

## DAFTAR PUSTAKA

- [1] Badan Siber dan Sandi Negara Republik Indonesia, “Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.” 2021.
- [2] Badan Siber dan Sandi Negara Republik Indonesia, “LANSKAP KEAMANAN SIBER INDONESIA 2022,” Badan Siber dan Sandi Negara, 2022.
- [3] A. Kurniati, L. E. Nugroho, and M. N. Rizal, “Manajemen Risiko Teknologi Informasi pada e-Government: Ulasan Literatur Sistematis,” vol. 22, no. 2.
- [4] M. Brunner, C. Sauerwein, M. Felderer, and R. Breu, “Risk management practices in information security: Exploring the status quo in the DACH region,” *Comput. Secur.*, vol. 92, 2020, doi: 10.1016/j.cose.2020.101776.
- [5] A. Shamel-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, “Taxonomy of information security risk assessment (ISRA),” *Comput. Secur.*, vol. 57, pp. 14–30, Mar. 2016, doi: 10.1016/j.cose.2015.11.001.
- [6] D. Ionita, P. Hartel, W. Pieters, and R. J. Wieringa, “Current Established Risk Assessment Methodologies and Tools,” 2014, doi: 10.13140/RG.2.2.22914.68806.
- [7] D. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 3rd ed. Boca Raton: CRC Press, 2021. doi: 10.1201/9781003090441.
- [8] E. Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*, 1st ed. Syngress, 2011.
- [9] Kementerian Sekretariat Negara Republik Indonesia, “Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.” 2019.
- [10] Pemerintah Kabupaten Blitar, “Peraturan Bupati Blitar Nomor 64 Tahun 2022 Tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah.” 2022.
- [11] D. Gibson, *Managing risk in information systems*. in Jones & Bartlett learning information systems security & assurance series. Sudbury, MA: Jones & Bartlett Learning, 2011.
- [12] “OWASP Top Ten 2017 | Application Security Risks | OWASP Foundation.” Accessed: Oct. 30, 2023. [Online]. Available: [https://owasp.org/www-project-top-ten/2017/Application\\_Security\\_Risks.html](https://owasp.org/www-project-top-ten/2017/Application_Security_Risks.html)
- [13] Joint Task Force Transformation Initiative, “Guide for conducting risk assessments,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.
- [14] Badan Standarisasi Nasional, “SNI ISO/IEC 27032:2014 Teknologi Informasi-Teknik keamanan-Pedoman keamanan siber.” 2014.
- [15] Pemerintah Kabupaten Blitar, “Peraturan Bupati Blitar Nomor 15 Tahun 2020 Tentang Pedoman Pengelolaan Risiko di Lingkungan Pemerintah Kabupaten Blitar.” 2020.
- [16] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, “Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi

- Birokrasi Republik Indonesia Nomor 5 Tahun 2020 Tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.” 2020.
- [17] O. D. Niverta, F. Setiadi, and K. A. Achmad, “E-GOVERNMENT RISK MANAGEMENT ANALYSIS USING PERMENPAN RB NUMBER 5 OF 2020 AT COMMUNICATION AND INFORMATION OFFICE OF XYZ REGENCY,” *JIPJ J. Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 8, no. 2, pp. 407–418, May 2023, doi: 10.29100/jipi.v8i2.3475.
  - [18] B. H. Al-fajri, R. Fauzi, and R. Mulyana, “PERANCANGAN MANAJEMEN RISIKO OPERASIONAL SPBE/E-GOV PADA KATEGORI RISIKO INFRASTRUKTUR, APLIKASI, LAYANAN, DATA DAN INFORMASI BERDASARKAN PERMEN PANRB NOMOR 5 TAHUN 2020 (STUDI KASUS: PEMERINTAH KOTA BANDUNG),” p. 9.
  - [19] R. Bisma, “Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan,” vol. 06, 2022.
  - [20] F. D. Suryoputro, L. Abdurrahman, and R. Mulyana, “PERANCANGAN MANAJEMEN RISIKO OPERASIONAL SPBE/E-GOVERNMENT ELEKTRONIK PADA KATEGORI SUMBER DAYA MANUSIA, DATA DAN INFORMASI, APLIKASI, DAN KEAMANAN BERDASARKAN PERMEN PANRB NOMOR 5 TAHUN 2020 STUDI KASUS PEMERINTAH DAERAH KABUPATEN BANDUNG BARAT”.
  - [21] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, “Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency,” *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.
  - [22] H. Setiawan, F. A. Putra, and A. R. Pradana, “Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute,” presented at the 2017 International Conference on Information Technology Systems and Innovation, ICITSI 2017 - Proceedings, 2017, pp. 251–256. doi: 10.1109/ICITSI.2017.8267952.
  - [23] D. I. Sensuse, A. Syahrizal, F. Aditya, and M. Nazri, “Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik,” in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, Nov. 2020, pp. 1–7. doi: 10.1109/ICIC50835.2020.9288593.
  - [24] A. Anang, A. Gandhi, and Y. G. Sucahyo, “The Design of Information Security Risk Management: A Case Study Human Resources Information System at XYZ University,” in *2021 4th International Conference of Computer and Informatics Engineering (IC2IE)*, Sep. 2021, pp. 198–203. doi: 10.1109/IC2IE53219.2021.9649035.
  - [25] B. Ghazali, K. Kusrini, and S. Sudarmawan, “Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating,” *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, Jan. 2019, doi: 10.24076/citec.2017v4i4.119.
  - [26] V. Gerardo and A. N. Fajar, “Academic IS Risk Management using OCTAVE Allegro in Educational Institution,” *J. Inf. Syst. Inform.*, vol. 4, no. 3, pp. 687–708, Sep. 2022, doi: 10.51519/journalisi.v4i3.319.
  - [27] Ricko Dwi Pambudi and K. Ramli, “INFORMATION SECURITY RISK MANAGEMENT DESIGN OF SUPERVISION MANAGEMENT

- INFORMATION SYSTEM AT XYZ MINISTRY USING NIST SP 800-30,” *J. Tek. Inform. Jutif*, vol. 4, no. 3, pp. 591–599, Jun. 2023, doi: 10.52436/1.jutif.2023.4.3.978.
- [28] Joint Task Force Transformation Initiative, “Managing information security risk :: organization, mission, and information system view,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-39, 2011. doi: 10.6028/NIST.SP.800-39.
  - [29] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), “International Standard ISO/IEC 27005 Information technology — Security techniques — Information security risk management.” 2018.
  - [30] A. Alwi and K. A. Zainol Ariffin, “Information Security Risk Assessment for the Malaysian Aeronautical Information Management System,” presented at the Proceedings of the 2018 Cyber Resilience Conference, CRC 2018, 2019. doi: 10.1109/CR.2018.8626841.
  - [31] A. Shirazi and M. Kazemi, “A New Model for Information Security Risk Management,” presented at the Lecture Notes in Information Systems and Organisation, 2020, pp. 551–566. doi: 10.1007/978-3-030-34269-2\_38.
  - [32] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. Sri Arsa, “Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City),” *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 4, pp. 30–40, Aug. 2020, doi: 10.5815/ijcnis.2020.04.03.
  - [33] Badan Standarisasi Nasional, “SNI ISO Guide 73:2016 Manajemen Risiko-Kosakata.” 2016.
  - [34] M. E. Whitman and H. J. Mattord, *Principles of information security*, Sixth Edition. Australia: Cengage Learning, 2018.
  - [35] B. Von Solms and R. Von Solms, “Cybersecurity and information security – what goes where?,” *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, Mar. 2018, doi: 10.1108/ICS-04-2017-0025.
  - [36] H. Taherdoost, “Cybersecurity vs. Information Security,” *Procedia Comput. Sci.*, vol. 215, pp. 483–487, 2022, doi: 10.1016/j.procs.2022.12.050.
  - [37] A. Althonayan and A. Andronache, “Shifting from Information Security towards a Cybersecurity Paradigm,” in *Proceedings of the 2018 10th International Conference on Information Management and Engineering - ICIME 2018*, Salford, United Kingdom: ACM Press, 2018, pp. 68–79. doi: 10.1145/3285957.3285971.
  - [38] R. De Bruin and S. H. von Solms, “Cybersecurity Governance: How can we measure it?,” in *2016 IST-Africa Week Conference*, Durban, South Africa: IEEE, May 2016, pp. 1–9. doi: 10.1109/ISTAFRICA.2016.7530578.
  - [39] Kementerian Sekretariat Negara Republik Indonesia, “Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik.” 2018.
  - [40] A. Alzahrani, A. Alqazzaz, Y. Zhu, H. Fu, and N. Almashfi, “Web Application Security Tools Analysis,” in *2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, Beijing, China: IEEE, May 2017, pp. 237–242. doi: 10.1109/BigDataSecurity.2017.47.
  - [41] Badan Siber dan Sandi Negara, “Laporan Tahunan Monitoring Keamanan Siber 2021,” Badan Siber dan Sandi Negara, 2021.

- [42] “OWASP Top 10:2021.” Accessed: Nov. 16, 2022. [Online]. Available: <https://owasp.org/Top10/>
- [43] C. Schou and S. Hernandez, *Information assurance handbook: effective computer security and risk management strategies*. New York: McGraw-Hill Education, 2015.
- [44] “OWASP Risk Rating Methodology | OWASP Foundation.” Accessed: Jan. 24, 2022. [Online]. Available: [https://owasp.org/www-community/OWASP\\_Risk\\_Rating\\_Methodology](https://owasp.org/www-community/OWASP_Risk_Rating_Methodology)
- [45] T. Mahler, Y. Elovici, and Y. Shahr, “A New Methodology for Information Security Risk Assessment for Medical Devices and Its Evaluation.” arXiv, Feb. 17, 2020. Accessed: Apr. 25, 2023. [Online]. Available: <http://arxiv.org/abs/2002.06938>
- [46] U. Mcube, M. Gerber, and R. Von Solms, “Scenario-based IT risk assessment in local government,” in *2016 IST-Africa Week Conference*, May 2016, pp. 1–9. doi: 10.1109/ISTAFRICA.2016.7530587.
- [47] “Getting Started,” NIST, Feb. 2018, Accessed: Oct. 18, 2023. [Online]. Available: <https://www.nist.gov/cyberframework/getting-started>
- [48] “CWE - New to CWE.” Accessed: Jun. 21, 2023. [Online]. Available: [https://cwe.mitre.org/about/new\\_to\\_cwe.html](https://cwe.mitre.org/about/new_to_cwe.html)
- [49] “CWE - CWE-798: Use of Hard-coded Credentials (4.11).” Accessed: Jun. 23, 2023. [Online]. Available: <https://cwe.mitre.org/data/definitions/798.html>
- [50] X. Yuan, E. B. Nuakoh, J. S. Beal, and H. Yu, “Retrieving relevant CAPEC attack patterns for secure software development,” in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*, Oak Ridge, Tennessee: ACM Press, 2014, pp. 33–36. doi: 10.1145/2602087.2602092.
- [51] “CAPEC - Schema Documentation - Schema Version 3.5.” Accessed: Jun. 23, 2023. [Online]. Available: <https://capec.mitre.org/documents/schema/index.html>
- [52] C. Garcia-Porras, S. Huamani-Pastor, and J. Armas-Aguirre, “Information Security Risk Management Model for Peruvian SMEs,” in *2018 IEEE Sciences and Humanities International Research Conference (SHIRCON)*, Lima: IEEE, Nov. 2018, pp. 1–5. doi: 10.1109/SHIRCON.2018.8592994.
- [53] Badan Siber dan Sandi Negara Republik Indonesia, “Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik.” 2020.
- [54] P. Baybutt, “Guidelines for designing risk matrices,” *Process Saf. Prog.*, vol. 37, no. 1, pp. 49–55, Mar. 2018, doi: 10.1002/prs.11905.
- [55] M. U. Aksu *et al.*, “A quantitative CVSS-based cyber security risk assessment methodology for IT systems,” in *2017 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2017, pp. 1–8. doi: 10.1109/ICCST.2017.8167819.
- [56] J. Li, C. Bao, and D. Wu, “How to Design Rating Schemes of Risk Matrices: A Sequential Updating Approach,” *Risk Anal.*, vol. 38, no. 1, pp. 99–117, Jan. 2018, doi: 10.1111/risa.12810.
- [57] N. J. Duijm, “Recommendations on the use and design of risk matrices,” *Saf. Sci.*, vol. 76, pp. 21–31, Jul. 2015, doi: 10.1016/j.ssci.2015.02.014.
- [58] S. Fenz and A. Ekelhart, “Verification, Validation, and Evaluation in Information Security Risk Management,” *IEEE Secur. Priv. Mag.*, vol. 9, no. 2, pp. 58–65, Mar. 2011, doi: 10.1109/MSP.2010.117.
- [59] Sugiyono, *METODE PENELITIAN KUANTITATIF, KUALITATIF, DAN R&D*, vol. 19. 2013.
- [60] S. D. Gantz, *The basics of IT audit: purposes, processes, and practical information*.

Amsterdam: Syngress, an imprint of Elsevier, 2014.

- [61] A. R. Otero, "Information Technology Control and Audit, Fifth Edition," *Inf. Technol.*
- [62] Kementerian Komunikasi dan Informatika Republik Indonesia, "Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 16 Tahun 2022 Tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi." 2022.
- [63] P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," in *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, Coimbatore, India: IEEE, Feb. 2016, pp. 1–5. doi: 10.1109/STARTUP.2016.7583912.
- [64] A. Doupé, M. Cova, and G. Vigna, "Why Johnny Can't Pentest: An Analysis of Black-Box Web Vulnerability Scanners," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 6201, C. Kreibich and M. Jahnke, Eds., in *Lecture Notes in Computer Science*, vol. 6201., Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 111–131. doi: 10.1007/978-3-642-14215-4\_7.
- [65] L. Dencheva, "Comparative analysis of Static application security testing (SAST) and Dynamic application security testing (DAST) by using open-source web application penetration testing tools".
- [66] DOMARS, "Threat modeling for drivers - Windows drivers." Accessed: Jan. 20, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers>
- [67] S. Barnum, "Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description." Cigital, Inc., 2008.
- [68] P. R. Garvey, *Analytical methods for risk management: a systems engineering perspective*. in *Statistics, textbooks and monographs*. Boca Raton: CRC Press, 2009.
- [69] E. Lavens, P. Philippaerts, and W. Joosen, "A Quantitative Assessment of the Detection Performance of Web Vulnerability Scanners," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna Austria: ACM, Aug. 2022, pp. 1–10. doi: 10.1145/3538969.3544416.