Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 5 Iss. 2 April 2025, pp: 635-644
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Analysis of Employee Capacity Gap in Managing Network Security and Its Implementation Towards Insider Threat Prevention

Felix Noel Sitorus[1], Ruki Harwahyu[2*]

[1,2]Department of Electrical Engineering, Faculty of Engineering,
Universitas Indonesia, Indonesia

E-Mail: ruki.h@ui.ac.id

Received Dec 3rd 2024; Revised Feb 24th 2025; Accepted Mar 6th 2025; Available Online Apr 13th 2025, Published Apr 13th 2025
Corresponding Author: Ruki Harwahyu

Abstract

Network security is crucial for protecting organizational information in the rapidly evolving digital era. Threats to networks do not only come from external sources, such as malware or hacking, but also from within the organization, known as insider threats. These threats can cause significant losses, whether due to intentional or unintentional actions by employees or internal parties with access to the system. Therefore, employees' ability to manage network security is key to addressing these threats. Handling insider threats must be a top priority for organizations. This study aims to analyze the employee capacity gap in managing network security and its impact on preventing insider threats in XYZ Organization. By implementing ISO 27001 security standards, particularly within the context of the Information Security Management System (ISMS) using the PDCA approach, this research evaluates how human resource management relates to information asset management and network security maintenance. The findings indicate that gaps in employees' knowledge and skills regarding network security significantly contribute to vulnerabilities against insider threats. This study also highlights how the implementation of ISO 27001, which emphasizes asset analysis and the PDCA cycle, can help organizations improve information security governance and prevent insider threats.

Keyword: Employee Capacity, Gap Analysis, Insider Threat Prevention, ISO 27001, Network Security

1. INTRODUCTION

Network security is one of the critical aspects of protecting an organization's information assets in the ever-evolving digital era, as cybersecurity challenges are becoming increasingly complex. Threats to network security do not only originate from external parties such as malware and hacking; organizations also need to be vigilant against internal threats, commonly referred to as insider threats, which can cause significant damage to a company. These threats include malicious activities carried out by employees or internal parties with access to the system, either intentionally or unintentionally. One factor influencing an organization's ability to address these threats is the capacity of employees to manage network security. Therefore, addressing insider threats must become a primary focus for every organization [1].

Insider threats have rapidly become a serious concern for businesses. As evidenced by insider threat statistics, these cases have increased, and many businesses are unprepared to handle them. While implementing some of the best IT security software will certainly help, many challenges remain, especially when the attacker is right in the organization's "backyard." Figure 1 are three global insider threat statistics regarding their frequency, primary motivations, and top perpetrators.

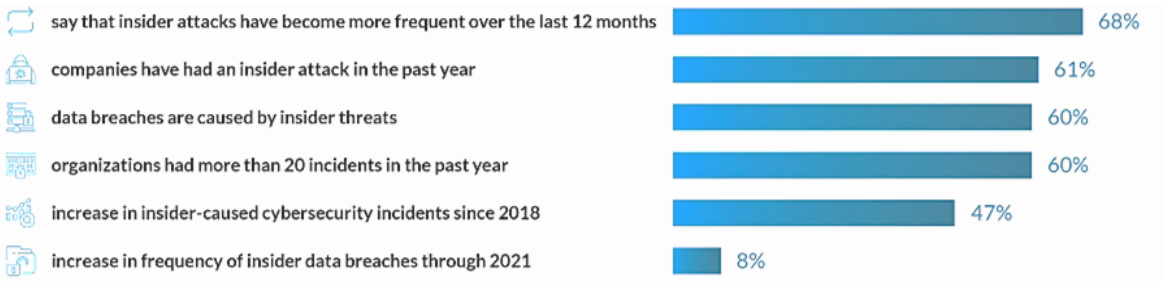

Figure 1. Statistics on Insider Threat Attack Frequency [2]

60% of data breaches are caused by insider threats [3]. 68% of organizations observed that insider threat attacks became more frequent over the past 12 months [4]. The number of cybersecurity incidents caused by insider threats increased by 47% since 2018 [5]. Another report predicts that insider threat-related data breaches will increase by 8% by 2021 [6]. 61% of companies experienced insider attacks in the past year [7]. 60% of organizations have more than 20 insider attack incidents annually [8]. In general, it can be shown in Figure 2.

Figure 2. Statistics on Primary Motivations for Insider Threats [7]

Fraud (55%), financial gain (49%), and intellectual property theft (44%) are the main motivations for insider threats [7]. In general, it can be shown in Figure 3.

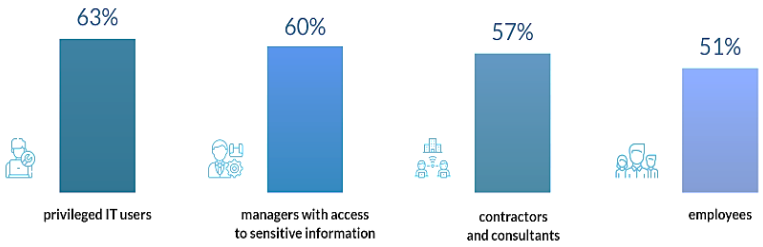

Figure 3. Statistics on Top Insider Threat Actors [7]

63% of organizations believe that privileged IT users pose the greatest insider threat risk [4]. 60% of companies identify managers with access to sensitive information as top insider threat actors, followed by contractors and consultants (57%), and permanent employees (51%) [7]. 78% of organizations lack highly effective processes for managing IT privileges [4].

There is no single, straightforward approach to deterring insider threats. Statistics reveal how organizations use various strategies/tactics and tools to combat these threats, including user behavior analytics, application audit systems/features, user training, and information security governance [2]. Insider threats are a serious challenge in cybersecurity requiring special attention and effective prevention strategies. By implementing strict access policies, closely monitoring activities, providing security training, and utilizing advanced technology, companies can reduce the risks posed by insider threats [1], [2], [4], [6], [7], [9], [10], [11], [12]. Awareness and appropriate preventive actions are key to protecting company data and systems from potential damage caused by insider threats [12], [13].

One tactic for organizations to combat insider threats is basic mitigation through implementing information security governance [2]. Mitigating this threat involves ensuring employees have adequate capacity to manage network security. The ISO 27001 standard, through the implementation of an Information Security Management System (ISMS) and the Plan-Do-Check-Act (PDCA) approach, plays a crucial role in enhancing information security management and preventing insider threats. Information security is a preventive measure against various information misuse threats and protection for information assets to ensure business process continuity and reduce business risks [14].

The application of ISO 27001 allows organizations to measure performance and provide relevant information about information security [15]. Through such evaluations, companies can ensure the readiness level of information security implementation and use it as a basis for evaluating and developing information security management as an effort to combat insider threats through basic mitigation via information security governance.

Organization XYZ, as an institution relying on network systems, faces challenges in ensuring its employees have sufficient competence to prevent and handle insider threats. However, capacity gaps among employees can create vulnerabilities that enable these threats. Therefore, an in-depth analysis of employee capacity gaps in managing information security and the implementation of insider threat prevention is needed as a strategic step to strengthen organizational security. This necessity prompted the study, "Analysis of Employee Capacity Gaps in Managing Network Security and Its Implementation on Insider Threat Prevention."

This study aims to analyze employee capacity gaps in managing network security and their implications for insider threat prevention in Organization XYZ. The research employs a qualitative-descriptive approach, collecting data through in-depth interviews, surveys, and document studies. The findings indicate that gaps in

employees' knowledge and skills related to network security significantly contribute to vulnerabilities to insider threats. The study also highlights how implementing ISO 27001, which emphasizes asset analysis and the PDCA cycle, can assist organizations in improving information security governance and preventing insider threats.

2. MATERIALS AND METHOD

This study employs a descriptive qualitative approach by conducting in-depth interviews with employees involved in network security management. Data is also collected through observation and documentation related to information security policies and the implementation of ISO 27001 in organization XYZ. This stage of research uses the Plan, Do, Check, Act (PDCA) approach, which is a cycle or management method designed to make process improvement and effectiveness of a process or system continuously or continuously, such as a circle that does not have an end [37],[38], based on data collected and analyzed. Research method it can be shown in Figure 4.

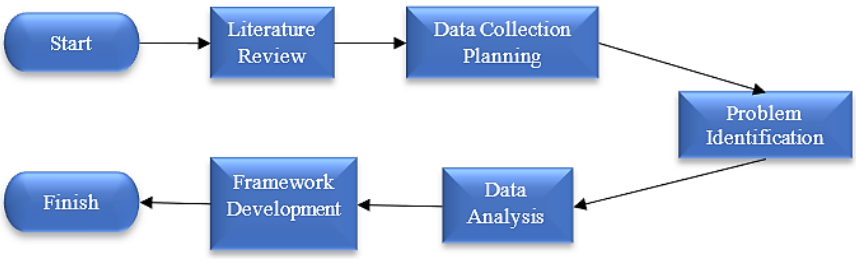

Figure 4. Research Methodology

2.1. Plan Phase

This phase consists of defining security policies that can be used for a series of processes in network security operations that will be the policy and basis of implementation as well as ISO/IEC 27002 relating to network security and access control to address the threat of insider threat of XYZ company that allows businesses to implement appropriate security as well as regardless of the value of threats and vulnerabilities to information security that can occur.

2.2. Do Phase

This stage is the implementation of the results of the plan stage, carried out by asking the Information Technology (IT) division at company XYZ and seeing the situation there directly. This Do Phase is carried out with a series of activities as follows:

2.2.1 Identifying Risks

Identifying and Calculating Asset Value. The first stage in risk identification is to identify assets in the IT division related to informatization. There are two types of assets, key assets and supporting assets. After all the assets of the IT division of company XYZ are identified, the next thing is to do a calculation to find out how much each asset is worth. The researcher calculated the value of assets based on the aspects of information security, namely confidentiality, integrity and availability.

Identifying weaknesses, threats, and assessing assets. Weaknesses are one of the threats to information security procedures, planning, implementation or control in the IT division to protect their information, and basically weaknesses have different vulnerabilities. A threat is an event that can harm business processes in the IT division. The purpose of this stage is to find possible threats that can compromise the system in the IT division. The result of this stage is a list of weaknesses and threats that may harm the IT division. Furthermore, weaknesses and threats were identified using ISO/IEC 27001 as a code practice to maximize asset maintenance and then access control on its security. After finding out the weaknesses and threats to the assets in the IT division, the next thing is to determine the possibility of incidents to assets in the IT division carried out by the researcher with the Compliance Manager.

2.2.2 Analyzing and Evaluating Risks

After identifying the risks contained in the IT division, the risks that will later be faced by the IT division in the event of a failure in security. The next step is to conduct an analysis and evaluation of the risks that have been previously identified. The risk analysis and evaluation are:

1. Analyzing the Impact and Risk
2. Identifying the IT Division's Risk Level
3. Assess IT Division's Risk

2.3. Check Phase

From the results obtained at the do stage, the next stage is the check stage, which is to select the control objectives and network security controls that will be implemented in company XYZ based on the value of the information risk that has been assessed in the previous stage. At this stage, monitoring, review, and internal audit are carried out by conducting a maturity level using the System Security Engineering Capability Maturity Model (SSE-CMM). The steps in determining the maturity level are as follows:

1. Making a Statement
   After determining what control objectives and network security controls will be applied from the risk measurement, then a statement is made based on the security controls of each control objective selected to be implemented. This statement is created and adjusted based on the ISO/IEC 27001 standard.

2. Determination of Ability Level Values
   To assess the level of security capability in each statement, the System Security Engineering Capability Maturity Level (SSE-CMM) is used, it can be shown in Table 1.

Table 1. System Security Engineering Capability Maturity Level (SSE-CMM)

Skor	Average
1	Performed Informally
2	Planned and tracked
3	Well Defined
4	Quantitatively Controlled
5	Continuously Improving

3. Determination of Maturity Level
   The determination of maturity level is the average of all security controls for which the capability level has been calculated, each clause has several control objectives, and each control objective has several information security controls, the average taken by each control objective and the average of the entire clause that produces the maturity level value in the clause.

2.4. Act Phase

After obtaining the results of the check stage, the next step is the act stage. This stage is carried out to improve and develop network security management by providing recommendations for the objectives of control and information security control that have been assessed at the level of competence in the previous stage. The recommendations given refer to ISO/IEC 27001.

3. RESULTS

3.1. Plan Phase

1. Based on the results of the researcher's analysis, it was found that the organizational structure contained 20 parts where each part had one to two employees, but for the information security section there was only one person who handled it.
2. Analyze the company's vision and mission, with the vision of becoming a company with high finances and becoming a role model, especially human capital, but with the problems found, the vision has not fully run according to expectations. And the analysis of the mission is to improve and facilitate the distribution of goods and services but with problems such as cyber-attacks that can disrupt company activities.
3. Policy determination is the purpose of the implementation of SMKI involving all employees of XYZ company, the head of the Information Technology division as the supervisor of the implementation of SMKI policies, and system security control is carried out in stages.
4. There are 17 asset lists with types of hardware, software, and supporting facilities.

3.2. Do Phase

The following is a conclusion from the identification of the average results of probability and threat value on the main asset and the supporting asset. The assessment is carried out based on decimal rounding above 0.5 for each category of threat value on the asset (Table 2 and Table 3).

Table 2. Conclusion of Average Results of Probability and Threat Value of Major Assets

No	Asset Name	Threat Level	Low	Medium	High
1	Internal Web Portal Database	0,36		□	
2	RQM (Risk Quality Management)	0,26	□		
3	Employee Database	0,38		□	
4	Legal and Compliance Database	0,31	□		

No	Asset Name	Threat Level	Low	Medium	High
5	Internal GCG Database	0,30			
6	Knowledge Management Database	0,30			
7	Oracle Hyperion Planning Database	0,24			
8	Management Information System Database	0,30			

Table 3. Conclusion of Average Results of Probability and Threat Value of Supporting Assets

No	Asset Name	Threat Level	Low	Medium	High
1	Personal Computer (PC)/Laptop	0,25			
2	Server Physical	0,40			
3	Windows server 2012 R.2	0,35			
4	Windows 10	0,25			
5	Microsoft Office 2016	0,25			
6	Microsoft SQL Server 2008	0,30			
7	Air Conditioner (AC)	0,37			
8	Uninterruptible Power Supply (UPS)	0,30			
9	Fiber Optic	0,30			
10	CCTV	0,36			
11	Switch	0,35			
12	Wi-Fi	0,35			
13	Aplikasi IT Service Desk	0,30			
14	Oracle Database 11.2.0.1	0,30			
15	Avira Antivirus 2019	0,30			
16	Kaspersky Antivirus 2018	0,30			
17	Server Storage	0,30			

1. Identify risks
   a. Based on the identification and calculation of asset values, it was found that the value of the main asset with a value of 8-11 and the value of supporting assets with a value of 3-7
   b. The result of the identification of weaknesses, threats, and value in assets is that the main and supporting assets are in the Low-Medium category

2. Analyze and evaluate risks
   a. The results of analyzing the impact and risk on the main and supporting assets, namely the Business Impact Analysis (BIA) value is in the very high critical category, namely assets that have a great influence on the company's work processes
   b. Identify the risk level on the main and supporting assets with a BIA value of 80- 95
   c. The results of assessing the risk in the IT division, namely business risks that can occur due to old vendors handling them, the risk of data loss, and natural disasters.

3.3. Check Phase

3.3.1 Selecting Control Objectives and Safety Controls

After taking measurements on the security asset, the researcher takes actions or controls that can reduce the risk. The selection of control and security control objectives in this study is based on the control and security control objectives of ISO/IEC 27001, by making adjustments to the results of the risk assessment obtained on information security assets in XYZ company. The selection of clauses was carried out using ISO/IEC 27001.

3.3.2 Selecting As a Clause of ISO/IEC 27001

The table 4 is a mapping carried out by the researcher based on the clauses of ISO/IEC 27001.

Table 4. Objectives of Controls and Safety Controls (ISO/IEC 27001)

Clause	Control Objective	Security Control
Human Resource Security	During Work	1. Management Responsibilities 2. Information Security Awareness, Education, and Training 3. Disciplinary Process
	Termination of Employment and Job Changes	Responsibilities for Termination of Employment and Job Changes
Physical and Environmental Security	Secure Areas	1. Scope of Physical Security 2. Physical Access Control 3. Working in Secure Areas
	Equipment	1. Equipment Protection and Placement

Clause	Control Objective	Security Control
		2. Support Requirements 3. Cabling Security 4. Clean Desk and Clear Screen Policy
Information Security Incident Management	Information Security Incident Management and Improvement	1. Responsibilities and Procedures 2. Information Security Incident Reporting 3. Collection of Evidence
Adjustment	Compliance with Legal and Contractual/Agreement Requirements	Intellectual Property Rights

3.3.3 Determination of Auditee

The definition of an auditee in ISO/IEC 27001 is still unclear. Therefore, the researcher used the RACI (Responsible, Accountable, Consulted and Informed) Chart from COBIT. The determination of the auditee is based on the correlation between COBIT and ISO/IEC 27001.

Table 5. Mapping the COBIT 5 Domain with ISO/IEC 27001 Clause

COBIT 5	ISO 27001
APO07 (Manage Human Resources)	Clause 7 (Human Resource Security)
APO13 (Manage Security)	Clause 11 (Physical and Environmental Security)
DSS02 (Manage Service Requests and Incidents)	Clause 16 (Information Security Incident Management)
MEA03 (Monitor, Evaluate and Assess Compliance with External Requirements)	Clause 18 (Compliance)

3.3.4 Determining the Capability Level Value for the System Security Engineering Capability Maturity Model (SSE-CMM)

Determination of the level of capability to determine the level of maturity that can describe the measurement of the extent to which the IT division can meet the standards of the security management process well, where the maturity level assessment is carried out to each control in accordance with the audit carried out.

Table 6. Determining the Ability Level Value

COBIT Functional Structure Related to Research	Functional Division of Information Technology (IT)
Compliance	IT Division Compliance Manager
Information security manager	IT Division Security Officer
Head IT Operations	IT Division Data and Information Administrator
Chief Risk Officer	IT Division Risk and Quality Management Manager

The list of questions created in this study was created based on the security controls of each control objective selected and applied to the IT division of company XYZ. A list of questions created based on the ISO/IEC 27001 standard. This study uses a maturity level with the System Security Engineering Capability Maturity Level (SSE-CMM).

1. Choosing an objective control
2. Opt for a portion of ISO/IEC 27001 clauses
3. Determine the maturity level at:
    a. Clause 7 Human Resource Security with a result of 1.5 (done informally)
    b. Clause 11 Physical and Environmental Security with a result of 1.4 (done informally)
    c. Clause 16 Information Security Incident Management and Improvement with a result of 1.58 (conducted informally
    d. Clause 18 Adjustments with results 2.3 (planned and tracked).

3.4. Act Phase

After assessing the maturity level of the control objectives and information security controls, the researcher determined the recommendations that would be used to improve security controls. The recommendations produced came from observations and interviews conducted by researchers at company XYZ. The maturity level value of the average of all clause values after all assessments have been completed. The table 7 is a representation of the results of the maturity level assessment of the average of the overall clause value.

Table 7. ISO/IEC 27001 Clause Maturity Level Results

ISO 27001:2013 Clause	Maturity Level
Resource Security	1,5
Physical and Environmental Security	1,4
Incident and Security Management	1,58
Adjustment	2,3

After a maturity level assessment, analysis, and evaluation, the next is the determination of conditions, whether it is in accordance with the ISO/IEC 27001 standard and the provision of recommendations. Recommendations can be used for improvements in company XYZ.

Table 8. Findings and Recommendations based on ISO/IEC 27001

Human Resource Security					
Management Responsibilities					
Control	Usage Guidelines	Implementation		Evidence	GAP
		Yes	No		
All employees and other relevant parties associated with the organization implement information security in accordance with policies and procedures	The availability of an organizational information security guide aligned with national information security standards		□		Based on management controls, the organization should provide guidelines related to information security
	The provision of motivation, learning programs for skill enhancement, and qualification processes for fundamental competencies related to information security		□		Based on management controls, the organization should implement activities that motivate and enhance employees' skills in information security

Recommendation:

1. Management needs to provide guidelines that comply with national regulations regarding information security within the organization.
2. Management needs to organize activities to motivate employees and develop their fundamental skills related to information security.

From the results of the study, it can be seen that ISO/IEC 27001 focuses on policies for companies or agencies that have not implemented information technology policies before.

1. Determine the gap and
2. Provide recommendations from the results of the check stage
    a. Clause 7 Human Resource Security:
        1) The need for information security guidelines in accordance with the role of the organization based on state regulations
        2) The need for education and training facilities to improve employee capabilities related to information security
    b. Clause 11 Physical and Environmental Security:
        1) It is necessary to place it according to the security needs of the asset
        2) The need to supervise visitors who come, and the awareness of employees on the use of identity cards
        3) The need to increase personnel awareness related to the work area
    c. Clause 16 Information Security Incident Management and Improvement:
        1) The need for procedures for planning and preparing for incident response
        2) The need for security control reporting and physical breaches
        3) The need for procedures for the security of evidence and documentation
    d. Clause 18 Adjustments:
        1) The need for an IPR compliance policy on the legitimate use of software and information products

4. DISCUSSION

Based on the results discussed in the previous chapter, it can be concluded that the report from the analysis results can be used to achieve security management system standards by using ISO/IEC 27001 as a safety recommendation and improvement. The following are the results of this study using the Plan, Do, Check, Act method. It can be seen that the evaluation of ISO/IEC 27001 uses four (4) clauses, namely clause 7 (human

resource security), clause 11 (physical and environmental security), clause 16 (incident management), and clause 18 (adjustment). From the four clauses, it is known that clause 18 is at level two compared to other clauses that are still at level one. From the explanation of ISO/IEC 27001 above, it can be seen that there is still a lack of attention from the managerial side regarding the determination and determination of policies on information security. Where from these two standards, it is known that operational activities are running with planning but there is still a lack of determination and determination of existing policies related to security in company XYZ.

5. CONCLUSION AND RECOMMENDATION

5.1. Conclusion

1. Employee Capacity Gap
   The employee capacity gap in understanding and implementing network security procedures in XYZ Organization creates vulnerabilities that can be exploited by insider threats. The analysis indicates that:
   a. Risks to key assets (scores 8-11) and supporting assets (scores 3-7) fall into the Low-Medium category. However, without mitigation, these risks may escalate.
   b. For assets with a BIA score of 80-95, the risk is categorized as Very High Critical, indicating a significant impact on the company's operations if an insider threat occurs.

2. Impact of Employee Capacity Gaps on Insider Threat Prevention
   a. Gaps caused by insufficient training and understanding of security policies increase the likelihood of insider threat exploitation.
   b. Disruptions to key and high-value supporting assets can significantly impact organizational performance.
   c. Mitigation through employee capacity enhancement and the implementation of an effective risk management system is a priority to reduce risk.

3. Implementation of ISO 27001 in Managing Network Security
   a. Risk evaluation based on ISO 27001 highlights the need for improvement in several key clauses, particularly:
      1) Clause 7 (Human Resource Security): A score of 1.5 indicates the need for better workforce training and management.
      2) Clause 11 (Physical Security): A score of 1.4 emphasizes the necessity of strengthening physical access controls.
      3) Clause 16 (Incident Management): A score of 1.58 highlights the importance of improving security incident response.
      4) Clause 18 (Compliance): A score of 2.3 indicates better legal compliance, but consistency is required.

4. Mitigation Strategies
   a. Focus on Employee Training and Awareness
      Minimizing security gaps by enhancing knowledge and enforcement of security policies.
   b. Prioritizing High-Risk Areas
      Developing mitigation plans that include protection for key and high-value supporting assets.
   c. Continuous Improvement Based on ISO 27001
      Utilizing risk evaluation results to guide ongoing improvements, covering technical, human, process, and legal compliance aspects.

5.2. Recommendations

Based on the research findings, XYZ Organization should promptly:

1. Enhance employee capacity through regular training.
2. Integrate risk evaluations with a comprehensive network security strategy.
3. Implement relevant security controls based on ISO 27001 standards to strengthen defenses against insider threats.

REFERENCES

[1] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 20, no. 2, pp. 389–396, May 2021, doi: 10.30812/matrik.v20i2.1093.

[2] BSSN, 'BSSN: Indeks Keamanan Siber RI Peringkat 24 dari 194 Negara' CNN Indonesia. Accessed: Jan. 02, 2025. [Online]. Available: https://www.cnnindonesia.com/teknologi/20210907150335-185-

690926/bssn-indeks-keamanan-siber-ri-peringkat-24-dari-194-negara
[3] M. said Hasibuan and R. Y. Rahman, "Evaluasi Keamanan Informasi Pada Sman 1 Xyz Menggunakan Indeks Kami Versi 4.2," JURNAL FASILKOM, vol. 13, no. 02, pp. 181–187, Aug. 2023, doi: 10.37859/jf.v13i02.4916.
[4] F. Olaoye, "Insider Threat Detection and Prevention," 2024. [Online]. Available: https://www.researchgate.net/publication/383565287
[5] nd Darian Rizaludin and M. Noor Al-Azam, "Automatic Sign of Commencement of Work from Enterprise Resource Planning." [Online]. Available: http://ip.address.api/index.php?
[6] D. Hariyadi, M. Kusuma, and A. Sholeh, "Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework," 2021.
[7] A.-H. Julianda, R. Fauzi, R. A. Nugraha, and J. S. Informasi, "Pages 242-255 ISSN : 2597-4084 Published By STIE Amkop Makassar Analisis Dan Perancangan Domain Data Security Management Menggunakan Dama," 2022.
[8] R. N. J. Meimo Nakashita et al., "Analisis Manajemen Risiko Teknologi Informasi dengan Metode FMEA dan Kontrol ISO 27001:2013 Pada Perusahaan Kontruksi Kapal," Jurnal Ilmiah Media Sisfo, vol. 18, no. 2, pp. 166–176, Oct. 2024, doi: 10.33998/mediasisfo.2024.18.2.1795.
[9] M. Abdul, F. Ys, B. Parga Zen, and D. E. Wasitarini, "Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi," 2023.
[10] A. Lisa Maryanto, M. Noor Al Azam, A. Nugroho, and P. Sistem Informasi, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami Evaluation Of Information Security Management In Technology-Based Beginning Company Using The Kami Index," vol. 11, no. 1, 2022.
[11] I. M. Lopes, T. Guarda, and P. Oliveira, "Implementation of ISO 27001 Standards as GDPR Compliance Facilitator," Journal of Information Systems Engineering and Management, vol. 4, no. 2, 2019, doi: 10.29333/jisem/5888.
[12] J. Kajian Stratejik Ketahanan Nasional Jurnal Kajian Stratejik Ketahanan Nasional Volume, R. Hendra Kurniawan, A. Rivai Ras, R. Hendra, and A. Rivai, "Analisis Ancaman Terhadap Penerapan Framework Manajemen Insiden Di Indonesia," 2019. [Online]. Available: https://scholarhub.ui.ac.id/jksknAvailableat:https://scholarhub.ui.ac.id/jkskn/vol2/iss2/4
[13] P. Perpustakaan Daerah Provinsi Sumatera Selatan, C. Renaldi Simanjuntak, S. Akbar Pratama, G. Barovih, and I. Teknologi dan Bisnis Palcomtech, "Remanajemen Jaringan Menggunakan Framework NIST Network Remanagement Using the NIST Framework at the Regional Library of South Sumatra Province," 2023.
[14] I. Herrera Montano, J. J. García Aranda, J. Ramos Diaz, S. Molina Cardín, I. de la Torre Díez, and J. J. P. C. Rodrigues, "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat," Cluster Comput, vol. 25, no. 6, pp. 4289–4302, Dec. 2022, doi: 10.1007/s10586-022-03668-2.
[15] R. A. Alsowail and T. Al-Shehari, "Techniques and countermeasures for preventing insider threats," PeerJ Comput Sci, vol. 8, 2022, doi: 10.7717/PEERJ-CS.938.
[16] M. N. Al-Mhiqani et al., "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," Aug. 01, 2020, MDPI AG. doi: 10.3390/app10155208.
[17] Wikipedia, "Manajemen risiko." Accessed: Jan. 03, 2025. [Online]. Available: https://id.wikipedia.org/wiki/Manajemen_risiko#cite_note-1
[18] V. Yasin, S. Tinggi, M. Informatika, and D. K. Jayakarta, "Kajian Cyber Security Dalam Rangka Koperasi Menghadapi Revolusi Industri 4.0," 2023, doi: 10.52362/jisamar.v7i3.1132.
[19] H. Ardiyanti, "CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA." [Online]. Available: http://kominfo.go.id/index.php/content/detail/3980/
[20] M. Abdul, F. Ys, B. Parga Zen, and D. E. Wasitarini, "Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi," 2023.
[21] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis," IEEE Trans Eng Manag, vol. 68, no. 1, pp. 87–100, Feb. 2021, doi: 10.1109/TEM.2020.2977815.
[22] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking," Digital Transformation Technology, vol. 3, no. 2, pp. 857–863, Dec. 2023, doi: 10.47709/digitech.v3i2.3379.
[24] R. A. Alsowail and T. Al-Shehari, "Empirical detection techniques of insider threat incidents," IEEE Access, vol. 8, pp. 78385–78402, 2020, doi: 10.1109/ACCESS.2020.2989739.
[25] G. G. Prapenan and G. C. Pamuji, "Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013," in IOP Conference Series: Materials Science and

Engineering, IOP Publishing Ltd, Aug. 2020. doi: 10.1088/1757-899X/879/1/012047.
[26] Indonesiare, "Mengenal Standard ISO 27001." Accessed: Jan. 03, 2025. [Online]. Available: https://indonesiare.co.id/id/article/mengenal-standard-iso-27001
[27] K. S. Al Fajri and R. Harwahyu, "Information Security Management System Assessment Model by Integrating ISO 27002 and 27004," MALCOM: Indonesian Journal of Machine Learning and Computer Science, vol. 4, no. 2, pp. 498–506, Feb. 2024, doi: 10.57152/malcom.v4i2.1245.
[28] D. E. R. Hidayatullah, R. Kunthi, and R. Harwahyu, "Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department," International Journal of Electrical, Computer, and Biomedical Engineering, vol. 2, no. 3, Sep. 2024, doi: 10.62146/ijecbe.v2i3.81.
[29] ISO, "ISO/IEC 27001 and related standards Information security management, ISO," ISO. Accessed: Jan. 03, 2025. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html
[30] A. Lisa Maryanto, M. Noor Al Azam, A. Nugroho, and P. Sistem Informasi, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami Evaluation Of Information Security Management In Technology-Based Beginning Company Using The Kami Index," vol. 11, no. 1, 2022.
[31] J. Landers, S. Spence, and B. Morgan, "Evaluating the Effectiveness of Insider Threat Mitigation Preventive Measures."
[32] R. N. J. Meimo Nakashita et al., "Analisis Manajemen Risiko Teknologi Informasi dengan Metode FMEA dan Kontrol ISO 27001:2013 Pada Perusahaan Kontruksi Kapal," Jurnal Ilmiah Media Sisfo, vol. 18, no. 2, pp. 166–176, Oct. 2024, doi: 10.33998/mediasisfo.2024.18.2.1795.
[33] A. Intan Mafiana, L. Hanun, H. Mufidatul Ilmi, and S. Febriliani, "Implementasi Manajemen Keamanan Informasi Berbasis ISO 27001 Pada Sistem Informasi Akademik Universitas," Journal of Digital Business and Innovation Management JDBIM (Journal of Digital Business and Innovation Management, vol. 2, no. 2, pp. 139–163, 2023, doi: 10.1234/jdbim.v2i2.57580.
[34] P. Rachman, "Implementasi Plan-Do-Check-Act (Pdca) Berbasis Key Performance Indicators (Kpi): Studi Kasus Di Smp-Sma Integral Ar-Rohmah Dau Malang," Jurnal Manajemen Pendidikan Islam, vol. 04, no. 02, pp. 132–145, 2020, doi: 10.33650/al-tanzim.v4i2.
[35] F. Z. Zebua, A. B. Ndraha, and Y. Telaumbanua, "Evaluasi Implementasi Sistem Keuangan Desa (Siskeudes) Di Desa Orahili Tumori Evaluation Of The Emplementation Of The Village Financial Management System (Siskeudes) In Orahili Tumori Village," Jurnal EMBA, vol. 10, no. 4, pp. 1410–1416, 1410.
[36] O. A. Nurkholiq, O. Saryono, I. Setiawan, J. Fungsional, L. Kepala, and A. Ahli, "Analisis Pengendalian Kualitas (Quality Control) Dalam Meningkatkan Kualitas Produk", [Online]. Available: https://jurnal.unigal.ac.id/index.php/ekonologi