RISK MANAGEMENT OF INFORMATION SECURITY IN INAPORTNET USING ISO/IEC 27005:2018

TUGAS AKHIR

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

Oleh:

BINTANG RAHMAT RIADI
12050313703

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2025

LEMBAR PERSETUJUAN

RISK MANAGEMENT OF INFORMATION SECURITY IN INAPORTNET USING ISO/IEC 27005:2018

TUGAS AKHIR

Oleh:

BINTANG RAHMAT RIADI
12050313703

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 21 Januari 2025

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

LEMBAR PENGESAHAN

RISK MANAGEMENT OF INFORMATION SECURITY IN INAPORTNET USING ISO/IEC 27005:2018

TUGAS AKHIR

Oleh:

BINTANG RAHMAT RIADI
12050313703

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 17 januari 2025

Pekanbaru, 21 Januari 2025
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 : M. Jazman, S.Kom., M.Infosys

Anggota 1 : Eki Saputra, S.Kom., M.Kom.

Anggota 2 : Mona Fronita, S.Kom., M.Kom.

Lampiran Surat:

Nomor : Nomor 25/2021

Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama	:	Bintang Rahmat Riadi
NIM	:	12150313703
Tempat/ Tgl. Lahir	:	Pekanbaru, 28 Mei 2002
Fakultas/Pascasarjana	:	Sains dan Teknologi
Prodi	:	Sistem Informasi

Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya*:

Risk management of informasion security in Inaportnet using ISO/IEC 27005:2018

Menyatakan dengan sebenar-benarnya bahwa:

1. Penulisan Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya* dengan judul sebagaimana tersebut diatas 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 bersedia menerima sanksi sesuai peraturan perundang-undangan.

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

Pekanbaru, 21 Januari 2025

Yang membuat pernyataan,

METERAI TEMPEL 10000 BAA4EAJX416163492

Bintang Rahmat Riadi

NIM.12050313703

**pilih salah satu sesuai jenis karya tulis*

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 Peneliti 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, 21 Januari 2025
Yang membuat pernyataan,

BINTANG RAHMAT RIADI
NIM. 12050313703

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Alhamdulillahi Rabbil 'Alamiin, 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 tak lupa pula kita ucapkan kepada junjungan dan suri tauladan kita Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Shalli'ala Ali Sayyidina Muhammad*. Semoga kita semua selalu senantiasa mendapat syafaat-Nya di dunia maupun di akhirat, *Aamiin Ya Rabbal'alamiin*.

Dengan penuh rasa syukur dan kebanggaan, Peneliti menyusun Tugas Akhir ini sebagai bagian dari pencapaian akademik Peneliti. Tugas Akhir ini tidak hanya merupakan wujud dari hasil kerja keras dan dedikasi Peneliti selama ini, tetapi juga merupakan bentuk penghargaan dan terima kasih Peneliti kepada kedua orang tua yang telah memberikan dukungan dan kasih sayang yang tiada henti.

Terima kasih ayah, ibu, dan kakakku yang tersayang atas setiap doa, bimbingan, serta dukungan semangat yang telah kalian berikan kepada Peneliti selama penelitian ini. Peneliti selalu mendoakan yang terbaik untuk ayah, ibu, dan kakak Peneliti semoga Allah *Subhanahu Wa Ta'ala* selalu menjaga mereka di mana pun berada, bahagia dunia akhirat, serta diberikan tempat istimewa di sisi-Nya sehingga kita bisa berkumpul kembali bersama-sama di *Jannah*-Nya.

Peneliti ucapkan terima kasih kepada Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah mewariskan ilmu yang bermanfaat dan arahan kepada Peneliti untuk menyelesaikan studi di Program Studi Sistem Informasi ini serta teman-teman yang selalu memberikan dukungan, semangat dan inspirasi kepada Peneliti. Semoga kita semua selalu diberikan kemudahan, rahmat, serta karunia-Nya. *Amiin*.

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamiin, bersyukur kehadirat Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan Tugas Akhir ini dengan baik dan tepat waktu yang berjdulul "*Risk Management of Infomartion Security in Inaportnet Using ISO/IEC 27005:2018*". *Shalawat* serta salam Peneliti ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Shalli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Tugas Akhir ini dibuat sebagai salah satu syarat untuk mendapatkan gelar Sarjana Komputer di Program Studi Sistem Informasi Fakultas Sains dan Teknologi 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. Peneliti ingin mengucapkan banyak terima kasih kepada:

1. Bapak Prof. Dr. H. 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 serta Dosen Penguji I Peneliti yang telah memberikan arahan, masukan, dan nasihat dalam perkuliahan, serta penyelesaian Tugas Akhir ini.
4. Ibu Siti Monalisa, ST., M.Kom sebagai Sekretaris Program Studi Sistem Informasi.
5. Bapak M. Jazman, S.Kom., M.Infosys sebagai dosen pembimbing Tugas Akhir ini serta Dosen Pembimbing I Peneliti yang telah banyak memberikan arahan, masukan, dan nasihat dalam perkuliahan, serta penyelesaian Tugas Akhir ini.
6. Bapak T. Khairil Ahsyar, S.Kom., M.Kom sebagai Kepala Laboratorium Program Studi Sistem Informasi dan sebagai Ketua Sidang Peneliti yang telah banyak memberikan arahan, masukan, dan nasihat dalam perkuliahan, serta penyelesaian Tugas Akhir ini.
7. Ibu Mona Fronita, S.Kom., M.Kom sebagai Dosen Penguji II Peneliti yang telah memberikan arahan, masukan, serta nasihat dalam penyelesaian Tugas Akhir ini.
8. 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*.

9. Seluruh Pegawai dan Staf Fakultas Sains dan Teknologi yang telah membantu dan mempermudah proses administrasi selama perkuliahan ini
10. Keluarga tercinta Ayahanda Fitriadi, Ibunda Yusra, Chintia Deva Rianti, M.Si, dan Fhajril Isqhifari, S.TP yang selalu mendoakan dan terus memberi semangat kepada Peneliti.
11. Kakanda Ipan, Bagas, Rojak, Awi, Pujok, dan Ariq yang sudah memberikan arahan selama masa perkuliahan.
12. Teman-teman seperjuangan yakni Kost Waqaf dan SOS yang selalu mendukung dan menyemangati Peneliti.
13. Semua pihak yang namanya tidak dapat disebutkan satu-persatu yang telah banyak membantu dalam menyelesaikan penelitian Tugas Akhir.

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 banyak terdapat kekurangan dan jauh dari kata sempurna. Untuk itu, kritik dan saran atau pertanyaan dapat diajukan melalui *e-mail* 12050316613@students.uin-suska.ac.id. Semoga laporan ini bermanfaat bagi kita semua. Akhir kata Peneliti ucapkan terima kasih.

Pekanbaru, 21 Januari 2025

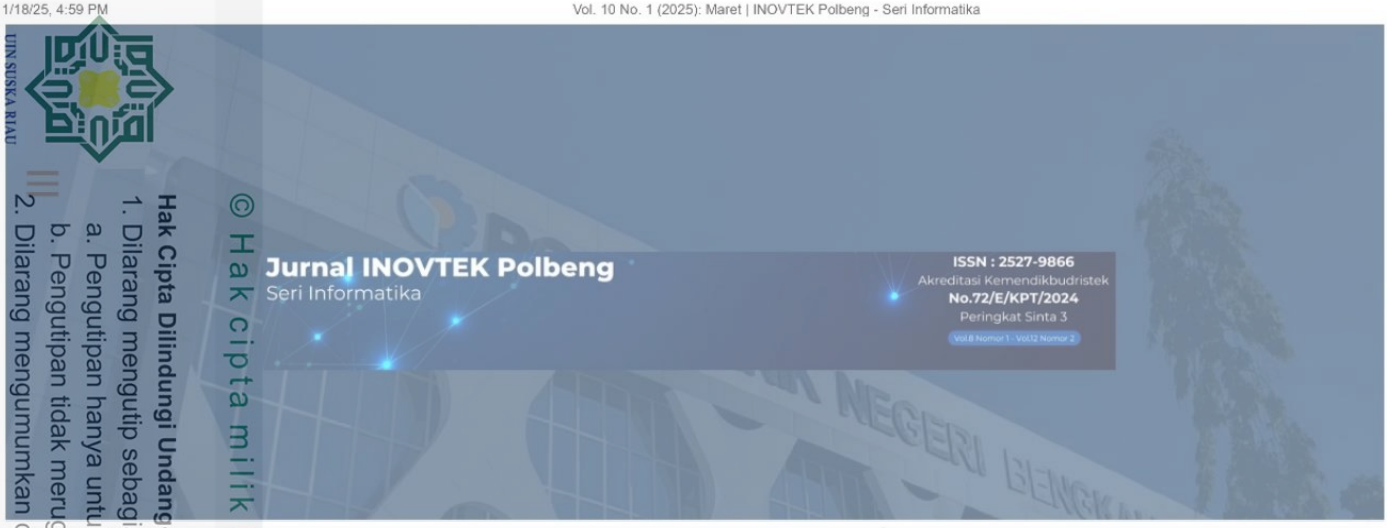
Peneliti,

BINTANG RAHMAT RIADI
NIM. 12050313703

Vol. 10 No. 1, Maret 2025 ISSN: 2527-9866

Jurnal Inovtek Polbeng
Seri Informatika

Jurnal Inovtek Polbeng Seri Informatika | Halaman 1 - 194 | ISSN 2527-9866



Vol. 10 No. 1 (2025): Maret

PUBLISHED: 30-03-2025

Articles

PDF

Analysis Of Acceptance Ond Use Of QRIS Payment Method Using The Utaut-3 Model

Atha Kurniawan, Muhammad Jazman, Mona Fronita, Tengku Khairil Ahsyar (Author)

191-20

PDF

Redesign Of User Experience In Inaportnet Using The User Experience Questionnaire Method TND User-Centered Design

muhammad irvandra irvan, muhamad Jazman jazman, Eki Saputra Eki, Syaifullah, Tengku Khairil Ahsyar (Author)

PDF

Development Of Automatic Waste Classification System Using CNN-Based Deep Learning To Support Smart Waste Management

Lintungan Stephen Pieters (Author)

PDF

Risk Management Of Information Security In Inaportnet Using ISO/IEC 27005:2018

Bintang Rahmat Riadi (Author)

PDF

Sentiment Analysis Of Gojek, Grab, Maxim Applications Using Support Vector Machine Algorithm

Muhammad Iqrom, M. Afdal, Rice Novita, Medyantiwi Rahmawita, Tengku Khairil Ahsyar (Author)

PDF

Analysis Of Service Quality On User Satisfaction Using The E-Servqual, IPA And CSI Methods

Cipta Julian Trivani (Author)

PDF

Development Of A Mobile Web-Based Food And Beverage Ordering Application In AYouth Cafe With QR Code Technology

Aqilla Faradila A.Sagaf, Ichsan Ibrahim (Author)

PDF

Adaptive Dynamic Activity Mapping: A Novel Approach To Real-Time Heatmap With YOLOv8

M. Nursiyanto, Mrs. Dona Yuliawati, Anggi Andriyadi (Author)

271

Analysis Of User Satisfaction With The Mnet Plus Application Using The End-User Computing Satisfaction Method

Gunawan Witjaksono, Nanda Silva (Author)

283

PDF

RISK MANAGEMENT OF INFORMATION SECURITY IN INAPORTNET USING ISO/IEC 27005:2018

Bintang Rahmat Riadi[1], Muhammad Jazman[2], Eki Saputra[3], Mona Fronita[4], Tengku Khairil Ahsyar[5]
[1,2,3,4,5] Universitas Islam Negeri Sultan Syarif Kasim Riau, Jl. HR. Soebrantas No. 155 Km. 15, Panam
email: 12050313703@students.uin-suska.ac.id[1], jazman@uin-suska.ac.id[2], eki.saputra@uin-suska.ac.id[3], monafronita@uin-suska.ac.id[4], tengkukhairil@uin-suska.ac.id[5]

Abstract - This study aims to analyse information security risks in the Inaportnet system at the Port Authority Class II Tanjung Buton using the ISO/IEC 27005:2018 standard. The system is a digital innovation designed to expedite port services but faces significant challenges in information security. The first step involved identifying assets within the Inaportnet system, followed by recognizing potential threats and vulnerabilities associated with these assets. This process is crucial as it lays the groundwork for understanding where risks may arise. The research employs the Failure Mode and Effects Analysis (FMEA) method to identify, assess, and prioritise risks based on assets, threats, vulnerabilities, and existing controls. A total of 17 risks were identified, categorized from "very low" to "low" priority levels. The highest risk involves operational disruption due to sudden power outages, with an RPN score of 72. This study proposes risk mitigation recommendations, including Systems connected to the internet that are vulnerable to cyberattacks, such as hacking or malware, which can result in data theft or service disruptions. Therefore, it is essential to implement firewalls and intrusion detection systems to safeguard the network against external threats. The findings provide practical guidance for improving the information security and operational reliability of the Inaportnet system. By implementing these mitigations, the Port Authority is expected to enhance the reliability of port services and protect critical information.

Keywords - Risk Management, Information Security, Inaportnet, ISO/IEC Standard 27005:2018, FMEA.

I. INTRODUCTION

Risk management is a systematic process for identifying, studying, and managing risks that can affect the achievement of an organization's objectives. Risks can be financial, operational, strategic, or threats to sustainability. In this context, risk management becomes an important instrument for the continuity of the organization's operations and increasing stakeholder confidence. By managing risks proactively, organizations can reduce potential losses and take advantage of opportunities that may arise.[1].

In the context of port operations, which serve as gateways for goods between countries, risk management plays a crucial role in ensuring the smooth flow of activities at the port. Ports themselves require agency service companies responsible for preparing facilities before a ship's arrival and providing assistance while the ship is at the port, in accordance with the regulations applicable to each port[2]. Inaportnet is an internet-based system used in Indonesia for managing ship services, including arrival and departure clearances, as well as loading and unloading activities. It allows shipping companies and stevedoring firms to submit service requests online, reducing the need for in-person interactions with government officials[3]. This system aims to expedite customs processes and ship docking, contributing to increased port operational speed. However, challenges remain, such as inadequate user training and internet

connectivity issues, which hinder the system's optimal performance. Additionally, many agents have yet to fully understand how Inaportnet operates, resulting in inefficiencies in service delivery[4].

Compared to other port systems, such as Portbase in the Netherlands, Inaportnet demonstrates room for improvement, particularly in terms of operational efficiency and security measures [5]. Recommendations for enhancing the Inaportnet system include integrating features from Portbase, which could improve its reliability and operational efficiency. While this system shows great potential for enhancing port performance, further improvements are needed, particularly in user training and system strengthening, to maximize its full potential[6]

System security is a crucial factor in increasing user trust in Inaportnet. Research shows that, although security factors have not yet had a significant impact on user satisfaction, they remain essential for ensuring long-term system reliability and acceptance[7], Security measures implemented in the intranet system, such as point-to-point tunnelling, the use of digital certificates for access control, and the application of virtual IP addresses, can strengthen the reliability and security of the system. These steps are expected to enhance the user experience and, in turn, improve their satisfaction with the system[8].

In order to improve information security risk management, the ISO 27005:2018 standard is used to identify security risks within information systems at ports. Based on ISO 27001, port organizations or authorities can assess risks and design necessary policies and specifications based on the results of the risk identification and assessment process[9]. Many users lack adequate training on how to use Inaportnet effectively, leading to inefficiencies and potential errors in service requests. This knowledge gap can exacerbate operational risks. By implementing ISO/IEC 27005:2018, stakeholders can systematically address vulnerabilities in Inaportnet, thereby enhancing its reliability and security while fostering greater user trust in the system[10]. This risk assessment is expected to provide an overview of the risks associated with the information system assets at the Port Authority and Harbor Master Office of Tanjung Buton Class II, as well as the readiness of these assets to face potential risks. Therefore, it is hoped that this will lead to the development of mitigation plans and improvement recommendations to strengthen security within the institution.

II. SIGNIFICATION STUDY

Risk management

Risk management is a series of processes that involve identifying risks, analyzing them to determine the potential impact on the organization's business processes, and developing actions or protocols to reduce the impact of risks to a level that is acceptable or tolerable for the organization.[11]. An organization cannot determine security controls in the implementation of an Information Security Management System (ISMS) without risk management, as security controls are the most crucial aspect in the planning of an ISMS. [12].

Information Security Management System (ISMS)

In providing and ensuring information system protection, the ISO 27000 family, specifically ISO 27001 and ISO 27002, provides control objectives, specific controls, requirements, and

guidelines that organizations applying these standards can use to achieve a certain level of information security[14]. ISO 27001 provides guidelines for implementing an Information Security Management System (ISMS) and serves as a framework for obtaining international certification from a third party. Unlike ISO 27002, which also outlines detailed guidelines for implementation within an organization, ISO 27001 describes the system as an overall business risk management approach. This management system means that information security must be planned, implemented, monitored, reviewed, and improved. The goal of ISMS is to minimize the level of risk generated as a result of data and information exchange, processing, storage, traffic, and disposal[15].

Inaportnet

Inaportnet is an internet-based/Web Service system related to the services for the arrival and departure of ships, as well as their loading and unloading activities. This system is designed so that service users (Shipping Companies and Stevedoring Companies) can submit service requests, often referred to in the maritime industry as clearance in/out, for ship arrivals and departures, as well as the Loading and Unloading Activity Plan for cargo on board, without the need to visit government offices for clearance. It also minimizes face-to-face interactions between service users and the authorized government officials[16].

ISO / IEC 27005: 2018

ISO/IEC 27005 is a standard applicable to all types of organizations, including companies, government agencies, and non-profit organizations. This standard covers the description of information security management processes and their associated activities. Risks will always threaten the integrity of information security, which is why the information held by an organization must be protected and secured, as it holds value and is considered an asset. To maintain the security of information within an organization, standardization in handling and risk management is required. [17]. The distinctive difference between ISO/IEC 27005 and ISO/IEC 27001 and 27002 is that ISO/IEC 27005 focuses on risk analysis, while ISO/IEC 27001 and ISO/IEC 27002 provide more detailed guidance on the planning, implementation, and operation of security controls.[18]. The illustration of the information security risk management process using ISO/IEC 27005:2018 can be seen in the following image.

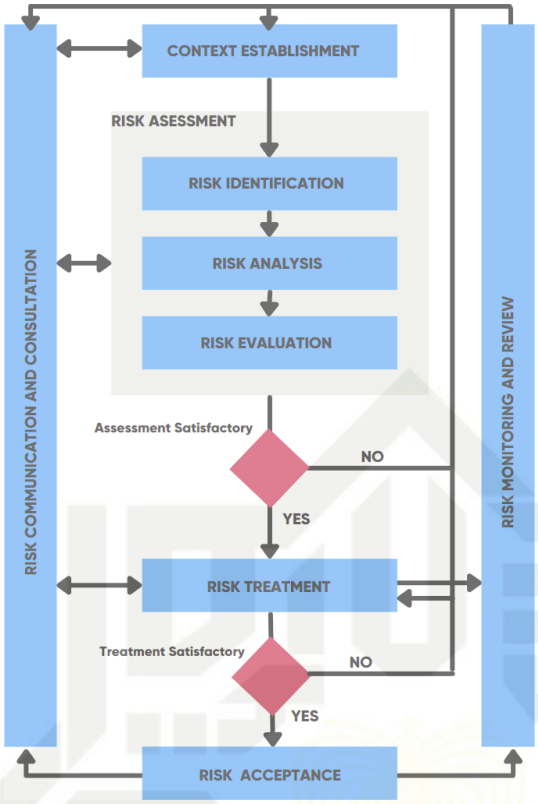


Figure 1. The illustration of the process in ISO/IEC 27005:2018

FMEA

FMEA (Failure Mode and Effects Analysis) is a technique used to identify, prioritize, and reduce defects that may arise from a system, design, or process before reaching the end user or customer. In other sources, it is mentioned that FMEA is a technology designed to identify potential failure modes in a process before they occur. In other words, FMEA is a structured procedure for identifying and preventing as many failure modes as possible. A failure mode refers to anything that constitutes a defect or failure in design, conditions outside the specified or established standards, or changes in the product that disrupt its functionality.[19]. The issues faced by Inaportnet include operational disruptions, with the most critical failure highlighted being operational interruptions caused by sudden power outages. This indicates that the current protocols are insufficient to address this vulnerability, leading to potential service disruptions.

This study aims to produce actionable recommendations to mitigate identified risks, particularly those related to operational disruptions and cybersecurity threats. By proposing specific measures, such as the implementation of firewalls and intrusion detection systems, this research seeks to enhance the overall security posture of Inaportnet. Implementing an effective risk management strategy fosters greater confidence among stakeholders, including shipping companies, government officials, and customers. When stakeholders perceive that the Inaportnet system is secure and reliable, their confidence in port operations increases. This trust can lead to stronger partnerships, increased business opportunities, and a better reputation in the maritime industry.

In defining a risk, we need a context establishment process, within which there are several sub-processes, including Risk Evaluation Criteria, Impact Criteria, and Risk Acceptance Criteria. In general, as explained in the ISO/IEC 27005:2018 document, context establishment requires information about case studies. Therefore, context establishment can be done in conjunction with the interview process with informants and can receive information from informants regarding the context that is already applicable in the case study[20]. One of the crucial phases in this research, is where several activities will be carried out, including asset identification and inventory in the case study, identification of threats to the assets in the case study, and also identification of vulnerabilities present in the case study. This phase will process and further analyze what has been produced in the previous phase (Risk Identification). In this phase, the analysis will be based on the list of threats that have been previously identified for the existing assets. Risk evaluation, in broad terms, is the phase where the risk value calculation is performed and the priority of the risks is determined. To perform the calculation and prioritize the risks, it will refer back to the Context Establishment, assisted by FMEA (Failure Modes and Effects Analysis). Risk Acceptance, or in English, Risk Acceptance, aims to assess whether the risks that have been identified or have undergone treatment are acceptable. If a risk is still deemed unacceptable (treatment is not yet appropriate), it will be returned to the Risk Identification phase.

III. RESULT AND DISCUSSION

Chapter 4 delves deeply into the identification of assets within the Inaportnet system at the Class II Port Authority of Tanjung Buton, establishing a solid foundation for understanding potential risks and vulnerabilities. This meticulous identification process sets the stage for subsequent risk analysis and mitigation strategies, guided by the principles outlined in ISO/IEC 27005:2018. By comprehensively listing main and supporting assets, this chapter lays bare the critical elements requiring protection, thus informing targeted risk management approaches to bolster operational reliability and information security within the Inaportnet. Identification of assets in the Inaportnet system at the Class II Tanjung Buton Port Authority is very important because it is the basis for understanding potential risks and vulnerabilities that can affect operational efficiency and information security.

Table 1. Identification *Asset*

No	Asset	type Asset
1	Website inaportnet Kesyahbandaran Kelas II Tanjung Buton	Primary asset
2	PC (6 unit)	Supporting asset
3	Routers	Primary asset
4	Switch Hub	Primary asset
5	Firewall	Supporting asset
6	Rack Network	Supporting asset
7	IBM X3950 M2	Supporting asset
8	UPS	Supporting asset

9	Storage Server	Supporting asset
10	Database Server	Supporting asset
11	Macbook air	Supporting asset
12	Leptop ASUS Vivobook 15 A1504VA	Supporting asset
13	HP 14 inch Laptop 14s-dq5568TU	Supporting asset
14	Print	Supporting asset

The process of identifying threats to security assets previously identified is carried out by combining information from sources with the threat profile of security assets at the Kesyahbandaran dan Otoritas Kelas II Tanjung Buton.

Table 2. Identification *Threat*

No	Seciurity assets	Threat	Causes of Threats	Sources of Threats
1	Website inaportnet Kesyahbandaran Kelas II Tanjung Buton.	Service Not Running	The application is experiencing an error/unable to be accessed as the troubleshooting process is taking longer than expected.	1. Technician 2. Website Development
2	PC	Slow and Error PC	The PC is infected with a virus	Virus
3	Windows 7	Not functioning as expected	There is a virus on the PC	Virus
4	Daya Listrik	Power outage	A sudden power outage	1. Technician 2. Source power
5	UPS	The battery in the UPS is unable to store power	The UPS is unable to support the power load of the hardware devices	Technician
6	Database Server	The website and database server do not have standard security configurations	Unauthorized access is being made to modify the configuration on the database server	1. Teknisi 3. Pengembangan Website 2. Hacker
7	Firewal	The service is not running Weak password or using the default password	There is a policy that limits the application Modifying configurations that do not comply with standards by unauthorized parties	1. Teknisi 2. Source Power Hacker

Threat identification is a crucial step in the risk analysis process. Risk identification should also be carried out in accordance with the applicable standard, namely ISO/IEC 27005:2018. By identifying threats, it will be easier to determine the potential risks that may occur.

Identification Existing Control

The existing controls identified within the Inaportnet system are essential for safeguarding the assets at the Class II Port Authority of Tanjung Buton, ensuring that security measures are effectively implemented to mitigate potential riks. It is done to avoid repetitive work or unnecessary costs, such as in the duplication of controls. Additionally, while identifying existing controls, checks should be carried out to ensure that the controls are functioning properly.

Table 3. Identifacation Existing Control

No	Asset	Details
1	Website inaportnet Kesyahbandaran Kelas II Tanjung Buton.	1. Install Antivirus 2. Update Antivirus 3. Create privileges user 4. Only a few personnel have access rights to the server and data center
2	PC	1. Install Antivirus 2. Update Antivirus 3. Internet access is not permitted, and only access to the Inaportnet website server is allowed 4. Installing illegal programs is not allowed
3	UPS	Conduct regular checks on the battery and electrical voltage.
4	Database Server	1. Establishing standard information security configurations 2. Implement security configuration standards above existing standards 3. Implement DRP
5	Firewall	Conduct a review of configurations and policies

Identifying Existing Controls is also one of the steps defined by the ISO/IEC 27005:2018 standard. The table above outlines the existing risks associated with each asset.

The discussion of the risk identification results is based on the list of threats previously identified for existing assets. In this table, the risks are formed based on the threats and causes that have been previously determined through interviews with sources.

Table 5. List of Threat Scenarios for the Website and Assets of the Kesyahbandaran dan Otoritas Kelas II Tanjung Buton

Threat Scenario Number	issues
1	Lack of control over Hardware that could lead to troubleshooting, causing disruption in data input
2	Lack of control over software that could lead to troubleshooting, causing disruption in data input
3	The login password for the Inaportnet website of the Tanjung Buton Class II Port Authority is still the default and too easy
4	The electrical supply is unstable in the environment of the Tanjung Buton Class II Port Authority and Harbormaster Office
5	Lack of security, leading to a virus on the computer that runs the Inaportnet website of the inaportnet Kesyahbandaran Kelas II Tanjung Buton

6	Slow loading occurs when accessing the Inaportnet website of the inaportnet Kesyahbandaran Kelas II Tanjung Buton
7	No updates or antivirus installation on the computer devices
8	The absence of a policy regarding access rights usage on the Inaportnet website of the inaportnet Kesyahbandaran Kelas II Tanjung Buton
9	Lack of understanding regarding the confidentiality of data on the Inaportnet website of the inaportnet Kesyahbandaran Kelas II Tanjung Buton, as well as the IP address network configuration
10	Lack of maintenance on outdated computer devices that need upgrading
11	Many users are accessing Inaportnet because there are no restrictions, making it easily accessible to unauthorized individuals
12	Lack of regular maintenance for the operating system (OS) in Kesyahbandaran dan Otoritas Kelas II Tanjung Buton
13	The default firewall configuration has not been adjusted
14	The network configuration has not been adjusted
15	The lack of human resources (HR) at the Kesyahbandaran dan Otoritas Kelas II Tanjung Buton.
16	There is an issue with the network connection being lost on the computer devices
17	A sudden power outage causes the website process to stop

The table above provides information on the causes or reasons why a threat can actually occur. By understanding the causes, it will certainly help determine the appropriate mitigation steps to be taken

In this stage, data from the risk, threat, and vulnerability lists were combined and assessed using the Failure Mode and Effects Analysis (FMEA) method. The assessment was categorized into three parts: severity, occurrence, and detection. These three assessments were then used to calculate the Risk Priority Number (RPN). The following is the result of the assessment conducted by the author using the FMEA method.

Table 6. RPN Value

Threat Scenario Number	Occurence	Severity	Detection	RPN
1	1	2	3	6
2	1	2	4	8
3	2	3	4	24
4	2	4	5	40
5	1	3	3	9
6	1	3	4	12
7	1	5	5	25
8	1	4	3	12
9	1	3	3	9
10	1	4	3	12
11	1	2	4	8
12	1	4	2	8
13	1	2	3	6
14	1	4	2	8
15	1	3	4	12
16	1	3	5	15
17	2	6	6	72

The column headings in the table above begin with a number, followed by the asset name, risk ID, occurrence value, severity value, detection value, and finally the RPN value. The RPN (Risk Priority Number) presented in the table is calculated by multiplying the occurrence, severity, and detection values. A higher RPN indicates a higher priority risk.

After the assessment and calculation of the RPN are completed, the next step is to establish preventive or mitigation actions for these risks. This is mandatory to enhance the credibility of the mitigation plan. The table below shows the results of risk mitigation based on the RPN values from the previous section:

Table 5. Risk Mitigation

Threat Scenario Number	RPN	Category	Mitigation Measures
1	6	Very Low	Use software to monitor hardware health, such as processor temperature, memory usage, and hard drive performance
2	8	Very Low	Perform regular backups of data and software configurations to ensure quick recovery in case of disruptions
3	24	Low	Use a minimum of 8 characters for passwords and ensure that no common words or easily guessed personal information are used
4	40	Low	Install an UPS (Uninterruptible Power Supply) for critical devices such as servers, routers, and other network equipment to ensure they continue to receive power even during electrical disruptions
5	9	Very Low	Ensure that the antivirus is regularly updated to protect devices from the latest threats.
6	12	Very Low	Monitor network performance in real-time to detect potential issues, such as high latency or limited bandwidth
7	25	Low	Ensure that every computer used to access or manage Inaportnet is equipped with trusted and up-to-date antivirus software
8	12	Very Low	Ensure that users understand their responsibilities regarding data access
9	9	Very Low	Use a firewall to restrict network access only to trusted IP addresses
10	12	Very Low	Upgrade the most impactful components, such as adding more RAM, replacing the hard drive with an SSD, or upgrading the processor if possible
11	8	Very Low	Ensure that only verified users are allowed to access the system
12	8	Very Low	Perform a backup of important data before each OS update to prevent data loss in case of failure during the update process
13	6	Very Low	Adjust firewall rules based on the specific needs of the network, such as restricting access to certain ports and allowing only trusted IP addresses

14	8	Very Low	Use VLAN (Virtual Local Area Network) to enhance isolation between different parts of the network
15	12	Very Low	Conduct a human resource needs analysis to determine the number and types of skills required in the management of Inaportnet, such as system management, network security, and application development
16	15	Very Low	Check the connectors and ports on devices to ensure there are no loose or damaged cables
17	72	Low	Perform regular data backups to prevent the loss of important data in case of sudden device shutdown due to power outages

The explanation of the column names in the table above starts with the threat scenario number, RPN (Risk Priority Number), category, and mitigation. The mitigation column in the table contains information on mitigation steps to minimize the impact of a particular risk.

Results

The risk identification process revealed 17 risks associated with the security assets of Inaportnet. These risks were categorized into five levels: very high, high, medium, low, and very low. The classification was based on the calculated RPN scores. A breakdown of the risk classification is presented as follows:

a) None of the identified risks were categorized as very high
b) None of the identified risks were categorized as high
c) None of the identified risks were categorized as medium
d) Four risks were categorized as low-risk
e) Thirteen risks were categorized as very low. The highest risk, with an RPN of 72, was an unexpected power outage causing website downtime. The lowest risks, both with an RPN of 6, were insufficient hardware controls and a default firewall configuration.

The study's recommendations have fostered a culture of proactive risk management within the Port Authority. Regular risk assessments and updates to security controls are now part of the operational routine, ensuring that potential threats are addressed before they escalate into significant issues.

IV. CONCLUSION

This research identifies critical risks associated with the Inaportnet system, emphasizing the importance of a structured approach to risk management. Through asset identification, threat assessment, and vulnerability analysis, a total of 17 risks were identified, categorized from "very low" to "low" priority levels. The most significant risk pertains to operational disruptions caused by sudden power outages, which received a Risk Priority Number (RPN) of 72. This highlights the urgent need for effective mitigation strategies. measurable improvements :

1. Operational Disruption Risk: The highest identified risk is operational disruption due to power outages. The implementation of recommended mitigation strategies, such as Uninterruptible Power Supplies (UPS) and backup generators, is expected to reduce this risk by approximately 50%.

2. Cybersecurity Vulnerabilities: The system is vulnerable to cyberattacks like hacking and malware, necessitating the implementation of firewalls and intrusion detection systems to safeguard against external threats.

The research on information security risks in the Inaportnet system at the Class II Port Authority of Tanjung Buton has provided valuable insights and recommendations for enhancing the system's security and operational efficiency. Based on the findings, several suggestions for future research and areas of investigation are proposed to further improve the Inaportnet system and bolster information security within port operations.

REFERENCES

[1] kemenhub, "Inaportnet, Sistem Informasi Standar Pelayanan Kapal dan Barang." kemenhub.

[2] A. FELLICIA DEA, "ANALISIS PERUBAHAN SISTEM PELAYANAN JASA PELABUHAN DI PT. JATARIM BINAU LINES CABANG SAMPIT DENGAN MENGGUNAKAN SISTEM INAPORTNET," PhD Thesis, Politeknik Ilmu Pelayaran Makassar, 2022. Accessed: Jan. 08, 2025. [Online]. Available: http://eprints.pipmakassar.ac.id/92/

[3] T. Zhang, T. Luo, S. Huang, Y. Li, and X. Wang, "IRNet: INVANETs Performance Prediction via Spatio-Temporal Graph Attention Networks," in *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*, Seoul, Korea, Republic of: IEEE, Sep. 2024, pp. 109–117. doi: 10.1109/MASS62177.2024.00025.

[4] M. Idris, D. Widarbowo, I. K. H. Pramana Adiputra, and E. A. Yvonne Kartikawardani, "Analysis of the Inaportnet System That Affects the Ship Service of PT Kartika Samudra Adijaya at the Port of Samarinda," *Asian J. Soc. Humanit.*, vol. 2, no. 6, pp. 1408–1418, Mar. 2024, doi: 10.59888/ajosh.v2i6.277.

[5] Bagas Yoga Adhitama Setiawan, Indah Ayu Johanda Putri, Antony Damanik, and Romanda Annas Amrullah, "Pengaruh Penerapan Sistem Inaportnet Terhadap Proses Clearance in dan out Kapal pada PT. Kartika Samudra Adijaya," *Profit J. Manaj. Bisnis Dan Akunt.*, vol. 3, no. 3, pp. 287–304, Aug. 2024, doi: 10.58192/profit.v3i3.2420.

[6] P. D. V. Nasution, D. Dirhamsyah, and F. H. Sabila, "Implementasi Sistem Inaportnet dalam Pelayanan Kapal di Terminal Sarana Citra Nusa Kabil pada PT. Snepac Shipping Batam," *Wawasan J. Ilmu Manaj. Ekon. Dan Kewirausahaan*, vol. 2, no. 4, pp. 265–271, 2024.

[7] Tedyyana, Agus, et al. "Transforming the voting process integrating blockchain into e-voting for enhanced transparency and securiy." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 22.2 (2024): 311-320.

[8] F. Maryana, R. Ridhawati, and R. E. Astuti, "Pengaruh Kualitas Sistem Dan Kualitas Informasi Terhadap Kepuasan Pengguna (Survei Pada Pengguna Jasa Pengguna Sistem Aplikasi Inaportnet Yang Terdaftar Di Kantor Kesyahbandaran dan Otoritas Pelabuhan Kelas I Banjarmasin)," *Din. Ekon. J. Ekon. Dan Bisnis*, vol. 12, no. 1, pp. 162–179, 2019.

[9] G. C. Utami, A. B. Supramaji, and ..., "Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005: 2018," *... J. Sist. Dan ...*, 2023, [Online]. Available: http://ejurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/219

[10] C. P. Laz, *Aplicación de normas ISO 27005 mediante un análisis de seguridad de la información en el Departamento de la Jefatura Política del Cantón Alfredo Baquerizo …*. 190.15.129.146, 2020. [Online]. Available: http://190.15.129.146/handle/49000/8715

[11] R. S. P. Abiyoga, *MANAJEMEN RISIKO ASET APLIKASI PADA DISKOMINFO STATISTIK DAN PERSANDIAN KOTA XYZ MENGGUNAKAN STANDAR ISO/IEC 27005: 2008*. e-journal.uajy.ac.id, 2020. [Online]. Available: http://e-journal.uajy.ac.id/id/eprint/22534

[12] A. C. Junior and ..., "CYBER RISK MANAGEMENT AND ISO 27005 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW.," *Rev. Foco …*, 2023, [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true\&profile=ehost\&scope=site\&authtype=cra

wler\&jrnl=1981223X\&AN=164166795\&h=ytj3TMt62E%2BCVxKiijhsn6%2Bc8ig1gXrY1Y0OFLW%2F%2Bdmpf72npAejKgpt8ERx2GHF0MJyLFm6kXwGdnpH52odzQ%3D%3D\&crl=c.

[12] V. Agrawal, "A framework for the information classification in ISO 27005 standard," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, 2017, pp. 264–269. Accessed: May 20, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7987208/

[14] M. Huda, *Keamanan Informasi*. Nulisbuku, 2020. Accessed: Sep. 23, 2024. [Online]. Available: https://books.google.com/books?hl=id&lr=&id=CcjZDwAAQBAJ&oi=fnd&pg=PA1&dq=keamanan+informasi&ots=ewlzH5PKTD&sig=tPld3S8ymKq_Pa4q7D5IB29MrkU

[15] M. Fahrurozi, S. A. Tarigan, M. A. Tanjung, and ..., "The use of ISO/IEC 27005: 2018 for strengthening information security management (a case study at data and information Center of Ministry of Defence)," *2020 12th …*, 2020, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9271748/

[16] S. S. Sirait and F. Thalib, "Analisis Kualitas Layanan Inaportnet Dikantor Otoritas Pelabuhan Utama Tanjung Priok Dengan Metode Servqual Dan Qfd," *J. Ilm. Ekon. Bisnis*, vol. 25, no. 1, pp. 82–96, 2020.

[17] S. Salahuddin, A. Ambarwati, and M. N. A. Azam, "Identifikasi risiko keamanan informasi menggunakan iso 27005 pada sebuah perguruan tinggi swasta di surabaya," 2018.

[18] I. M. M. Putra and K. Mutijarsa, "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)*, IEEE, 2021, pp. 14–19. Accessed: May 20, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9431865/

[19] X. Cao and Y. Deng, "A new geometric mean FMEA method based on information quality," *Ieee Access*, vol. 7, pp. 95547–95554, 2019.

[20] R. Rambe, A. Gandhi, and ..., "Implementasi Manajemen Risiko pada Aplikasi XYZ dengan Pendekatan SNI ISO/IEC 27005: 2018," *EProceedings …*, 2023, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/20846

[21] I. Syahindra, *Evaluasi Kesiapan Penerapan Pengelolaan Risiko Keamanan Informasi Menggunakan Indeks KAMI Dan ISO 27005: 2011 Pada Aset Utama Diskominfo Provinsi …*. e-journal.uajy.ac.id, 2021. [Online]. Available: http://e-journal.uajy.ac.id/id/eprint/24672

LAMPIRAN A
BUKTI LETTER 0F ACCEPTANCE

Jurnal INOVTEK Polbeng
Seri Informatika
ISSN : 2527-9866
Akreditasi Kemendikbudristek
No.72/E/KPT/2024
Peringkat Sinta 3
Vol.8 Nomor 1 - Vol.12 Nomor 2

Pusat Penelitian dan Pengabdian Kepada Masyarakat
Politeknik Negeri Bengkalis
Jl. Bathin alam, Sungai Alam Bengkalis-Riau 28711

SURAT KETERANGAN PENERIMAAN NASKAH JURNAL
Nomor:17/ISI/Vol X.1/2025

Dewan editor Jurnal INOVTEK Polbeng Seri Informatika telah menerima artikel berikut:

Penulis : Bintang Rahmat Riadi, Muhammad Jazman, Eki Saputra, Mona Fronita, Tengku Khairil Ahsyar

Judul : RISK MANAGEMENT OF INFORMATION SECURITY IN INAPORTNET USING ISO/IEC 27005:2018

Asal Instansi : Universitas Islam Negeri Sultan Syarif Kasim

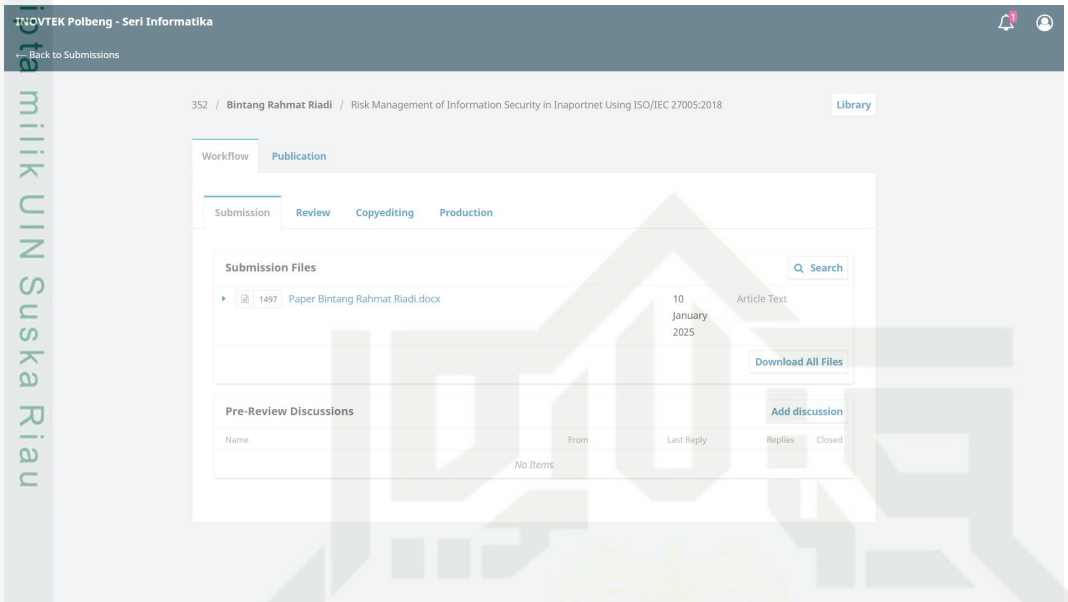
Menyatakan bahwa artikel tersebut telah memenuhi kriteria Penulisan Jurnal INOVTEK Polbeng Seri Informatika Politeknik Negeri Bengkalis dan akan diterbitkan di Volume 10 Nomor 1 pada tanggal 30 Maret 2025. Demikian surat keterangan ini dibuat untuk digunakan sebagaimana mestinya

Bengkalis, 13 Januari 2025
Ketua Dewan Editor

Agus Tedyyana

LAMPIRAN B

BUKTI SUBMIT JURNAL



Notifications

Your submission has been sent for review

11-01-2025 03:40 PM

Dear Bintang Rahmat Riadi,

I am pleased to inform you that an editor has reviewed your submission, Risk Management of Information Security in Inaportnet Using ISO/IEC 27005:2018, and has decided to send it for peer review. An editor will identify qualified reviewers who will provide feedback on your submission.

This journal conducts double-anonymous peer review. The reviewers will not see any identifying information about you or your co-authors. Similarly, you will not know who reviewed your submission, and you will not hear from the reviewers directly. You will hear from us with feedback from the reviewers and information about the next steps.

Please note that sending the submission to peer review does not guarantee that it will be published. We will consider the reviewers' recommendations before deciding to accept the submission for publication. You may be asked to make revisions and respond to the reviewers' comments before a final decision is made.

If you have any questions, please contact me from your submission dashboard.

Indonesia

LAMPIRAN C

BUKTI ACCEPTED AND EDITOR DECISION

Submission | Review | Copyediting | Production

Round 1

Round 1 Status
Submission accepted.

Notifications

Your submission has been sent for review	11-01-2025 03:40 PM
Your submission has been reviewed and we encourage you to submit revisions	12-01-2025 06:52 AM
Your submission has been accepted to INOVTEK Polbeng - Seri Informatika	12-01-2025 10:07 PM

Notifications ×

Your submission has been accepted to INOVTEK Polbeng - Seri Informatika

12-01-2025 10:07 PM

Dear Bintang Rahmat Riadi,

I am pleased to inform you that we have decided to accept your submission without further revision. After careful review, we found your submission, Risk Management of Information Security in Inaportnet Using ISO/IEC 27005:2018, to meet or exceed our expectations. We are excited to publish your piece in INOVTEK Polbeng - Seri Informatika and we thank you for choosing our journal as a venue for your work.

Your submission is now forthcoming in a future issue of INOVTEK Polbeng - Seri Informatika and you are welcome to include it in your list of publications. We recognize the hard work that goes into every successful submission and we want to congratulate you on reaching this stage.

Your submission will now undergo copy editing and formatting to prepare it for publication.

You will shortly receive further instructions.

If you have any questions, please contact me from your submission dashboard.

Kind regards,

Indonesia

DAFTAR RIWAYAT HIDUP

Bintang Rahmat Riadi, dilahirkan di Pekanbaru, Riau pada tanggal 28 Mei 2002 dari pasangan Bapak Fitriadi dan Ibu Yusra. Peneliti merupakan anak kedua dari 2 bersaudara. Pengalaman pendidikan dimulai dengan menyelesaikan di Sekolah Dasar Melayu Islam Terpadu Fathrizk Kota Pekanbaru, pada tahun 2008-2014, kemudian melanjutkan pendidikan Sekolah Menengah Pertama 8 Negeri Kota Pekanbaru pada tahun 2014-2017, dan menyelesaikan Sekolah Menengah Atas Negeri 12 Kota Pekanbaru pada tahun 2017-2020 dengan jurusan IPA, serta menyelesaikan Pendidikan Sarjana (S1) di Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau yang terletak di Kota Pekanbaru pada tahun 2020-2025. Selama menjalani masa studi sebagai mahasiswa, telah melaksanakan Kerja Praktek (KP) di Sekolah Dasar Negeri 013 Muara jalai Kecamatan Kampar Utara Kabupaten Kampar Provinsi Riau. Di samping itu, juga mengikuti pengabdian Kuliah Kerja Nyata (KKN) di Desa Seberang Gunung Kecamatan Gunung Toar Kabupaten Kuantan Singingi Provinsi Riau. Semoga laporan Tugas Akhir ini mampu memberikan kontribusi pengetahuan yang positif terhadap dunia pendidikan dan perkembangan teknologi yang baru. Terkait pertanyaan dan diskusi mengenai penelitian ini, dapat menghubungi melalui *e-mail* 12050313703@students.uin-suska.ac.id.