

Data Quality Risk Management in the Data Quality Issue Management System at Private Banking Using the OCTAVE Allegro Approach

Puspa Riri Agustiana*

Information Technology, Pradita
University, 15810, Indonesia
puspa.riri@student.pradita.ac.id


**Corresponding author*

Wilson

Information Technology, Pradita
University, 15810, Indonesia
wilson@student.pradita.ac.id

Jarot S. Suroso

Information Technology, Pradita
University, 15810, Indonesia
jarot.suroso@pradita.ac.id

 Submitted: 2025-05-07; Accepted: 2025-05-13; Published: 2025-06-05

Abstract—The success of a private bank is significantly dependent on managing the data quality efficiently so that the operations can run effectively, ensure compliance with regulations, and make its customers happy. Having poor data quality can also result in some pretty major monetary losses, operational inefficiencies, or damage to your reputation. This paper explores the application of the OCTAVE Allegro approach within a Supply Chain Data Quality Issue Management System, to deal with these challenges. The use of an information security risk assessment tool such as OCTAVE Allegro enforces a structured method to gather, analyze, and prioritize data quality risks. It details the benefits of its approach — greater risk comprehension, more effective mitigation strategies, and adherence to industry norms. Using this framework, banks can improve decision-making, enforce data governance policies as well as prevent more serious and costlier data-related errors. Implementation challenges such as how to make OCTAVE Allegro applicable to external requirements, and organizational resistance are explored, and this leads to an evaluation of the proposed strategies. In the end, this paper shows that the implementation of OCTAVE Allegro effectively helps private banks construct a safe and trustworthy data ecosystem. The approach enhances how the process supports improved data quality risk management and ultimately success in a growingly data-centered sector.

Keywords— Banking, Data Quality, OCTAVE Allegro, Risk Management, Security

I. INTRODUCTION

The banking industry relies heavily on data-driven decision-making and customer data protection. However, poor data quality poses significant risks, including financial loss due to errors in financial reporting caused by inaccurate or incomplete data, operational inefficiencies resulting from delays and disruptions in processes, regulatory non-compliance due to data inaccuracies, and reputational damage from data breaches and quality issues.

As a solution, enterprises started putting in place data quality issue management systems. These systems,

however, do require a strong risk management framework to identify, assess, and mitigate potential risks to data quality. The OCTAVE Allegro framework is a simplified form of the Operationally Critical Threat, Asset, and Vulnerability Evaluation framework, and can apply very well for data quality risk management. OCTAVE Allegro enables organizations to determine what their information assets are, their vulnerabilities, and the potential risks so that they can evaluate threats like data breaches, system failure, and human error. This allows organizations to help them prioritize risk, apply relevant controls, and track their data quality to ensure they remain compliant.

Today, managing risks related to data quality isn't just a technical requirement; it's a necessity for survival in the digital age. With more people banking online and using mobile payment systems, the risks have only grown. Without proper risk management, banks face potential disasters that could disrupt their operations and put customer data at risk. For example, banking data isn't just numbers—it includes personal information, financial transactions, and even credit histories. If any of this information falls into the wrong hands, the consequences could be catastrophic. That's why banks must go beyond traditional methods and adopt advanced cybersecurity measures that protect data quality and privacy.

The rise of digital banking has made life easier for customers, but it's also opened new doors for cybercriminals. Think about how convenient it is to transfer money or pay bills with just a few taps on your phone. Now, imagine the same convenience being exploited by someone trying to steal sensitive information or disrupt financial systems. Cybercriminals are constantly evolving their tactics, and banks must stay one step ahead. Technologies like artificial intelligence (AI) and machine learning are becoming essential in this fight (Gerardo & Fajar, 2022). They can detect unusual patterns or potential threats in real-time, giving banks the ability to respond before significant damage is done.

But technology alone isn't enough. Banks also need strong policies and regulations to keep their systems secure. These aren't just boxes to tick off for compliance—they're about building resilience and ensuring that banks can withstand attacks while continuing to operate

smoothly. By adhering to strict guidelines, banks not only protect their customers but also reinforce their reputation as reliable and trustworthy institutions. After all, trust is at the heart of banking.

This is where the OCTAVE Allegro approach comes into play. Unlike generic methods, this structured risk assessment framework is designed to fit the specific needs of an organization. It helps banks take a closer look at what really matters—their critical assets. By evaluating different threat scenarios and prioritizing actions, OCTAVE Allegro provides a clear roadmap for managing risks. Instead of reacting to every issue that arises, banks can focus on the area's most likely to be targeted and take proactive steps to protect them.

What makes this methodology stand out is its practicality. Banks operate in a fast-paced and ever-changing environment, and OCTAVE Allegro recognizes that. It allows institutions to tailor their cybersecurity strategies to their unique challenges and priorities. This approach isn't just about checking for vulnerabilities—it's about understanding the bigger picture and building a defense system that works seamlessly with daily operations.

At its core, this paper emphasizes the importance of integrating strong risk management practices into data quality systems. By adopting approaches like OCTAVE Allegro, banks can do more than just address immediate problems. They can create a sustainable system that not only enhances data quality and cybersecurity but also strengthens their ability to adapt to new challenges.

In a world where customer trust and operational stability are everything, taking proactive measures isn't just a good idea—it's essential. This paper explores how banks can leverage structured methodologies to stay ahead of the curve, safeguard their most valuable assets, and maintain their position as trusted institutions in an increasingly complex digital landscape (Günther et al., 2019).

II. LITERATURE REVIEW

Using frameworks such as OCTAVE Allegro, banks can pinpoint assets at risk, evaluate possible threats, and rank strategies to minimize impact. This methodical way of working allows sensitive information to be protected, operational stability to be improved, and data governance to be facilitated over the long term, meeting the developing business needs.

A. Risk Assessment

Risk is the possibility of loss or damage caused by a particular act, as the main problem must be appropriately managed and thoroughly divided into steps. However, regarding information systems, risks will be shown from system failures, human errors, or any external attacks, which can negatively affect an organization's operations, finances, reputation, and decision-making.

Risk assessment is usually the process of figuring out what could go wrong, how bad the situation could be, and what the users can do to prevent or minimize what will happen. It mainly focused on protecting an organization's information systems, as it involved steps like identifying

what parts of the system are most important, considering any potential threats, and understanding their possible consequences (Suroso & Fakhrozi, 2018).

Risk is assessed based on the soil's composition (percentage of sand, silt, and clay). A higher percentage of sand and a lower percentage of clay indicate a higher risk of erosion, potentially leading to critical levels of erosion. The risk assessment index developed in the study quantifies this risk based on the soil's ability to withstand the erosive forces of rainfall and water flow (Abidin et al. 2017).

Infers the challenges organizations experience with fragmented performance management systems with separate systems for data storage, business reporting, and data analysis across different functions, locations, and units. This lack of fragmentation occurs due to a strong focus on operational efficiency in IT investment, neglecting seamless data access. As a result, huge data reside in a few disconnected databases and forms which become a hindrance in an effective organizational decision-making process. This study illustrates the negative effect integration quality has on performance organizations. It also demonstrates the need to connect systems necessary for complete and intelligent analysis of the data so that the decisions are made at the organizational level (Bruno et al., 2017).

Industrial enterprises increasingly rely on data-driven decision-making to optimize operations and strategic planning. However, the quality of this data often remains a significant challenge, hindering the effectiveness of data-driven insights. While numerous methodologies exist for assessing data quality (DQ), their complexity often limits their applicability, especially for small and medium-sized enterprises (SMEs).

To propose a novel approach to simplify DQ assessment and make it more accessible to SMEs. Our methodology focuses on selected, context-relevant data, whether structured or semi-structured, and employs a set of generic test criteria applicable to various domains and tasks. By combining data-driven and domain-driven aspects, the approach enables partial automation and reduces the need for extensive domain-specific knowledge.

The results of the DQ assessment are summarized into quality dimensions, facilitating benchmarking and actionable insights. We validate our methodology using real-world data from an enterprise resource planning (ERP) and manufacturing execution system (MES) in a sheet metal manufacturing company. The specific application aims to calculate key logistic performance indicators, demonstrating the practical relevance of our approach.

B. Security in Banking

It is responsible for protecting sensitive information about customers, ensuring the accuracy of transactions, and complying with regulations. Identifying, analyzing, and prioritizing cybersecurity risks in Vietnam's banking and monetary system using a risk assessment framework based on neutrosophic sets, Z-numbers, and MCDM techniques (DELPHI and DEMATEL). The Risks: Malware Infections and Supply Chain Vulnerabilities The

best strategy that you identified is, investing in advanced threat detection systems. The limitations were advice which are the Vietnam abstract orientated and only compare several MCDM methods (Irsheid et al., 2022). Future research directions involve these 2 aspects, such as expanding geographic coverage and further exploring other MCDM methods.

E-banking has transformed the way consumers access banking services by giving the convenience and efficiency of accessing banking services through electronic channels. This innovation has however brought forth several security concerns and risks, leading to an important reassessment of banks' strategy to proactively address these challenges. Consequently, this Journal highlights the real-time security threat flow toward e-banking applications and discusses the various potential risks and cyber threats affecting consumers' confidential data. Through mitigation strategies such as access control and timely updates, this research provides key insights into how banks and users can protect each other from cybercrime, ensuring secure online banking experiences (Mogos & Mohd Jamail, 2020).

Such rapid adoption has brought a surge in cyberattacks against financial institutions. Hackers target e-banking systems by exploiting vulnerabilities to retrieve sensitive customer data such as personal information, financial transactions, and account credentials. They can lead to huge costs, loss of reputation, and loss of customer trust. Hence, banks need to be extremely secure to protect their customers and their e-banking solutions to function.

To meet these challenges, banks need a security system that incorporates a multi-layered approach. This means incorporating robust authentication methods, such as biometric login or two-factor authentication, to confirm user identity. The system should undergo regular security audits and vulnerability assessments to detect and patch potential flaws. It is also crucial to keep your software up to date and patch any new vulnerabilities. Implementing these measures can dramatically improve the security of their e-banking platforms and keep their clients safe from cyber-attacks.

C. OCTAVE Allegro

OCTAVE Allegro provides a practical and efficient approach to assessing and mitigating information security risks. Its flexibility allows it to adapt to organizations of various sizes and complexities. Whether executed by individuals or teams, OCTAVE Allegro offers a scalable solution.

The framework guides organizations through a structured process, starting with identifying critical information assets such as databases, servers, network infrastructure, and intellectual property. Next, it assesses vulnerabilities, including weaknesses in security controls, configuration errors, and potential attack vectors. Then, it identifies potential threats to these assets, such as malicious hackers, insider threats, natural disasters, and human error.

The identified vulnerabilities and threats are combined to assess the overall risk to the organization. This involves considering the likelihood of a threat exploiting a

vulnerability and the potential impact of such an attack. Based on the risk assessment, appropriate security controls are developed to mitigate the identified risks. These controls can be technical, administrative, or physical, such as implementing strong passwords, firewalls, intrusion detection systems, and employee training.

A detailed action plan is created to implement the selected security controls, including timelines, responsibilities, and budget allocations. The organization's security posture is continuously monitored and reassessed to ensure the effectiveness of the implemented controls. Regular security audits, vulnerability assessments, and penetration testing can help identify and address emerging threats.

By following these steps, organizations can effectively manage their information security risks and protect their valuable assets. OCTAVE Allegro's streamlined approach and focus on practical solutions make it a powerful tool for organizations seeking to improve their security posture (Alfarisi & Surantha, 2022).

D. OCTAVE Allegro in Banking

The analysis of security risk and defining risk in the information system at Universitas Advent Indonesia uses the OCTAVE Allegro method. It also outlined an eight-step process of a framework for a methodology to identify the critical information assets: student, staff finances, grades, and attendance. The areas of impact emphasized customer reputation, financial stability, and operational efficiency, identifying vulnerabilities in malicious code, unauthorized access, and security holes, setting security rules and reassessing risks regularly with OCTAVE Allegro, recommending more studies and comparisons over methodologies, and grounding itself in established risk management literature (Nguyen et al., 2024).

What developed into a vital resource for organizations, especially in education, is information. With more dependence on Information and Communication Technologies (ICT), the risk of cyber-related threats increases. The COVID-19 pandemic has expedited the digital transformation of higher education institutions, thereby, becoming prime targets for cyberattacks.

As a result, successful information security management is essential to ensuring the confidentiality, integrity, and availability of sensitive data. The goal of this study is to Egypt's logical information security risks within the higher education sector and to make recommendations on how to mitigate such risks (Suroso et al., 2019). Institutions can take a proactive approach to securing digital assets by identifying and assessing threats and vulnerabilities.

We use the OCTAVE Allegro risk management framework, which systematically analyzes the organization regarding its information assets and the usage, storage, and transmission of those assets. The framework also enables institutions to prioritize risks and implement relevant security controls by recognizing potential threats and vulnerabilities (Azhari & Riadi, 2023). The findings from this study will offer recommendations and insights to improve the information

security landscape of the higher education sector to secure its future in the digital world (Aryanti et al., 2023).

Nowadays, we have adopted technology in our lives to help us do all our routine work. Yet this increasing dependency on technology comes with considerable risks that can compromise the security of sensitive data, especially within organizations (Wagiu et al., 2019). The function of the Academic Information System at Kalbis Institute of Technology, a Private Institute with Systematic Academic in East Jakarta was established in 2012, by applying such a system to support its stakeholders within the campus (Sanjaya, 2020). Acknowledging the criticality of protecting this system, a thorough risk assessment has been conducted to determine and assess possible threats and vulnerabilities.

For this study, the OCTAVE Allegro method is used as a systematic assessment tool, leveraging the OCTAVE Allegro Worksheet. Through the analysis of these risks, the study intends to generate a more in-depth perspective of the security threats to the academic information system at Kalbis Institute. The project's outcomes will ultimately provide risk assessments and strategic recommendations for improved information systems protection within the institution, thus safeguarding the core activities of the university. By conducting this analysis, we aim to contribute to a more secure technological landscape that aligns with the dynamic requirements of educational institutions in an ever-evolving digital landscape.

III. MATERIAL AND METHOD

This methodology, known as OCTAVE; short for Operationally Critical Threat, Asset, and Vulnerability Evaluation, is a simplified version of the full Operationally Critical Threat, Asset, and Vulnerability Evaluation framework which is designed to provide a more structured approach to information security risk management. It allows organizations to systematically identify information security risks, assess their impact and likelihood, and prioritize these risks based on their potential harm to the organization. OCTAVE Allegro helps organizations prioritize their resources and the security controls they need to put into place by focusing on critical assets, vulnerabilities, and threats.

It consists of eight steps to identify and assess information assets, vulnerabilities, and threats, analyze and prioritize risks, and develop a plan of security controls. With these steps, organizations can develop a full picture of their security posture enabling them to secure vital resources better.

Benefits of OCTAVE Allegro Framework
Improved Risk Awareness: OCTAVE Allegro promotes an ongoing process that takes organizational tactics and vulnerabilities into account; this results in better risk awareness, as the organization understands exactly where they currently stand about risks and opportunities for improvement.
Improved Decision-Making: As the risk management process integrates with existing organizational practices, it helps decision-makers to identify risks more effectively and prioritize responses with better alignment toward business objectives.
More Effective Resource Allocation:

Ensuring that key properties remain over time based on their significance to core business operations helps organizations avoid spending resources against things that are not impactful enough; it also moves away from point solutions. **More Proactive Security Posture:** Risk identification is an ongoing process that engages a diverse set of people; this is critical in building a proactive security posture by framing the risk knowledge into concrete tactical or strategic decisions. This approach will help organizations improve their cyber resilience and protect their critical data from potential cyberattacks.

This research utilized the OCTAVE Allegro methodology, a simplified version of the Operationally Critical Threat, Asset, and Vulnerability Evaluation framework. OCTAVE enables organizations to systematically identify and assess information security risks, prioritize mitigation efforts, and make informed decisions to safeguard their valuable assets.

OCTAVE offers three methodologies: OCTAVE, OCTAVE-S, and OCTAVE Allegro. OCTAVE Allegro is a simplified version that is particularly suitable for smaller organizations. It involves a collaborative workshop where participants work together to identify critical assets, potential threats, and vulnerabilities and then develop strategies to mitigate these risks. This approach allows for a more efficient and focused risk assessment process. Here is the 8-step flow for OCTAVE Allegro Methodology, which starts from the Establish Drivers Phase - Profile Assets Phase - Identify Threats Phase and the last is the Risk Mitigation Phase in Figure 1.

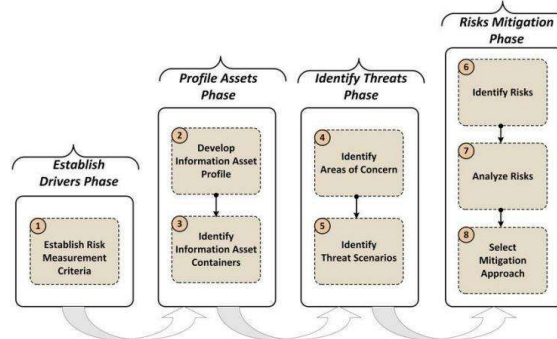


Figure 1. OCTAVE Allegro step-by-step

IV. RESULT & DISCUSSION

Here are the key steps in risk assessment conducted using OCTAVE Allegro identified critical data quality vulnerabilities and cyber protection data:

A. Establish Drivers

To begin the risk assessment process in the data quality management system, it is essential to first identify critical data assets and evaluate the potential consequences of any disruptions or breaches. These impacts—such as customer trust, bank reputation, and regulatory penalties—are categorized in Table 1 as low, medium, or high. This classification serves as a foundation for prioritizing risks according to the severity of possible losses.

Table 1. Impact Area

Impact Area	Low	Medium	High
Customers' trust & Data Protection	The bank's reputation is minimally impacted and does not require much effort	The bank's reputation is badly affected and requires costs to cover it	The bank's reputation is badly affected, and customers distrust banks.
Bank Reputation	Less than 1% reduction in customers due to loss of trust	2% to 5% reduction in customers due to loss of trust	More than 5% reduction in customers due to loss of trust
Penalties	The data protection implemented was not given enough attention, and a complete security assessment was not carried out.	The data protection implemented was neglected, and security assessment was solely focused on password encryption.	Insufficient attention was given to data protection measures, and no comprehensive security assessment was performed.

B. Profile Assets

1. Develop Information Asset Profile

Once the impact areas are established, the next step is to profile the information assets involved in the data quality system. This includes identifying the data sources, ownership, and the rationale for considering each asset as critical. The table 2 below presents the key assets and explains their role in supporting data flow and decision-making processes within the bank.

Table 2. Information Asset Profiling - Data Quality System

Critical Asset	Source System	Critical Asset	Source System
Rationale for selection	The source system is the parent of the data produced and is another storage medium besides the user interface system database.	Rationale for selection	The source system is the parent of the data produced and is another storage medium besides the user interface system database.
Description	The source of all data	Description	The source of all data
Owner	Team Development & Team Business	Owner	Team Development & Team Business

2. Identify Information Asset Containers

To understand the technical context in which these assets operate, it is essential to map their risk environment, particularly in terms of infrastructure and access control. Table 3 describes the technical environment and the designated owners of the systems, helping to assess vulnerabilities stemming from internal operational settings.

Table 3. Information Asset Risk Environment - Data Quality System

Information Asset Risk Environment Map (Technical & Network)	Information Asset Risk Environment Map (Technical & Network)	Information Asset Risk Environment Map (Technical & Network)	Information Asset Risk Environment Map (Technical & Network)
Internal Controller Description Internal network with VPN	Owner Data Management with VPN	Internal Controller Description Internal network with VPN	Owner Data Management with VPN

C. Identify Threats

The subsequent step in the OCTAVE Allegro framework involves identifying potential threat scenarios that could compromise the integrity of data assets. As shown in Table 4, this includes detailing the areas of concern, the actors involved, their motives, the methods used, and the anticipated outcomes. By analyzing these components, organizations gain a clearer understanding of how data breaches or disruptions might occur.

Table 4. Properties of threat

Area of concern	Threats scenario
Changes in data storage	Actors Means Motives Outcome Security Requirement
	Business Unit Data reduction is hampered. Error running progress Modify Source table change schedule planning

D. Identify and Mitigate Risk

1. Identify Risk

After identifying potential threats, it is crucial to prioritize the associated risks based on their severity and relevance. The table 5 below provides a numeric scale to score each impact area—customer trust, reputation, and penalties—according to the assessed risk levels. This helps determine which risks require urgent mitigation.

Table 5. Priority Impact Area - Data Quality System

Impact Area	Priority	Value Impact		
		Low	Medium	High
Customers' trust & Data Protection	1	10	20	30
Bank Reputation	2	5	10	15
Penalties	3	2	4	6

2. Analyze Risks

Effective risk assessment involves evaluating both the likelihood and the consequences of identified threats. The table 6 presents a detailed analysis of risk scenarios,

including the severity of their outcomes, and assigns values and scores to each impact area. This analysis forms the basis for selecting the most appropriate mitigation strategies.

Table 6. Risk Analysis

Area of concern				
Changes after storage data changes	Consequences	Requires precision and running steps according to the schedule		
	Severity	Impact Area	Value	Score
		Customers' trust & Data Protection	High	30
		Bank Reputation Penalties	Medium	10
			Medium	4

3. Select Mitigation Approach

Once risks have been assessed and prioritized, the next step is to define appropriate mitigation strategies. The table 8 below categorizes each risk into one of three pools—Mitigate, Defer/Mitigate, or Accept—based on urgency and feasibility. This classification guides decision-makers in allocating resources and planning responses accordingly.

Table 7. Mitigation Approach

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Defer / Mitigate
Pool 3	Acc

To visualize the relative risk levels and simplify interpretation, a risk matrix is used. The following table 8 displays how risk scores fall into specific ranges, each linked to a different response category. This matrix helps organizations quickly identify high-priority risks and take timely action

Table 8. Relative Risk Matrix

Pool Score		
Pool 1	Pool 2	Pool 3
35 - 60	19 - 34	0 - 18

V. CONCLUSION

The framework of OCTAVE Allegro is based automated data quality issue management system for the effective development, documentation, review, and resolution of data quality issues. Advancing the theory of data quality risk, the framework provided may be of value to academics looking to explore the research gaps and practical gaps this presents to businesses looking to improve their AU. More studies are required to examine the impact of novel technologies (artificial intelligence and machine learning) on data quality. Such temporal studies can also offer much-needed insights into the longer-term impact of data quality risk management practices.

To summarize, the significance of data quality in banking is reiterated based on the findings of this risk management evaluation. To enhance data quality, minimize operational risks, and drive business outcomes, banks must ensure data accuracy, completeness, and consistency across their systems. An effective data quality management program helps banks meet regulatory requirements, reduces fraud and cyberattacks, and enables better decision-making.

REFERENCES

- Abidin, R. Z., Sulaiman, M. S., & Yusoff, N. (2017). Erosion risk assessment: A case study of the Langat River bank in Malaysia. *International Soil and Water Conservation Research*, 5(1). <https://doi.org/10.1016/j.iswcr.2017.01.002>
- Alfarisi, S., & Surantha, N. (2022). Risk assessment in fleet management system using OCTAVE allegro. *Bulletin of Electrical Engineering and Informatics*, 11(1). <https://doi.org/10.11591/eei.v11i1.3241>
- Aryanti, U., Anwar, Moch. T., & Rahmawati, T. (2023). INFORMATION SECURITY RISK MANAGEMENT USING OCTAVE ALLEGRO METHOD AT UNIVERSITY. *International Journal of Ethno-Sciences and Education Research*, 3(4). <https://doi.org/10.46336/ijeer.v3i4.506>
- Azhari, A. R., & Riadi, I. (2023). Risk Assessment Analysis Website on Tech Company using OCTAVE Allegro Framework. *International Journal of Computer Applications*, 185(28). <https://doi.org/10.5120/ijca2023923031>
- Bruno, E., Iacoviello, G., & Lazzini, A. (2017). Data quality and data management in banking industry. Empirical evidence from small Italian banks. In *Lecture Notes in Information Systems and Organisation* (Vol. 20). https://doi.org/10.1007/978-3-319-49538-5_2
- Gerardo, V., & Fajar, A. N. (2022). Academic IS Risk Management using OCTAVE Allegro in Educational Institution. *Journal of Information Systems and Informatics*, 4(3). <https://doi.org/10.51519/journalisi.v4i3.319>
- Günther, L. C., Colangelo, E., Wiendahl, H. H., & Bauer, C. (2019). Data quality assessment for improved decision-making: A methodology for small and medium-sized enterprises. *Procedia Manufacturing*, 29. <https://doi.org/10.1016/j.promfg.2019.02.114>
- Irsheid, A., Murad, A., Alnajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, 204. <https://doi.org/10.1016/j.procs.2022.08.025>
- Mogos, G., & Mohd Jamail, N. S. (2020). Study on security risks of e-banking system. *Indonesian Journal of Electrical Engineering and Computer Science*, 21(2). <https://doi.org/10.11591/ijeecs.v21i2.pp1065-1072>
- P.-H. Nguyen et al., “Assessing cybersecurity risks and prioritizing top strategies in Vietnam’s finance and banking system using strategic decision-making

- models-based neutrosophic sets and Z number,” *Heliyon*, vol. 10, no. 19, Oct. 2024. <https://doi.org/10.1016/j.heliyon.2024.e37893>
- Sanjaya, J. (2020). Analisis Risk Assessment Terhadap Perusahaan IT di Bidang Finansial Menggunakan OCTAVE Allegro Framework. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, 10(1). <https://doi.org/10.35585/inspir.v10i1.2528>
- Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Computer Science*, 135. <https://doi.org/10.1016/j.procs.2018.08.167>
- Suroso, J. S., Januanto, A., & Retnowardhani, A. (2019). Risk Management of Debtor Information System at Bank XYZ Using OCTAVE Allegro Method. *Proceedings of the International Conference on Electrical Engineering and Informatics*, 2019-July. <https://doi.org/10.1109/ICEEI47359.2019.8988890>
- Wagiu, E. B., Siregar, R., & Maulany, R. (2019). Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method. *Abstract Proceedings International Scholars Conference*, 7(1). <https://doi.org/10.35974/isc.v7i1.1387>
- Borman, W. C., Hanson, M. A., Oppler, S. H., Pulakos, E. D., & White, L. A. (2020). Role of early supervisory experience in supervisor performance. *Journal of Applied Psychology*, 78(3), 443-449. <https://doi.org/10.1037/0021-9010.78.3.443>
- Wiskunde, B., Arslan, M., Fischer, P., Nowak, L., Van den Berg, Kovács, A. (2019). Indie pop rocks mathematics: Twenty One Pilots, Nicolas Bourbaki, and the empty set. *Journal of Improbable Mathematics*, 27(1), 1935–1968. <https://doi.org/10.0000/3mp7y-537>
- Vogels, A. G. C., Crone, M. R., Hoekstra, F., & Reijneveld, S. A. (2012). Comparing three short questionnaires to detect psychosocial dysfunction among primary school children: a randomized method. *BMC Public Health*, 9(1), 489. <https://doi.org/10.1186/1471-2458-9-489>