Internasional Journal of Integrative Sciences (IJIS)
Vol.4, No.5, 2025: 1047-1060

Information Security Risk Assessment and Mitigation Prioritization at the Naval Base Data Center Using the OCTAVE Allegro Framework Combined with the Delphi Method

Hadi Mardiyanto[1*], Yoyok Nurkarya S[2], Hadi Prasutiyon[3]
[1,2]STTAL Bumimoro, Surabaya
[3]Department of Marine Engineering, Hang Tuah University, Surabaya
Corresponding Author: Hadi Mardiyanto hadi.prasutiyon@hangtuah.ac.id

A R T I C L E I N F O

Keywords: Information Security, Risk Assessment, OCTAVE Allegro, Delphi Method, ISO/IEC 27002:2022, Data Center

Received : 21 March
Revised : 23 April
Accepted: 23 May

A B S T R A C T

The purpose of this study is to analyze potential risks that may threaten the security of the Naval Base Data Center, a facility crucial to supporting naval operational tasks. Risk assessment was conducted using the OCTAVE Allegro framework integrated with the Delphi method, and mitigation steps were formulated in accordance with ISO/IEC 27002:2022 to ensure effective risk management. Fifteen information-security experts participated via the Delphi process to identify fourteen principal risk factors affecting data confidentiality, integrity, and availability. The analysis revealed that the greatest risks stem from cyber threats—particularly ransomware attacks—and unauthorized administrative access. Based on the risk evaluation, recommended mitigations include strengthening security controls, updating hardware and software infrastructure, and providing ongoing personnel training. It is anticipated that these findings will offer a more systematic guide for managing information-security risks at naval data centers and will reinforce safeguards to support more secure operational continuity

INTRODUCTION

Rapidly evolving digital era, information technology plays a vital role in ensuring the smooth operation of the Navy's bases, which have a strategic duty to safeguard Indonesia's maritime security. IT systems enable naval bases to improve efficiency in coordinating among dispersed operational units and command centers (Budarsa et al., 2022). A core component of these operations is the data center, responsible for storing and managing mission-critical information. A reliable and secure data center is essential for providing timely and accurate data to support critical decision-making in defending national maritime sovereignty.

However, as the complexity of deployed technology increases, so too do the threats to information security. Internal threats—such as human error or improper system configuration—as well as external threats—such as cyberattacks—can jeopardize the continuity of data-center operations (Ramjanati et al., 2021; Vuda et al., 2023). Therefore, conducting a comprehensive risk assessment of information systems within the Naval Base Data Center is imperative. Such an assessment aims to identify, analyze, and evaluate potential threats to data confidentiality, integrity, and availability, and to provide appropriate mitigation recommendations to protect these information assets (Nurul et al., 2022).

This research employs the OCTAVE Allegro framework for security risk assessment. OCTAVE Allegro is a structured methodology designed to identify critical information assets, assess threat vectors, and prioritize risks in a systematic manner (Annisa, 2024). An integral component of this assessment is the Delphi method, which gathers expert judgments and achieves consensus on risk prioritization (Prajanti et al., 2020). In this study, the Delphi technique is used to solicit and weight expert opinions on the various risk factors present in the naval data center environment. This consensus-driven approach is crucial for obtaining objective, multi-dimensional insights into the complex landscape of information-security risk.

Once risks are identified and analyzed, mitigation measures are formulated according to their priority rankings. The ISO/IEC 27002:2022 standard serves as the primary reference for these mitigation strategies, offering best practices and control recommendations to safeguard information systems (Aulia et al., 2023). By aligning mitigation steps with this international standard, the study aims to propose controls tailored to the specific needs of the Naval Base Data Center, thereby reducing the most significant and potentially damaging threats.

Information-security in a naval data center is a critical enabler of uninterrupted naval operations. Hence, this study seeks to deepen understanding of the threats faced and to provide targeted mitigation solutions. Through the combined application of OCTAVE Allegro and the Delphi method—underpinned by ISO/IEC 27002:2022—the research endeavors to contribute significantly to enhancing data-center security and operational effectiveness in maritime defense. Furthermore, the findings are intended to offer practical guidance to military organizations and other institutions in conducting risk assessments and implementing robust security-risk management in an

increasingly complex digital world. Information security is not merely about threat prevention but also about ensuring operational continuity, thereby improving organizational readiness and effectiveness (Puriwigati et al., 2020).

In modern organizations, the design and management of information systems hinge on the effective integration of five core components—hardware, software, data, procedures, and people—and on transforming raw data into timely, actionable intelligence to support decision-making (Mintrom, 2015; Pangestu, 2007). As digital technologies evolve, innovations such as big data analytics, cloud computing, and real-time data processing have become critical enablers of operational efficiency and competitive advantage. Evidence shows that integrating these technologies with overarching business strategies fosters data-driven decisions and enhances responsiveness to market shifts (Putriku et al., 2024; Istiningrum, 2012). Consequently, practitioners must continually update their technical and analytical skillsets to design information-system solutions that meet the demands of an ever-changing global environment (Christian, 2015).

Information-system security faces both internal and external threats that can severely disrupt operations. Internal threats—ranging from inadvertent human errors and misconfigurations to deliberate sabotage—are particularly challenging because they often originate within the circle of authorized users, making them difficult to detect (Parker, 1998). External cyber-attacks, including phishing campaigns, ransomware, and large-scale Distributed Denial of Service (DDoS) attacks, can cripple data-center functionality and compromise critical information assets (Gordon & Loeb, 2002). Moreover, natural disasters such as earthquakes or floods pose physical risks to infrastructure, underlining the necessity for advanced threat-detection technologies, stringent security policies, and continuous staff training to maintain resilience.

LITERATURE REVIEW

Underpinning any robust security program is a well-structured risk-management process. Classic risk theory distinguishes between measurable risks and deep uncertainties that defy precise quantification (Knight, 1921). Modern frameworks advocate blending quantitative and qualitative analyses, though quantification of intangible assets like information can introduce subjectivity (Aven, 2016). Standards such as ISO/IEC 27002:2013 provide prescriptive controls—like strong access management, encryption, regular system updates, and disaster-recovery planning—to mitigate identified risks (ISO/IEC 27002:2013). Following a systematic cycle of threat identification, impact assessment, and control implementation—whether by reducing, transferring, accepting, or avoiding risk—ensures that organizations can protect their information assets while sustaining uninterrupted operations (Kaplan et al., 2012).

METHODOLOGY

This study employed a descriptive qualitative design supplemented by descriptive statistics (Widyaksa et al., 2024). Data were gathered via journal-article review, semi-structured interviews, and direct observation. A structured questionnaire was distributed to 15 information-security experts to reach consensus through a two-stage Delphi process (pre-Delphi and Delphi rounds). Qualitative data were coded and analyzed in NVivo, while quantitative responses were processed in Microsoft Excel (Okoli & Pawlowski, 2004).

Expert Panel Selection

Delphi validity depends on selecting experts with deep domain knowledge (Flanagan et al., 2016). Panelists were chosen based on predefined criteria—academic credentials, field expertise, professional experience, and reputation—to ensure credible input. Demographic details were recorded to document each expert's qualifications and maintain transparency in the consensus process.

Table 1. Expert Panel Demographics

Expert IDs	Field of Expertise	Role
E1–E11	Military Information Systems	Practitioner
E12–E15	Certified Information Security	Academic

OCTAVE Allegro Framework

The OCTAVE Allegro methodology guides rapid, asset-centric risk assessments in eight steps across four phases: (1) establish risk criteria; (2) profile information assets; (3) identify threat scenarios; and (4) select mitigation approaches (Caralli et al., 2007). Designed for collaborative workshops, Allegro streamlines focus on high-value assets without exhaustive data analysis.

Delphi Method

Originally developed at RAND in the 1960s, the Delphi technique elicits expert judgments through iterative questionnaires to build consensus on complex issues (Ramke et al., 2022). Best practice suggests 10–15 topics and 15–20 respondents per round (Lee et al., 2020). In this study, three rounds were conducted over 45 days, with consensus defined as ≥ 80 % agreement on a 0–7 Likert scale (Gunduz & Elsherbeny, 2020) or ≥ 70 % with median ≥ 3.25 (Karakikes & Nathanail, 2020).

Content Validity Index (CVI)

CVI quantifies expert agreement on item relevance at both item (I-CVI) and scale (S-CVI/Ave) levels (Almanasreh et al., 2018). I-CVI is the proportion of experts rating an item ≥ 3 (acceptable if ≥ 0.78); S-CVI/Ave is the average of all I-CVIs (acceptable if ≥ 0.80, excellent if ≥ 0.90) (Stancine et al., 2019; Marisa, 2021). The S-CVI/Universe approach was not used due to panel size and potential chance agreement (Roya & Behrooz, 2017).

Conceptual Framework

Integrating OCTAVE Allegro with the Delphi method, this study validates critical risk-focus areas (step 4 of Allegro) for a Naval Base Data Center, reducing individual bias through expert consensus (Prajanti & Ramli, 2019).

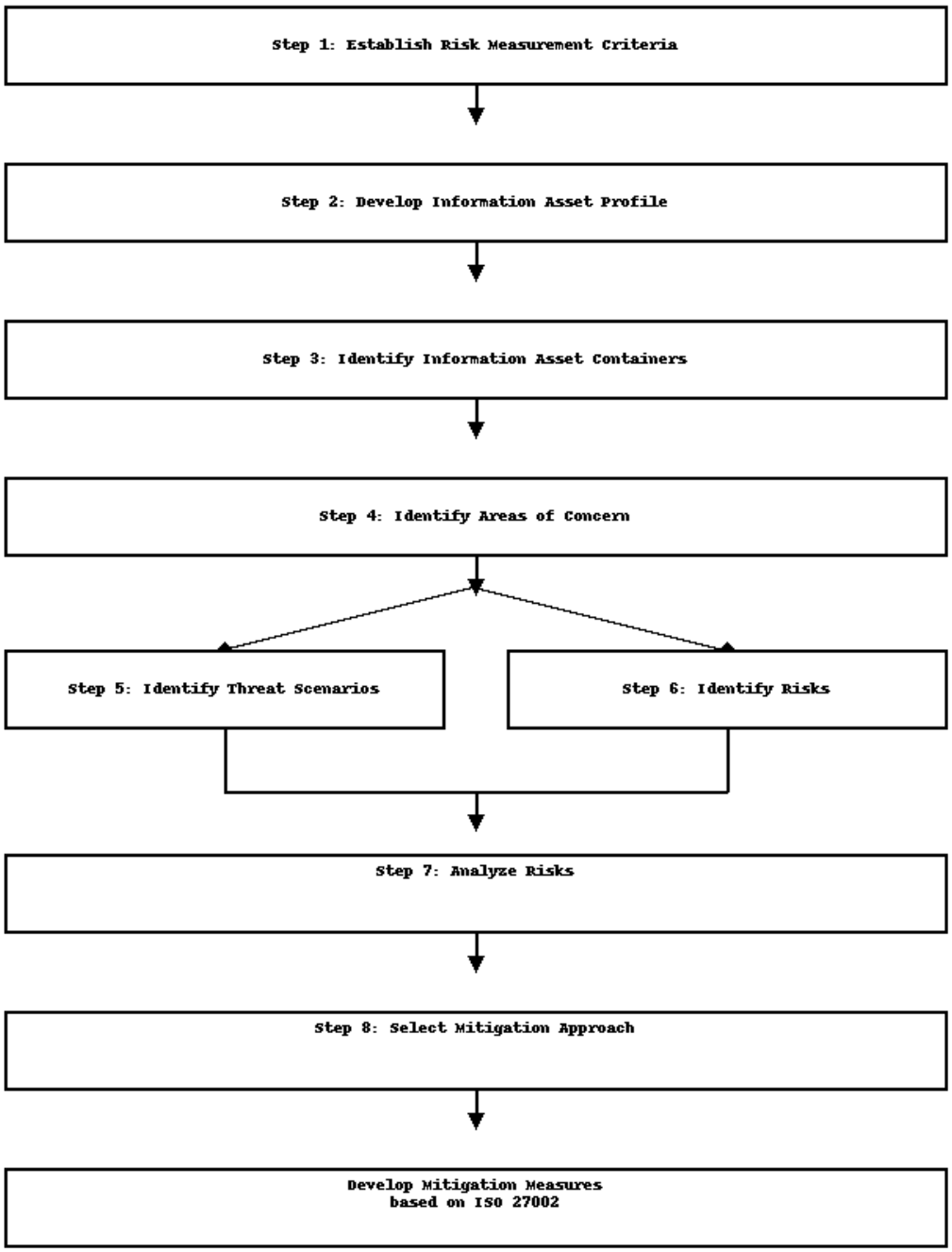

Figure 1. Conceptual Framework for Information Security Risk Assessment in the Data Center

RESULTS AND DISCUSSION

Before risk assessment, we collected detailed operational data on the Naval Base Data Center from the base's IT operations unit. To ensure accuracy, a panel of 15 stakeholders—military IT practitioners, academics, and information-security experts—was convened. Through interviews and a three-round Delphi survey, experts identified vital operational assets and reached consensus on risk factors threatening data confidentiality, integrity, and availability.

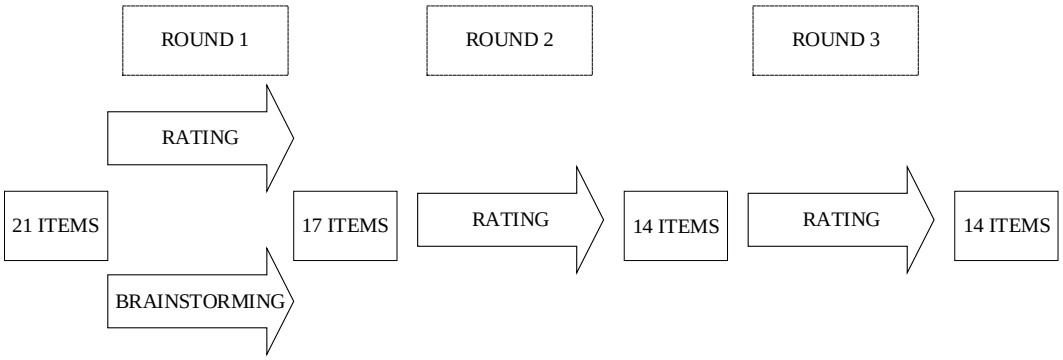

Figure 2. Delphi Rounds 1 to 3 with Number of Indicators

Step 1: Establishing Risk Measurement Criteria

Using OCTAVE Allegro's worksheet, five impact areas were defined to measure risk (Caralli et al., 2007): user reputation, financial loss, employee productivity, staff safety, and legal penalties. Experts in the base's IT division ranked these, placing employee productivity highest and **legal penalties** lowest (this study).

Step 2: Critical Asset Profiling

Experts catalogued all information assets and narrowed the list to two critical systems: the **Online Examination Application and the E-Office Administration System**. For each, they documented rationale, detailed descriptions, ownership (Naval Data Processing Department), and key security requirements (confidentiality, integrity, availability).

Step 4: Delphi Consensus on Risk Factors

Starting from 21 risk factors, three Delphi rounds reduced these to 14 validated items. Round 1 achieved a scale-level CVI (S-CVI/Ave) of 0.90; Round 2 maintained 0.90; and Round 3 reached unanimous agreement (S-CVI/Ave = 1.00), demonstrating strengthening consensus over successive rounds (Gunduz & Elsherbeny, 2020; Lakmini et al., 2023).

Steps 5–7: Threat Scenarios and Risk Analysis

Each of the 14 factors was expanded into detailed threat scenarios—defining actors, means, motives, and outcomes—and assigned a relative risk score by multiplying impact-area weights (0.07–0.33) by likelihood (1–3). The highest-scoring threat was cyberattacks (ransomware, DDoS, phishing) with a score of 45; administrative credential leaks and brute-force attacks scored 41 (this study).

Table 2. Impact Criteria Weighting

No.	Impact Area	Priority (Rank)	Low (1)	Medium (2)	High (3)	Weight Value	Scale (0–1)
1	Employee Productivity	1	5	10	15	5	0.33
2	Employee Safety and Health	2	4	8	12	4	0.27
3	Financial Impact	3	3	6	9	3	0.20
4	User Reputation and Trust	4	2	4	8	2	0.13
5	Legal Penalties and Lawsuits	5	1	2	3	1	0.07
Total						**15**	**1.00**

Step 8: Selecting Mitigation Approaches

Using a relative-risk matrix, scores of 30–45 required immediate mitigation, 16–29 were deferred, and 0–15 were accepted (Budarsa et al., 2022). Mitigation strategies were then mapped to ISO/IEC 27002:2022 controls.

Tabel 3. Relative Risk Matrix, (Budarsa et al., 2022).

Risk Relative Matrix		
Risk Score	**POOL**	**Mitigation Approach**
30-45	1	Mitigasi
16-29	2	Defer
0-15	3	Accept

Table 4. Mitigation Approach

No.	Area of Concern (AP)	Relative Risk Score	Level
1	Cyberattacks such as ransomware, malware, DDoS, MITM, and phishing	45	Mitigate
2	Leakage of access rights (administrator username and password)	41	Mitigate
3	Brute-force or phishing attacks against administrator credentials	41	Mitigate
4	Exploitation of system vulnerabilities in the server by external parties	38	Mitigate
5	Weak network configuration	35	Mitigate

No.	Area of Concern (AP)	Relative Risk Score	Level
6	Easy physical access surveillance in the data center	34	Mitigate
7	Absence of encryption standards	33	Mitigate
8	Lack of data-center staff awareness of security practices or privacy policy violations	28	Defer
9	No enforcement of password-change procedures in the system applications	27	Defer
10	No analysis of application logs	26	Defer
11	No alternative power sources and limited UPS capacity	25	Defer
12	Server downtime due to hardware failure	24	Defer
13	Bugs/errors during system updates	23	Defer
14	Internet connectivity disruptions by the service provider	23	Defer

This study combined the OCTAVE Allegro framework with the Delphi method to assess information-security risks at the Naval Base Data Center. Fifteen experts participated in three Delphi rounds to reach a valid consensus on risks that could disrupt data-center operations .

Delphi Round Outcomes

1. **Round 1:** Experts evaluated 21 initial risk factors. The Item-level Content Validity Index (I-CVI) ranged from 0.33 to 1.00, with most items rated perfectly valid (I-CVI=1.00). Four factors fell below the acceptability threshold and were removed, leaving 17 items. The sum of I-CVIs was 0.90, and the Scale-level CVI (S-CVI/Ave) was 0.81, indicating overall acceptable validity .
2. **Round 2:** The remaining 17 factors were re-rated, yielding I-CVI values between 0.53 and 1.00. S-CVI/Ave rose slightly to 0.82. Three additional factors failed to meet the cutoff and were excluded, resulting in 14 retained items .
3. **Round 3:** All 14 factors were reassessed. I-CVI values approached 1.00 across the board, and S-CVI/Ave reached 1.00—signifying unanimous expert agreement. No further deletions were necessary, confirming the final risk set's strong validity .

Risk Leveling and Prioritization

Using the Relative Risk Score—computed by combining each threat's impact-weighted score—risks were classified into three priority tiers :

1. **Mitigation (Score 30–45):** Immediate action required. Top risks included cyberattacks (ransomware, DDoS, malware, phishing) with a score of 45; administrator credential leaks (41); and brute-force or phishing attacks on admin accounts (41).
2. **Defer (Score 16–29):** Secondary priority. Examples: internet outages (23) and unlicensed-software bugs during updates (23).
3. **Accept (Score < 15):** Low priority; no further mitigation needed. No factors fell into this category in our study.

Implications

The findings underscore the necessity of promptly mitigating high-scoring threats—especially sophisticated cyberattacks and credential exploits—to prevent serious operational disruptions. The unanimous consensus achieved in Round 3 (S-CVI/Ave=1.00) provides a robust foundation for crafting structured, standards-aligned mitigation policies. Lower-scoring risks may be addressed over longer timelines but should not be ignored entirely. Overall, this research offers a clear roadmap for focusing resources on the most critical risks, thereby enhancing the data center's security posture and ensuring uninterrupted naval operations.

CONCLUSION AND RECOMMENDATION

This study demonstrates that combining the OCTAVE Allegro methodology with the Delphi technique effectively identifies and prioritizes information-security risks at the Naval Base Data Center. Through three Delphi rounds, fifteen experts validated fourteen critical risk factors—most notably cyberattacks, credential leaks, and brute-force attempts—that pose serious threats to data and operational continuity. Mitigation measures aligned with ISO/IEC 27002:2022 were found to significantly reduce these risks, with the highest-scoring threats receiving top priority for immediate action. The unanimous expert consensus achieved in Round 3 (S-CVI/Ave = 1.00) confirms the validity and applicability of the recommended controls. Consequently, this research not only maps the key vulnerabilities of the data center but also provides a structured, standards-based mitigation roadmap to strengthen its security posture and operational resilience.

FUTHER STUDY

This work opens several avenues for further investigation. Future studies could evaluate the real-world effectiveness of the proposed mitigation strategies—especially against high-risk threats like cyberattacks and credential compromise. Comparative analyses between OCTAVE Allegro and alternative risk frameworks (e.g., NIST SP 800-30, ISO 27005, or FAIR) would reveal which model best suits military or government data-center environments. Human factors, such as staff security awareness and the impact of training programs and policy enforcement on risk management, also warrant deeper exploration. Longitudinal research could track risk evolution and measure mitigation success over time. Finally, assessing the performance of deployed security technologies (firewalls, IDS/IPS, encryption solutions) will yield insights into their effectiveness against increasingly sophisticated cyber threats.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support of the Indonesian Navy's School of Staff and Command (Sekolah Staf dan Komando TNI AL) for providing invaluable insights and expertise that made this research possible.

REFERENCES

27002:2013, I. (2013). ISO 27002 : 2013 Code of practice for information security controls ISO 27002 : 2013 Code of practice for information security controls. 1–114.

Almanasreh, E., Moles, R., & Chen, T. F. (2018). Research in Social and Administrative Pharmacy Evaluation of methods used for estimating content validity. Research in Social and Administrative Pharmacy, xxxx, 0–1. https://doi.org/10.1016/j.sapharm.2018.03.066

Annisa Y. (2024). PERBAIKAN PROSES PENENTUAN PRIORITAS MITIGASI RISIKO ASET INFORMASI PADA KERANGKA KERJA OCTAVE ALLEGRO MENGGUNAKAN METODE MULTI-CRITERIA DECISION MAKING (MCDM).

Aulia Faradilla Setyowardhani, Ida Nurlela, Jenyta Primaranti, V., & Ghrandiaz, Y. (2023). Analisis Resiko Keamanan Informasi Website Repository Digital Library Menggunakan Framework ISO/IEC 27001 & 27002: Studi Kasus Perguruan tinggi X. Jurnal Riset Multidisiplin Dan Inovasi Teknologi, 2(01), 327–373. https://doi.org/10.59653/jimat.v2i01.500

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1–13. https://doi.org/https://doi.org/10.1016/j.ejor.2015.12.023

Budarsa, N., Indrawan, G., & Gunadi, A. (2022). ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ANALYTICAL HIRARCHY PROCESS PADA DATA CENTER PEMERINTAH KABUPATEN BULELENG. Jurnal Ilmu Komputer Indonesia (JIK), 7(1).

Buzan, B. (2008). People, States & Fear: An agenda for international security studies in the post-Cold War period: An Agenda for International Security Studies in the Post-cold War Era (ECPR Classics). 311. http://www.amazon.co.uk/People-States-Fear-international-International/dp/0955248817

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). The OCTAVE Allegro Guidebook, v1.0. http://www.sei.cmu.edu/publications/pubweb.html

Christian, L. (2015). Model Application of Accounting Information Systems of Spare Parts Sales and Purchase on Car Service Company. ComTech: Computer, Mathematics and Engineering Applications, 6(3), 371. https://doi.org/10.21512/comtech.v6i3.2227

Flanagan, T., Ashmore, R., Banks, D., & MacInnes, D. (2016). The Delphi method: Methodological issues arising from a study examining factors influencing the publication or non-publication of mental health nursing research. Mental Health Review Journal, 21(2), 85–94.

Ginting, A.J.B., Rahmadani, D., Sembiring, M.L., Saragih, L.S., & Putriku, A. E. (2024). Kemajuan Teknologi Informasi dalam Perkembangan Bisnis Global Advances in Information Technology in Global Business Development. Perkembangan Bisnis Global. Jurnal Kreativitas Ilmiah Mahasiswa, 2(4), 71–79.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Trans. Inf. Syst. Secur., 5(4), 438–457. https://doi.org/10.1145/581271.581274

Gunduz, M., & Elsherbeny, H. A. (2020). Operational framework for managing construction-contract administration practitioners' perspective through modified Delphi method. Journal of Construction Engineering and Management, 146(3), 4019110.

Istiningrum, A. A. (2012). Implementasi Penilaian Risiko Dalam Menunjang Pencapaian Tujuan Instansi Pendidikan. Jurnal Pendidikan Akuntansi Indonesia, 9(2). https://doi.org/10.21831/jpai.v9i2.963

Kaplan, R. S., Mikes, A., & others. (2012). Managing risks: a new framework. Harvard Business Review, 90(6), 48–60.

Karakikes, I., & Nathanail, E. (2020). Using the delphi method to evaluate the appropriateness of urban freight transport solutions. Smart Cities, 3(4), 1428–1447. https://doi.org/10.3390/smartcities3040068

Knight, F. H. (1921). RISK, UNCERTAINTY AND PROFIT. In Die 100 wichtigsten Werke der Ökonomie (pp. 108–109). https://doi.org/10.34156/9783791046006-108

Lakmini, N., Reilly, G. O., Cameron, P., & Alwis, S. De. (2023). International Journal of Disaster Risk Reduction Developing a hospital disaster preparedness evaluation tool for Sri Lanka - A modified Delphi study. International Journal of Disaster Risk Reduction, 95(July), 103866. https://doi.org/10.1016/j.ijdrr.2023.103866

Lee, J., Lee, S. H., & Chang, G. T. (2020). Expert consensus on the development of a health-related questionnaire for the pediatric field of Korean medicine: a Delphi study. BMC Complementary Medicine and Therapies, 20, 1–13.

Marisa, R. da silva; R. de C. (2021). Contributions of the Delphi technique to the validation of an occupational therapy assessment in the visual impairment field 1. Brazillian Journal of Occupational Theraphy, 1–15.

Mintrom, M. (2015). Herbert A . Simon , Administrative Behavior : A Study of Decision-Making. January 2016, 1–11. https://doi.org/10.1093/oxfordhb/9780199646135.013.22

Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. Information and Management, 42(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Pangestu, D. W. (2007). Teori Dasar Sistem Informasi Manajemen (SIM). IlmuKomputer. Com.

Parker, D. B. (1998). Fighting computer crime: a new framework for protecting information. John Wiley \& Sons, Inc.

Prajanti, A. D., & Ramli, K. (2020). A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods.

Puriwigati, A. N., & Buana, U. (2020). Sistem Informasi Manajemen-Keamanan Informasi. Jakarta. Retrieved Mei, 20, 2022.

Ramjanati, P., Kurnia Wijaya, F., & Son Muarie, M. (2021). Penilaian Risiko Keamanan Informasi Menggunakan Octave Allegro: Studi Kasus pada Perguruan Tinggi. 7(1).

Ramke, J., Evans, J. R., Habtamu, E., Mwangi, N., Silva, J. C., Swenor, B. K., Congdon, N., Faal, H. B., Foster, A., & Friedman, D. S. (2022). Grand Challenges in global eye health: a global prioritisation process using Delphi method. The Lancet Healthy Longevity, 3(1), e31–e41.

Roya, F., & Behrooz, F. (2017). Item Selection and Content Validity of the Risk Factors of Post-Intubation Tracheal Stenosis Observation Questionnaire for ICU-Admitted Patients Study design. 16(1), 22–33.

Stancine, K., Rocha, S., Silvestre, C. C., Maria, E., Jesus, S. De, Pereira, D., & Júnior, D. L. (2019). Development and content validation of an instrument to support pharmaceutical counselling for dispensing of prescribed medicines. September 2018, 1–8. https://doi.org/10.1111/jep.13102

Vuda, K. V., & Sarwat, A. I. (2023). Cyber-Secure Critical Infrastructure. 1–26.

Widyaksa, A., Subakti, U., Suharyo, O. S., Purnomo, J., & Susilo, A. K. (2024). Impact Assessment Of Minimum Essential Force (MEF) Achievement Of Indonesian Navy Using Integrated Delphi-Ahp-Topsis. Jurnal Maritime Research.