Intechno Journal :
Information Technology Journal
Vol. 7 No. 1 July 2025

Homepage: https://jurnal.amikom.ac.id/index.php/intechno

INTECHNO Journal
INFORMATION TECHNOLOGY JOURNAL

e-ISSN: 2655-1438
p-ISSN: 2655-1632

.

Integrating CVSS, OWASP, and APPI for a Comprehensive Risk Analysis of SQL Injection Vulnerabilities in E-Commerce

Muhammad Kholilul Adrian[1], Prajna Deshanta Ibnugraha[2], Hilal Hudan Nuha[3]
[1,2,3]Telkom University, Bandung, Indonesia

Article Info

Article history:

Received Jun 20, 2025
Revised Jul 21, 2025
Accepted Jul 30, 2025
Published Jul 31, 2025

Keywords:

SQL Injection
Risk Assessment
CVSS
OWASP
APPI (Act on the Protection of Personal Information)

ABSTRACT

Purpose: By integrating the technical severity evaluation provided by the Common Vulnerability Scoring System (CVSS), the business risk assessment framework of the OWASP Risk Rating Methodology, and the legal compliance standards outlined in Japan's Act on the Protection of Personal Information (APPI), this study aims to conduct a holistic risk analysis of SQL injection vulnerabilities within e-commerce platforms. The primary objective is to offer stakeholders a robust and actionable model for enhancing the security of online shopping environments.

Methods/Study design/approach: This study employed a mixed-methods experimental case study approach. A custom-built, intentionally vulnerable e-commerce web application was subjected to a simulated SQL injection attack to extract fictitious user and transaction data. The technical severity of the vulnerability was quantified using CVSS v3.1, while the OWASP Risk Rating Methodology was applied to assess the associated business risks. Additionally, the legal implications were evaluated in accordance with Japan's Act on the Protection of Personal Information (APPI).

Result/Findings: The simulation confirmed that a SQL injection attack could extract sensitive personal and transactional data. The vulnerability was rated "Critical" with a CVSS v3.1 score of 9.1, and the OWASP assessment indicated a "High" business risk due to financial impact, APPI non-compliance, and privacy violations. The leaked purchase history was classified under APPI as "Personal Information Requiring Special Attention."

Novelty/Originality/Value: This study's main contribution is its integrated methodology that links CVSS, OWASP, and APPI frameworks to assess cyber threats. It offers a multidimensional view, showing how a technical vulnerability can lead to serious legal and business consequences under specific data protection laws.

Corresponding Author:

Muhammad Kholilul Adrian
Email: muhammadkholilul16@gmail.com

1. INTRODUCTION

Since the onset of the Covid-19 pandemic, the e-commerce sector has experienced significant growth, creating expanded business opportunities while simultaneously increasing exposure to cyber threats such as SQL injection, which accounts for approximately 340 million attacks annually [1]. SQL, a programming language used for managing relational databases, is particularly vulnerable to input manipulation, making it a frequent target for exploitation. In addition to SQL injection, users' financial and personal data are also threatened by other forms of cyberattacks, including ransomware, malware, and phishing via email [2]. SQL injection is especially prevalent in PHP-based applications, where unvalidated input can enable unauthorized access to backend databases [3].

Personal data such as names, email addresses, and phone numbers possess considerable economic value but are highly vulnerable to misuse, particularly within cloud computing environments where multi-tenancy poses significant risks [2]. Research indicates that safeguarding sensitive information is essential for maintaining trust and ensuring business continuity [4][5]. Although the Common Vulnerability Scoring System (CVSS) is widely employed to assess the severity of security vulnerabilities, its reliability is compromised due to insufficient technical documentation [6]. To mitigate SQL injection attacks, the use of prepared statements and PHP Data Objects (PDO) is recommended as effective countermeasures [3].

Due to their vulnerability to authentication breaches, configuration flaws, and application-level attacks, large organizations must continuously update their security strategies [7][8]. While Information Security Risk Assessment (ISRA) emphasizes the importance of asset identification, the intangible nature of digital data introduces significant challenges [9][10]. In the realm of web applications, the OWASP Risk Rating Methodology offers adaptability by qualitatively assessing both impact and likelihood [11]. Despite the requirement under Japan’s Act on the Protection of Personal Information (APPI) to report data breaches within 72 hours, integration of these regulatory obligations with comprehensive risk analysis remains limited [12][13].

Data security is a fundamental component of both user trust and regulatory compliance, supported by technological measures such as firewalls, structured security protocols [14][4][5], and evaluations of system management effectiveness [10]. As cyber threats continue to evolve, the risk of large-scale data breaches remains a critical concern [15][8]. This study addresses an existing gap by integrating the APPI regulatory framework, the OWASP Risk Rating Methodology, and the CVSS scoring system to evaluate SQL injection vulnerabilities and their implications [6][11].

This study will analyze SQL injection data in relation to the Act on the Protection of Personal Information (APPI) to evaluate the significance of the compromised information using the OWASP Risk Rating Methodology and the Common Vulnerability Scoring System (CVSS). Furthermore, the research will propose preventive techniques against SQL injection to strengthen data security within e-commerce platforms. It is expected that the findings will assist e-commerce stakeholders in creating a secure and trustworthy online shopping environment.

2. METHOD

Through the use of SQL injection attack simulations, this methodology is intended to assess the effects of data leaks on e-commerce books. The risks are then examined using the OWASP and CVSS frameworks, which are connected to the APPI (Act on the Protection of Personal Information) regulations.
The process and steps to be carried out in this research are:

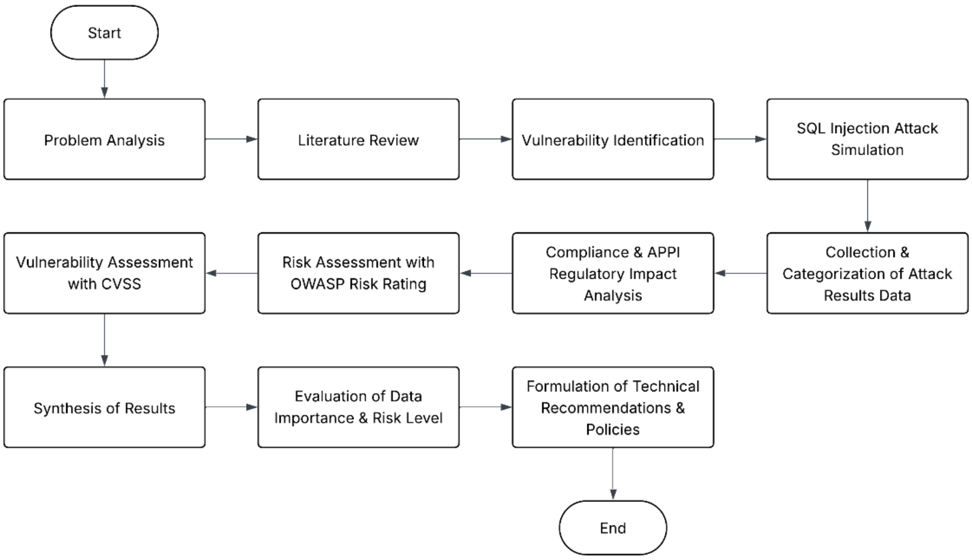
Start
Problem Analysis
Literature Review
Vulnerability Identification
SQL Injection Attack Simulation
Collection & Categorization of Attack Results Data
Compliance & APPI Regulatory Impact Analysis
Risk Assessment with OWASP Risk Rating
Vulnerability Assessment with CVSS
Synthesis of Results
Evaluation of Data Importance & Risk Level
Formulation of Technical Recommendations & Policies
End

Figure 1. Research flow diagram

.

2.1 Research Approach

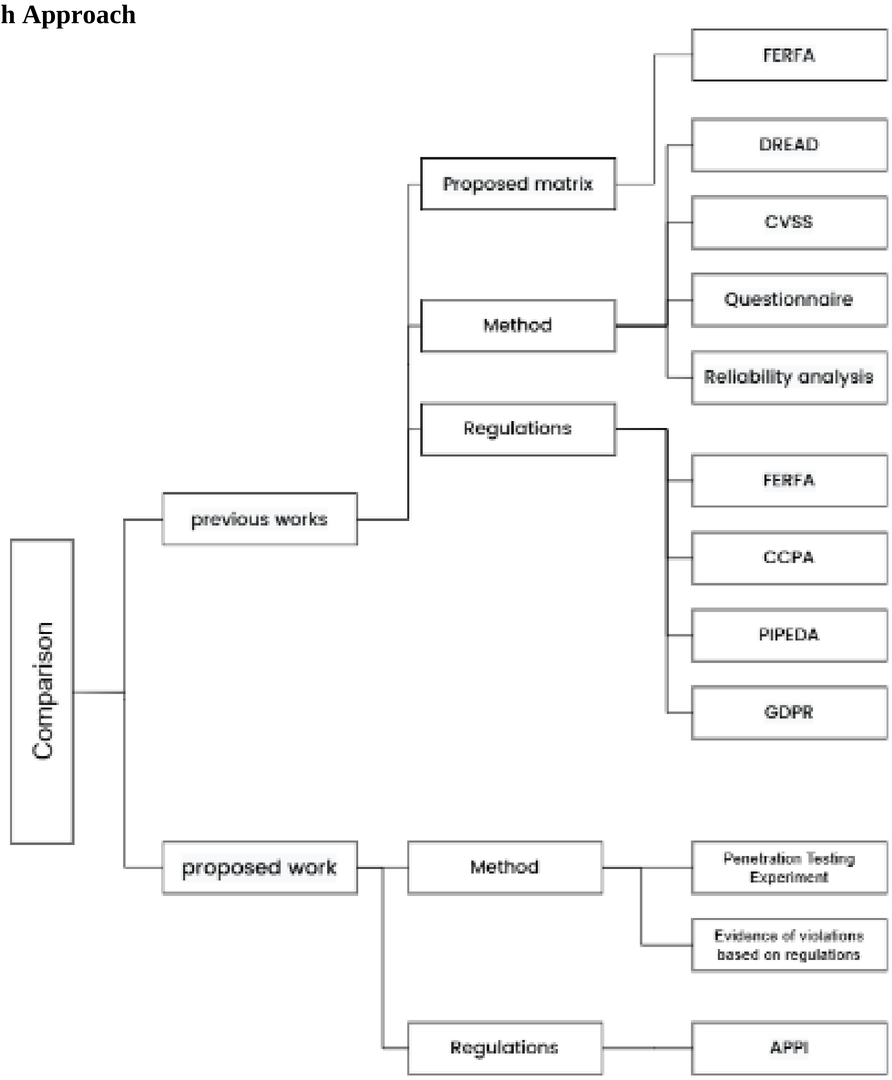

Figure 2. Proposed diagram

Using a mixed methods approach, this study incorporates both qualitative and quantitative analysis into an experimental case study design. On the quantitative side, the OWASP Risk Rating Methodology is used to analyze business risk, and the Common Vulnerability Scoring System (CVSS) is used to assess the technical severity of vulnerabilities. On the qualitative side, information gleaned from attack simulation results is examined and interpreted in light of APPI regulations, with a focus on determining what constitutes "Personal Information" and the associated legal ramifications. The controlled e-commerce setting used for this experimental case study simulates a cyberattack.

2.2 Research Object

The target system, test data, and the reference framework are the study's objects. The target system is a book-selling e-commerce web application that was purposefully created with SQL injection-prone technology, like outdated PHP versions. To ensure that no real personal data is used in the simulation process, the system's database is filled with dummy data that accurately mimics user data and transaction structures for testing purposes. The Common Vulnerability Scoring System (CVSS) version 3.1, the OWASP Risk Rating Methodology, and Japan's APPI regulations are the three primary frameworks cited in this study.

2.3 Research and Data Collection Stages

This study was conducted in the following methodical steps:

1) By emphasizing the discrepancy between security procedures in e-commerce applications and the compliance standards outlined in the APPI regulations, problem analysis seeks to develop the research focus based on the findings of the literature review.
2) The OWASP risk assessment methodology, the CVSS vulnerability assessment system, and the APPI regulatory documents were all carefully examined through a literature study.

3) The process of creating an e-commerce web application that was purposefully made to be susceptible to SQL Injection, deployed on a separate server, and filled with dummy data that mirrored the structure of actual user and transaction data was known as "test environment development and preparation."
4) Vulnerability identification was done by scanning the system with programs like OWASP ZAP and SQLMap to find attack-prone entry points.
5) The goal of the SQL Injection Attack Simulation was to extract data from the database, and every payload and successful attack step was meticulously recorded.
6) The process of gathering extracted data and classifying it into groups like Personally Identifiable Information (PII), authentication data, and transaction data is known as data collection and categorization.

2.4 Data Analysis Methods

This study employed three interrelated analytical techniques to evaluate the collected data. First, an impact analysis was conducted based on the APPI (Act on the Protection of Personal Information) to assess potential regulatory violations and their legal implications. This involved mapping each category of leaked data to the definition of "Personal Information" as outlined in the APPI. Second, the overall risk level was determined by assigning scores to both likelihood and impact factors using the OWASP Risk Rating Methodology. The business impact assessment incorporated potential legal penalties and reputational damage identified through the APPI analysis. Third, the technical severity of the vulnerability was objectively quantified using the Base Score metric from the Common Vulnerability Scoring System (CVSS) version 3.1.

2.5 Synthesis and Formulation of Recommendations

The final phase of this research involves synthesizing the findings and formulating actionable recommendations. This synthesis integrates the results from the three analytical frameworks—technical severity (CVSS), business risk (OWASP), and regulatory compliance (APPI)—to establish a comprehensive understanding of the interrelationships among them. The analysis focuses on identifying the highest impact scores and the most critical legal obligations associated with each data category to determine its overall criticality. Based on this assessment, specific technical mitigation strategies are proposed, including the implementation of a Web Application Firewall (WAF), the use of parameterized queries, and rigorous input validation.

3. RESULTS AND DISCUSSIONS

This section presents the results of the penetration testing experiments along with a comprehensive analysis of the findings. The evaluation was conducted by measuring three key dimensions: technical severity, business risk, and the implications for compliance with data protection regulations. These metrics provide a multidimensional perspective on the vulnerabilities identified and their potential impact within the context of e-commerce security.

3.1 Data Extraction Results Through SQL Injection

Penetration testing experiments conducted using the SQLMap tool successfully identified and exploited SQL Injection vulnerabilities in the id parameter of the tested e-commerce system. This exploitation enabled unauthorized data extraction from the master_db database. Among the accessible tables, Contact01 and transaction_journals were successfully retrieved, demonstrating the system's susceptibility to unauthorized access and data leakage.

The data successfully extracted included customer information that should have remained confidential. This finding confirms that the identified vulnerability is not merely theoretical but demonstrably exploitable in practice, enabling unauthorized access to various types of sensitive user data.

.

3.2 Severity and Risk Analysis

To measure the impact of vulnerabilities, quantitative analysis was performed using CVSS and OWASP Risk Rating.

1) Technical Severity Rating (CVSS v3.1)

The SQL Injection vulnerability identified in the system was assessed using the CVSS v3.1 scoring metric. Based on the evaluation parameters outlined in Table 1, the vulnerability received a score of 9.1, which falls under the "Critical" severity category. The corresponding vector string is CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N, indicating that the vulnerability is exploitable remotely without authentication, requires low attack complexity, and has a high impact on confidentiality and integrity, but no impact on availability.

Tabel 1. CVSS v3.1 Base Score Assessment

Metrics	Selected Values	Justification
Attack Vector (AV)	Network (N)	Exploitation is carried out from the public network.
Attack Complexity (AC)	Low (L)	No special conditions are required, only vulnerable inputs.
Privileges Required (PR)	None (N)	The attacker does not require authentication.
User Interaction (UI)	None (N)	No user interaction is required.
Scope (S)	Unchanged (U)	The attack remains within the same system boundaries.
Confidentiality (C)	High (H)	Personal data is successfully retrieved (name, email, address, transactions).
Integrity (I)	High (H)	There is potential for data modification.
Availability (A)	None (N)	Does not cause the system to become unavailable.

This Critical score highlights how dangerous this vulnerability is from a technical standpoint, as it is easy to exploit and has a maximum impact on the confidentiality, integrity, and availability of data.

2) Business Risk Assessment (OWASP)

Using the OWASP methodology, risks are assessed by considering probability and impact factors. The results, as shown in Table 2 dan 3, indicate a High risk level.

Table 2. OWASP Risk Rating Assessment Technical Impact Factors (TIF)

Technical Factor	**Score**	**Explanation**
Loss of Confidentiality	9	All personal data (name, email, address, phone number, transactions) was fully exposed through SQL Injection.
Loss of Integrity	3	There is a potential for data manipulation, but the overall system integrity remains mostly intact.
Loss of Availability	0	No impact on system uptime or service availability was observed.
Loss of Accountability	2	Lack of encrypted logs could hinder user activity tracking and forensic analysis.

The Technical Impact Factors (TIF) were utilized to evaluate the severity of the technical consequences resulting from the identified SQL Injection vulnerability. The loss of confidentiality received a very high rating (9), as the attack led to the complete exposure of sensitive personal data, including names, email addresses, physical addresses, phone numbers, and transaction records, indicating a total breakdown in data protection mechanisms. The loss of integrity was rated as moderate (3), reflecting the potential for unauthorized data manipulation, although no such activity was observed during the testing phase. Loss of availability and accountability were rated low (0 and 2, respectively), given that the system remained fully operational and logging mechanisms were inadequate due to unencrypted or poorly monitored activity. Collectively, these factors result in a medium-level technical risk, with a calculated TIF score of 4.

Table 3. OWASP Risk Rating Assessment Business Impact Factors (BIF)

Business Factor	Score	Explanation
Financial Damage	9	The data breach may result in regulatory fines, loss of customers, and significant recovery costs.
Reputation Damage	5	Public disclosure of the breach could damage customer trust and brand credibility

Non-compliance	9	The incident violates critical provisions of Japan's APPI, especially Articles 15, 16, 20, and 23.
Privacy Violation	9	Personal data was accessed without consent, constituting a serious violation of user privacy.

The Business Impact Factors (BIF) evaluate the organizational consequences of the SQL Injection vulnerability, resulting in a high-risk classification due to its significant implications across financial, legal, and reputational dimensions. The breach introduces substantial financial risk (score: 9), including potential regulatory fines under Japan's Act on the Protection of Personal Information (APPI), legal liabilities, and costs associated with incident response and recovery. It also indicates a high risk of regulatory non-compliance (score: 9), particularly due to violations of APPI Articles 15, 16, 20, and 23. Furthermore, the unauthorized disclosure of personal data constitutes a serious privacy breach (score: 9), while moderate reputational damage (score: 5) may undermine customer trust and damage the organization's credibility. Collectively, these factors highlight the urgent need for mitigation strategies, strengthened compliance measures, and enhanced user data protection. The high-risk rating underscores that this vulnerability is not solely a technical flaw, but a critical threat to business continuity, corporate reputation, and stakeholder trust.

3.3 Implications for APPI Regulation

The data breach was examined within the framework of Japan's Act on the Protection of Personal Information (APPI), with Table 4 providing a detailed mapping of the exposed data types to their corresponding classifications under the APPI**.**

Table 4. Mapping of Data Exposed to APPI Regulations

Data Type	APPI Classification	Implications of Violation
Name, Email, Address, Phone Number	Personal Information	Direct violation of data protection obligations.
Debit Card Information	Personal Information	Exposes customers to the risk of financial fraud.
Book Purchase History	Personal Information Requiring Special Attention	May indicate a person's beliefs, ideology, or personal preferences, thus requiring the highest level of protection.

The leakage of "Special Care-Required Personal Information" (such as purchase history) constitutes a highly serious violation under Japan's Act on the Protection of Personal Information (APPI). In accordance with legal obligations, such incidents require organizations to:

1) **Report the breach to the Personal Information Protection Commission (PPC) of Japan within 72 hours** of becoming aware of the incident.
2) **Promptly notify affected individuals** without undue delay, providing clear information about the nature of the breach and recommended protective actions.

Failure to comply with these legal obligations regarding the leakage of "Special Care-Required Personal Information" may lead to serious consequences under Japan's Act on the Protection of Personal Information (APPI). These consequences include substantial financial penalties for corporations and potential criminal liability for responsible individuals. This analysis therefore demonstrates that the significance of data lies not only in its economic value but also in the legal responsibilities it carries. Technical vulnerabilities, as assessed through the Common Vulnerability Scoring System (CVSS), directly result in elevated business and legal risks when evaluated using the OWASP Risk Rating Methodology and the APPI compliance framework.

4. CONCLUSION

As outlined in the introduction, this research successfully demonstrated the integration of the CVSS, OWASP, and APPI frameworks to conduct a comprehensive risk assessment of SQL injection vulnerabilities. The findings confirm that a technical vulnerability classified as "Critical" with a CVSS score of 9.1 constitutes a significant breach of Japan's APPI regulations and corresponds to a "High" level of business risk under the OWASP methodology. This outcome fulfills the primary objective of the study by establishing a clear and quantifiable link between technical security flaws and their associated legal and business consequences.

This integrated assessment model presents opportunities for future research by extending its application beyond SQL injection to other types of vulnerabilities, such as ransomware, which have been widely discussed

.

in existing literature. To enable comparative legal analysis, the methodology could be adapted to align with other data protection regulations, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). The proposed mitigation strategies offer a practical roadmap for developers and e-commerce stakeholders, encompassing measures such as the implementation of Web Application Firewalls (WAF), the use of parameterized queries, and rigorous input validation. Applying this framework to operational e-commerce platforms may also yield valuable insights into real-world scenarios.

CREDIT AUTHORSHIP CONTRIBUTION STATEMENT

Muahmmad Kholilul Adrian: Conceptualization, Methodology, Writting – original draft. **Prajna Deshanta Ibnugraha**: Validation. **Hilal Hudan Nuha**: Supervision.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

Data will be made available on request.

REFERENCES

[1] G. ANDREIANU, "Protecting Your E-Commerce Business. Analysis on Cyber Security Threats," *Proc. Int. Conf. Cybersecurity Cybercrime-2023*, vol. X, pp. 127–134, 2023.

[2] S. Vinoth, H. L. Vemula, B. Haralayya, P. Mamgain, M. F. Hasan, and M. Naved, "Application of cloud computing in banking and e-commerce and related security threats," *Mater. Today Proc.*, vol. 51, no. December, pp. 2172–2175, 2022, doi: 10.1016/j.matpr.2021.11.121.

[3] F. Q. Kareem *et al.*, "SQL Injection Attacks Prevention System Technology: Review," *Asian J. Res. Comput. Sci.*, no. July, pp. 13–32, 2021, doi: 10.9734/ajrcos/2021/v10i330242.

[4] F. Bolek, V., Romanová, A., & Korček, "The information security management systems in E-business," *J. Glob. Inf. Manag.*, pp. 1–29, 2023.

[5] L. Sumaryanti, D. H. Kusuma, R. Widijastuti, and M. N. Muzaki, "Improvement security in e-business systems using hybrid algorithm," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 5, pp. 1535–1543, 2021, doi: 10.12928/TELKOMNIKA.v19i5.20403.

[6] J. C. Costa, T. Roxo, J. B. F. Sequeiros, H. Proenca, and P. R. M. Inacio, "Predicting CVSS Metric via Description Interpretation," *IEEE Access*, vol. 10, pp. 59125–59134, 2022, doi: 10.1109/ACCESS.2022.3179692.

[7] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of E-Business Information System in Indonesia : Prospects and Challenges," *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 2, pp. 180–188, 2021, doi: 10.34306/ijcitsm.v1i2.49.

[8] S. El-Ebiary, Y. A. B., Almandeel, S., Ghanem, W. A. H., Abu-Ulbeh, W., Al-Dubai, M. M. M., & Bamansoor, "Security Issues and Threats Facing the Electronic Enterprise Leadership," *2020 Int. Conf. Informatics, Multimedia, Cyber Inf. Syst.*, pp. 24–28, 2020, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9354330

[9] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education-Una revisión sistemática de los riesgos de ciberseguridad en Educación más alta," *Futur. Internet*, vol. 13, no. 2, pp. 1–40, 2021.

[10] P. D. Ibnugraha, L. E. Nugroho, and P. I. Santosa, "Risk model development for information security in organization environment based on business perspectives," *Int. J. Inf. Secur.*, vol. 20, no. 1, pp. 113–126, 2021, doi: 10.1007/s10207-020-00495-7.

[11] S. T. Cruz, "Information security risk assessment," *Inf. Secur. Manag. Handbook, Sixth Ed.*, pp. 243–250, 2007, doi: 10.3390/encyclopedia1030050.

[12] S. Shin, "Survey of the Act on the Protection of Personal Information in Japan and International Standard Framework for De-identification," *IIAI Lett. Bus. Decis. Sci.*, vol. 4, p. 1, 2024, doi: 10.52731/lbds.v004.192.

[13] H. Miyashita, "EU-Japan mutual adequacy decision," no. June, pp. 1–13, 2020.

[14] E. M. KALA, "The impact of cyber security on business: how to protect your business.," *Open J. Saf. Sci. Technol.*, vol. 13(2), pp. 51–65, 2023.

[15] B. Esmaeilpour Ghouchani, S. Jodaki, M. Joudaki, A. Balali, and L. Rajabion, "A model for examining the role of the Internet of Things in the development of e-business," *VINE J. Inf. Knowl. Manag. Syst.*, vol. 50, no. 1, pp. 20–33, 2020, doi: 10.1108/VJIKMS-04-2019-0058.