Studi Sistem Informasi ini. Kemudian terimakasih untuk teman-teman seperjuangan yang telah memberikan dukungan dan motivasinya kepada saya. Semoga kita semua selalu diberikan rahmat serta karunia-Nya, dan dilimpahkan kemudahan dengan berlipat ganda. *Aamiin.*

Wassalamu'alaikum Warahmatullahi Wabarakaatuh

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamin, bersyukur kehadirat Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan Tugas Akhir ini. Shalawat serta salam tidak lupa pula kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli 'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Tugas Akhir ini dibuat sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer di Program Studi Sistem Informasi Universitas Islam Negeri Sultan Syarif Kasim Riau.

Pada penulisan Tugas Akhir ini, terdapat beberapa pihak yang sudah berkontribusi dan mendukung peneliti baik berupa materi, moril, dan motivasi. Oleh karena itu, peneliti ingin mengucapkan banyak terimakasih kepada:

1. Bapak Prof. Dr. Hairunas, M.Ag sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Hartono, M.Pd sebagai Dekan Fakultas Sains dan Teknologi.
3. Bapak Eki Saputra, S.Kom., M.Kom sebagai Ketua Program Studi Sistem Informasi sekaligus Penguji II peneliti yang banyak memberikan arahan dan masukan dalam penyelesaian Tugas Akhir ini.
4. Ibu Siti Monalisa, ST., M.Kom sebagai Sekretaris Program Studi Sistem Informasi.
5. Bapak T. Khairil Ahsyar, S.Kom., M.Kom sebagai Kepala Laboratorium Program Studi Sistem Informasi sekaligus Ketua Sidang peneliti yang telah memberi arahan, saran, serta nasihat yang bermanfaat.
6. Bapak Muhammad Jazman, S.Kom., M.Infosys sebagai Dosen Pembimbing peneliti yang telah banyak memberikan arahan, masukan, nasihat, serta motivasinya baik dalam penyelesaian Tugas Akhir, maupun juga dalam perkuliahan dan kehidupan sehari-hari. Setiap motivasi yang diberikan akan selalu peneliti ingat dan dijadikan sebagai pelajaran hidup.
7. Bapak Syaifullah, SE., M.Sc sebagai Penguji I peneliti yang telah banyak memberikan arahan, nasihat, masukan, serta motivasi dalam penyelesaian Tugas Akhir.
8. Bapak Nesdi Evrilyan Rozanda, S.Kom., M.Sc sebagai Dosen Pembimbing Akademik peneliti yang telah banyak memberikan arahan, masukan, dan motivasi selama perkuliahan mulai dari Semester 1 hingga Semester 8 ini.
9. Seluruh Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah banyak memberikan ilmunya kepada peneliti. Semoga ilmu yang diberikan dapat peneliti amalkan dan menjadi amal jariyah.

10. Kedua orang tua peneliti, yaitu Ibu Sulastrianis, S.Pd dan Ayah Ahadi Kontrisman tercinta yang tanpa lelah selalu memberikan semangat, motivasi, dukungan, serta doa terbaiknya dan selalu menjadi motivasi peneliti dalam menyelesaikan studi perkuliahan ini. Terimakasih atas semua pengorbanan dan kerja keras yang telah kalian lakukan dengan penuh keikhlasan demi menuju kesuksesan anakmu ini. Semoga Allah *Subhanahu Wa Ta'ala* selalu menjaga dan melindungi Ayah dan Ibu dimanapun kalian berada.
11. Kakak Rahma Pertiwi, S.Pd dan Adik tercinta terimakasih telah memberikan perhatian, semangat, dukungan, serta doa kepada peneliti.
12. Sahabat-sahabat tercinta peneliti, yaitu Anggi Saputra, Awwalin Nisa, Atikah Haura, Nur Fauziah, Ningtyas Pratiwi, Zizie Atira, Mutiara Rahmadani, Muhamad Irvandra, Ariq Hendrian, Hadiul Bagasta, Umairah Rizkya Gurning, Agisti Mutiara Ayulya, dan Riskina Saputri.
13. Teman-teman seperjuangan *Calm Class* 19 dan KKN Desa Koto Benai 2022.
14. Semua pihak yang namanya tidak dapat disebutkan satu persatu yang telah banyak membantu dalam pelaksanaan serta penyelesaian Tugas Akhir ini.

Semoga segala doa dan dorongan yang telah diberikan selama ini menjadi amal kebajikan dan mendapat balasan setimpal dari Allah *Subhanahu Wa Ta'ala*. Peneliti menyadari bahwa penulisan Tugas Akhir ini masih terdapat banyak kekurangan dan jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangat diharapkan demi kesempurnaan Tugas Akhir ini dan semoga laporan ini bermanfaat bagi kita semua. Akhir kata peneliti ucapkan terimakasih.

Pekanbaru, 26 Juni 2023
Peneliti,

RAHMI AULIA ASTRI
NIM. 11950324994

KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (media online)
Jalan Sisingamangaraja No. 338, Sumatera Utara, Medan
Website https://djournals.com/klik | Email: jurnal.klikbd@gmail.com
Publisher **Universitas Budi Darma**

Medan, 28 Mei 2023

No : 151/KLIK/LOA/V/2023
Lamp : -
Hal : Surat Penerimaan Naskah Publikasi Jurnal

Kepada Yth,
Bapak/Ibu **Rahmi Aulia Astri**
Di Tempat

Terimakasih telah mengirimkan artikel ilmiah untuk diterbitkan pada **KLIK: Kajian Ilmiah Informatika dan Komputer** (ISSN 2723-3898 (media online)), dengan judul:

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

Penulis: **Rahmi Aulia Astri, Muhammad Jazman, Eki Saputra, Syaifullah**

Berdasarkan hasil review, artikel tersebut dinyatakan DITERIMA untuk dipublikasikan pada **Volume 3, Nomor 6, Juni 2023.**

QR-Code di bawah merupakan kode digital sebagai penanda keaslian LOA yang telah dikeluarkan dan akan menuju pada link LOA yang telah dikeluarkan pada Jurnal KLIK.

Sebagai informasi tambahan, saat ini **KLIK: Kajian Ilmiah Informatika dan Komputer** (ISSN 2723-3898 (media online)) telah TERAKREDITASI dengan Peringkat SINTA 4 berdasarkan Surat Keputusan peringkat Akreditasi periode III 2022, dari Kementrian Pendidikan, Kebudayaan, Riset, dan Teknologi, Direktorat Jendral Pendidikan Tinggi, Riset dan, Teknologi No 225/E/KPT/2022, tanggal 7 Desember 2022.

Demikian surat ini kami sampaikan, atas perhatiannya kami ucapkan terimakasih.

Hormat Kami,

Surya Darma Nasution, M.Kom
Ketua Editor

Tembusan:
1. Peringgal
2. Author

Lampiran Surat :
Nomor : Nomor 25/2021
Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini:

Nama : Rahmi Aulia Astri
NIM : 11950324994
Tempat/Tgl. Lahir : Pekanbaru, 08 oktober 2000
Fakultas/~~Pascasarjana~~ : SAINTEK
Prodi : sistem Informasi
Judul ~~Disertasi/Thesis~~/Skripsi/Karya Ilmiah lainnya*:
CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT MENGGUNAKAN NIST SP 800-161 RI

Menyatakan dengan sebenar-benarnya bahwa :

1. Penulisan Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan Disertasi/Thesis/Skripsi/(Karya Ilmiah lainnya)* saya tersebut, maka saya besedia menerima sanksi sesua peraturan perundang-undangan.

Demikianlah Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 04 Juli 2023
Yang membuat pernyataan

Rahmi Aulia Astri
NIM : 11950324994

pilih salah satu sasuai jenis karya tulis

KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 3, No 6, April 2023, Hal 595-601
DOI 10.30865/klik.v3i6.799
https://djournals.com/klik

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

Rahmi Aulia Astri[1*], Muhammad Jazman[2], Syaifullah[3], Eki Saputra[4]
Fakultas Sains dan Teknologi, Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia
Email: [1]rahmiauliia16@gmail.com, [2]jazman@uin-suska.ac.id, [3]syaifullah@uin-suska.ac.id,[4]eki.saputra@uin-suska.ac.id
Email Penulis Korespondensi: rahmiauliia16@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 cyber security 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-ofthe-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.

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

Djatmiko'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	*Initial/Ad Hoc*	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	*Repeatable*	To accomplish the task, the same technique has been devised. These conventional practices are not taught or communicated.
2.50 – 3.49	3	*defined*	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	*managed*	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	*Optimized*	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.

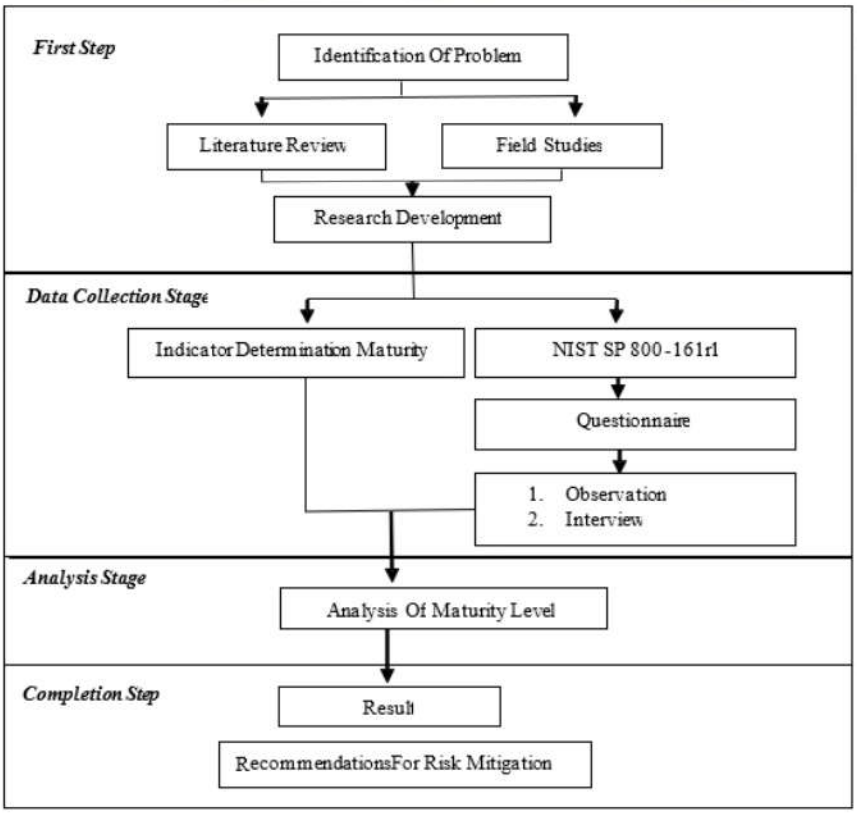

Figure 1. Research methodology

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.

a) Sets the context for risk-based decisions and the current state of the supply chain system or environment.
b) Assess, review and interpret threats, vulnerabilities and related information.
c) Respond, select and adapt and apply mitigation controls.
d) 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	*Access Control Policies and Procedures*	2.59	*defined*	3.46	*defined*	0.86
AC2	*Account Management*	2.38	*repeatable*	3.73	*managed*	1.35
AC3	*Access Enforcement*	2.80	*defined*	3.48	*defined*	0.69
AT3	*Role-Based Training*	2.81	*defined*	4.84	*optimistic*	2.04
AT4	*Training Records*	2.64	*defined*	4,16	*managed*	1.51
AU1	*Audit and Accountability Policy and Procedures*	2.56	*defined*	3,47	*defined*	0.91

Process	*Maturity Level*				
	Now	**Category**	**Target**	**Category**	**GAP**
Assessment and Authorization Policies and Procedures	2,41	*repeatable*	5.00	*optimistic*	2.59
Configuration Change Control	2.97	*defined*	3.00	*defined*	0.03
Contingency Plans	2.67	*defined*	5,42	*optimistic*	2.75
Identification and Authentication Policies and Procedures	2.60	*defined*	2.66	*defined*	0.06
Incident Monitoring	2.30	*repeatable*	2.68	*defined*	0.38
Controlled Maintenance	2.52	*defined*	3,28	*defined*	0.76
Monitoring Physical Access	2.65	*defined*	3.04	*defined*	0.39
System Security and Privacy Plans	2.40	*repeatable*	3,41	*defined*	1.02
Personnel Security Policy and Procedures	2.35	*repeatable*	3.00	*defined*	0.65
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

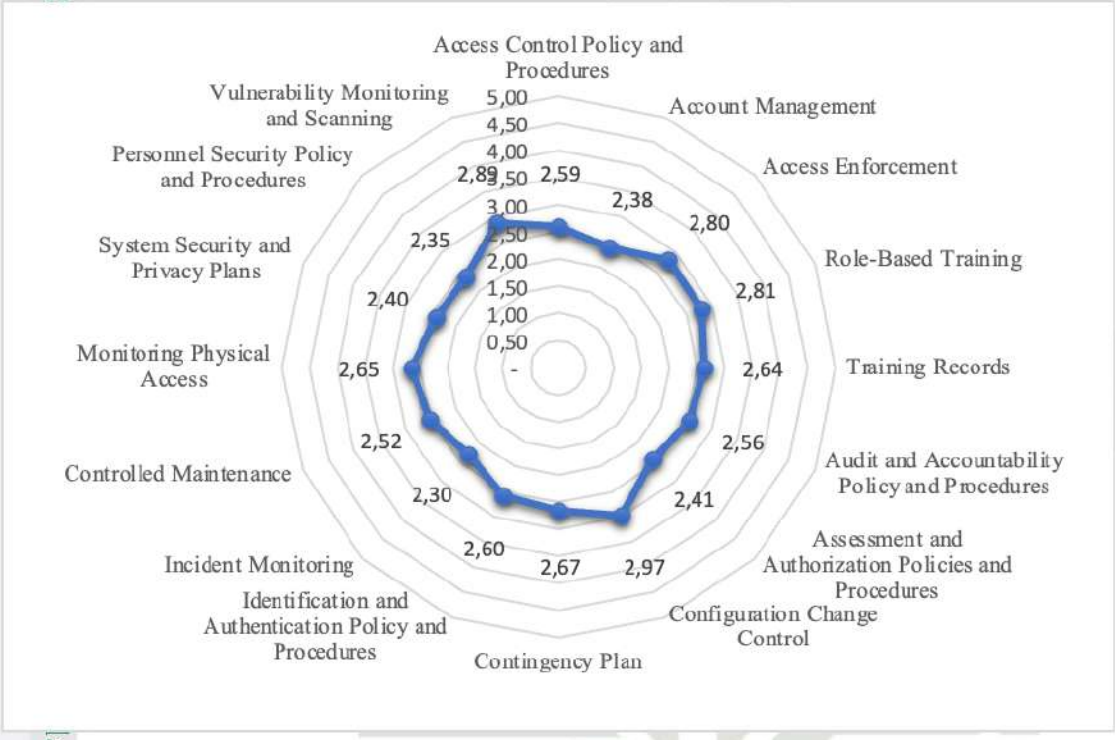

Figure 2. GAP Maturity Based on NIST SP 800-161

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] C.Kaoet *al.*, "Supply chain lifecycle decision analytics," in 2014 International Carnahan Conference on Security Technology (ICCST), IEEE, 2014, p. 1–7.

[2] J. McDaniel, M. Albert, B. Cohen, and CJ Ortiz, "Making Smart Decisions About Supply Chain Security in the Age of Globalization," 2017.

[3] I. 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] J. Topping, O. Michalec, and A. Rashid, "Contrasting global approaches for identifying and managing cybersecurity risks in supply chains,"*ArXiv Prepr. ArXiv220802244*, 2022.

[5] W. 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] E. 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 (SIAKAD) 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 Syalindra, CH Primasari, and ABP Iriantor, "XYZ PROVINCE DISCOMMINFO INFORMATION RISK EVALUATION USING COUR 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.

LAMPIRAN A

KUESIONER

TABLE B- 1: C-SCRM CONTROL SUMMARY

Control Identifier	Control Enhancement Name		Level			
			1	2	3	4
AC-1	*Policy and Procedures*	• Memilih kebijakan kontrol yang mengatasi tujuan, ruang lingkup, peran dan tanggung jawab, komitmen manajemen, koordinasi antar entitas organisasi dan kepatuhan.				
AC-2	*Account Management*	• Menentukan dan mendokumentasikan jenis akun yang diperbolehkan dan secara khusus dilarang untuk digunakan dalam sistem, Memerlukan persyaratan dan kriteria yan ditentukan organisasi untuk keanggotaan akun dan perannya dan Membuat, mengaktifkan, memodfikasi, menonaktifkan, dan menghapus akun sesuai dengan (kebijakan, prosedur kriteria yang di tentukan orfganisasi).				
AC - 3	*Access Enforcement*	• Sistem informasi tidak melepaskan informasi di luar batas sistem yang ditetapkan kecuali penerima komponen sistem atau sistem informasi yang ditentukan menyediakan perlindungan keamanan.				
AT-3	*Role-based Training*	• Memberikan pelatihan keamanan dan privasi berdasarkan peran dan tanggung jawab yang ditentukan oleh organisasi dan memberikan pelatihan mengenai pelangaran keamanan kedalam pelatihan berdasarkan peran dan tanggung jawab.				
AT-4	*Training Records*	• Dokumentasikan dan pantau aktivitas pelatihan keamanan dan privasi informasi, termasuk pelatihan kesadaran keamanan dan privasi berbasis peran dan tanggung jawab.				
AU-1	*Audit and Accountability Policy and Procedures*	• Menunjuk pejabat yang ditentukan organisasi untuk mengelola pengembangan, dokumentasi dan				

		sosialisasi serta membahas tujuan, ruang lingkup, peran, tanggung jawab, komitmen manajemen, koordinasi antar entitas organisasi, dan kepatuhan.				
CA-1	*Assessment and Authorization Policies and Procedures*	• Organisasi melarang koneksi langsung dari sistem keamanan ke jaringan eksternal tanpa menggunakan perangkat perlindungan yang ditentukan oerganisasi.				
CM-3	*Configuration Change Control*	• Menentukan dan mendokumentasikan jenis perubahan pada sistem yang dikontrol konfigurasi, meninjau perubahan yang dikontrol konfigurasi yang diusulkan pada sistem dan setujui atau tolak perubahan tersebut dengan pertimbangan eksplisit untuk analisis dampak keamanan dan privasi dan menyimpan rekaman perubahan yang dokontrol pada sistem selama priode yang ditentukan.				
CP-2	*Contingency Plans*	• Menetapkan situs penyimpanan alternatif termasuk perjanjian yang diperlukan untuk mengizinkan penyimpanan dan pengambilan informasi cadangan sistem informasi dan memastikan bahwa situs penyimpanan alternatif menyediakan keamanan informasi yang setara dengan situs utama				
IA-1	*Identification and Authentication Policies and Procedures*	• Organisasi mengharuskan individu yang mengakses sistem informasi menggunakan teknik atau mekanisme otentikasi tambahan yang ditentukan organisasi di bawah keadaan atau situasi yang ditentukan organisasi				
IR-5	*Incident Monitoring*	• Organisasi mengoordinasikan kegiatan penanganan insiden yang melibatkan peristiwa rantai pasokan dengan organisasi lain				
MA-2	*Controlled Maintenance*	• Organisasi melindungi sesi pemeliharaan dengan memperkerjakan autentikator yang ditentukan organisasi, memisahkan pemiliharaan dari				

		berbagai macam gangguam yang mengakibatkan hilangnya data.				
PE - 6	*Monitoring physical Access*	• Organisasi memperkerjakan keamana yang ditentukan organisasi, menilai keefektifan kontrol keamanan di lokasi dan menyediakan sarana bagi karyawan untuk berkomunikasi dengan personel keamanan informasi jika terjadi insiden atau masalah keamanan				
PL -2	*System Security and privacy Plans*	• Organisasi merencanakan dan mengoordinasikan aktivitas terkait keamanan yang memengaruhi sistem informasi dengan individu atau kelompok yang ditentukan organisasi sebelum melakaukan aktivitas tersebut untuk mengurangi dampak pada entitas organisasi lain.				
PS- 1	*Personel Security Policy and Procedures*	• Melakukan penyaringan individu sebelum mengizinkan akses ke sistem informasi dan menyeleksi ulang individu sesuai dengan kondisi yang ditentukan organisasi				
RA - 5	*Vulnerability Monitoring and Scanning*	• Organisasi melakukan pengecekan secara berkala untuk melihat hasil pemindaian kerentanan				

LAMPIRAN B
HASIL WAWANCARA

Narasumber : Bapak Safriadi

Jabatan : kepala IT

1. Sistem apa yang digunakan untuk mengontrol supply chain di perusahaan ini ?

   Jawab : Nama sistem yang digunakan adalah SAP atau Sistem Analisa Produksi

2. Dari tahun berapa sudah digunakan sistem ini ?

   Jawab : Sistem ini sudah digunkaan dari tahun 2007

3. Apa saja kendala yang terjadi pada sistem tersebut ?

   Kendalanya selama ini terkadang jika sudah bnyak data maka sistem akan melambat, jika membuka file yang sudah lama akan membutuhkan waktu yang lama, jarang adanya update atau pembaruan pada sistem.

4. Apakah pernah terjadi kebocoran data ?

   Jawab : Belum pernah terjadi kebocoran data, tetapi pernah terjadi data tidak normal biasanya akan diberikan notifikasi warning.

5. Apakah pernah terjadi manipulasi data ?

   Jawab : Data akan selalu di closing otomatis disetai akhir bulan maka jika terjadi data upnormal maka sistem akan memberikan notifikasi.

6. Bagaimana keamanan sistem selama ini ?

   Jawab: Kemanan pada sistem kurang kuat karna dengan user sama orang lain dapat masuk tanpa ada notif bahwa ada oang lain yang masuk, keamanan lainya seperti jika tidak digunakan dalam waktu 30 detik sistem akan otomatis log out dan harus masuk ulang dari awal.

7. Siapa saja yang bisa masuk ke sistem tersebut ?

   Jawab : Yang memiliki user dan pass maka akan bisa masuk maka diperlukan seseorang yang dapat dipercaya untuk login ke sistem.

8. Apakah sistem pernah dilakukan audit sebelumnya ?

   Jawab : Belum pernah

9. Jika sistem tidak digunakan dalam waktu yang lama apakah yang terjadi pada sistem ?

   Jawab : Sistem dalam waktu 30 detik akan otomatis keluar

10. Siapa saja yang berwenang yang bisa masuk kedalam sistem ?

    Jawab : Yang berwenang untuk bisa masuk kedalam sistem adalah orang bagian IT

LAMPIRAN C

DOKUMENTASI KEGIATAN

DAFTAR RIWAYAT HIDUP

Rahmi Aulia Astri lahir di Kota Pekanbaru, pada tanggal 08 Oktober 2000. Peneliti merupakan anak dari Bapak Ahadi Kontrisman dan Ibu Sulastrianis. Peneliti merupakan anak kedua dari tiga bersaudara, yang mana Rahma Pertiwi adalah kakak pertama dan Athailah Bil Arzeq adalah adik bungsu peneliti. Pada tahun 2006 peneliti memulai pendidikan dengan masuk TK Pembina Pematang Reba dan lulus pada tahun 2007. Lalu melanjutkan pendidikan Sekolah Dasar di SD Negeri 026 yang ada di Rengat Barat, Kab. Indragiri Hulu. Peneliti menyelesaikan pendidikan Sekolah Dasar pada tahun 2013. Setelah menyelesaikan pendidikan Sekolah Dasar, peneliti melanjutkan pendidikan tingkat SLTP di MTs Negeri Pekanheran yang sekarang sudah berganti nama menjadi MTsN 1 INHU, Indragiri Hulu. Kemudian, setelah 3 tahun menyelesaikan pendidikan di MTsN 1 INHU, pada tahun 2016 peneliti melanjutkan pendidikan tingkat SLTA di SMA Negeri 1 Rengat Barat dengan mengambil jurusan IPA. Setelah menyelesaikan pendidikan di SMA Negeri 1 Rengat Barat, peneliti pun melanjutkan pendidikan dengan mendaftar ke beberapa Universitas yang ada di Indonesia. Singkat cerita, pada tahun 2019 itu peneliti diterima menjadi mahasiswa Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau melalui jalur SBMPTN. Selama menjadi mahasiswa, peneliti mencoba aktif diberbagai kegiatan kampus terutama kegiatan yang ada di Program Studi Sistem Informasi ini. Peneliti juga tergabung dalam Himpunan Mahasiswa Sistem Informasi (HIMASI) pada periode 2021/2022 sebagai Anggota Divisi Sosial, Masyarakat, dan SDM. Akhir kata peneliti mengucapkan rasa syukur yang tak terhingga serta ribuan terimakasih atas bantuan dari seluruh pihak yang terkait sehingga selesainya Tugas Akhir ini yang berjudul *"CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT* MENGGUNAKAN *NIST SP 800-161R1"*.