

DAFTAR PUSTAKA

- Abdel Hakeem, S. A., & Kim, H. (2023). Authentication and encryption protocol with revocation and reputation management for enhancing 5G-V2X security. *Journal of King Saud University - Computer and Information Sciences*, 35(7), 101638. <https://doi.org/10.1016/J.JKSUCI.2023.101638>
- Achmadi, D. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *2018 International Workshop on Big Data and Information Security (IW BIS)*, 149–157. <https://doi.org/10.1109/IWBIS.2018.8471700>
- Aghili, S. F., Sedaghat, M., Singelée, D., & Gupta, M. (2022). MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. *Future Generation Computer Systems*, 131, 75–90. <https://doi.org/10.1016/J.FUTURE.2022.01.003>
- Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939–953. <https://doi.org/10.1002/asi.24311>
- Ajupov, A., Sherstobitova, A., Syrotiuk, S., & Karataev, A. (2019). The risk-management theory in modern economic conditions. *E3S Web of Conferences*, 110. <https://doi.org/10.1051/e3sconf/201911002040>
- Al Faruq, B. (2020). Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(3), 3514–3531. <https://doi.org/10.30534/ijatcse/2020/157932020>
- Alabbad, M., Mhaskar, N., & Khedri, R. (2024). Two formal design solutions for the generalization of network segmentation. *Journal of Network and Computer Applications*, 222, 103763. <https://doi.org/10.1016/J.JNCA.2023.103763>
- Alameka, D. (2023). SYSTEMATIC LITERATURE REVIEW: SEKTOR SERANGAN SIBER DAN METODE PENDETEKSI SERANGAN SIBER PADA WEBSITE PELAYANAN PUBLIK DI KALIMANTAN TIMUR. *IPDN repository*.
- Alexander, G. J. (2009). From Markowitz to modern risk management. *European Journal of Finance*, 15(5–6), 451–461. <https://doi.org/10.1080/13518470902853566>
- Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences (Switzerland)*, 10(10). <https://doi.org/10.3390/app10103660>

- Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information Security:A Review of Information Security Issues and Techniques. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, 1–6. <https://doi.org/10.1109/CAIS.2019.8769504>
- Almarhabi, K., Bahaddad, A., & Mohammed Alghamdi, A. (2023). Security management of BYOD and cloud environment in Saudi Arabia. *Alexandria Engineering Journal*, *63*, 103–114. <https://doi.org/10.1016/J.AEJ.2022.07.031>
- Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science*, *7*, e703. <https://doi.org/10.7717/peerj-cs.703>
- Almuhammadi, S., & Alsaleh, M. (2017). INFORMATION SECURITY MATURITY MODEL FOR NIST CYBER SECURITY FRAMEWORK. *Computer Science & Information Technology*, 51–62. <https://doi.org/10.5121/csit.2017.70305>
- Alotaibi, F., & Alshehri, A. (2020). Gender Differences in Information Security Management. *Journal of Computer and Communications*, *08*(03), 53–60. <https://doi.org/10.4236/jcc.2020.83006>
- Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee’s perspective. *Computers & Security*, *129*, 103208. <https://doi.org/10.1016/J.COSE.2023.103208>
- Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting and Social Change*, *198*, 123028. <https://doi.org/10.1016/J.TECHFORE.2023.123028>
- Argyridou, E., Nifakos, S., Laoudias, C., Panta, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Zamorano, J. M., Papachristou, P., & Bonacina, S. (2022). Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Healthcare Organisations (Preprint). *Journal of Medical Internet Research*. <https://doi.org/10.2196/41294>
- Awaliah, R. (2021). Studi Komparasi. *Universitas Islam Negri Alauddin*, *6*(2), 1–178. <http://www.ufrgs.br/actavet/31-1/artigo552.pdf>
- Azbeq, K., Ouchetto, O., & Jai Andaloussi, S. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian Informatics Journal*, *23*(2), 329–343. <https://doi.org/10.1016/J.EIJ.2022.02.004>
- Bashofi, I., & Salman, M. (2022). Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. *Proceedings - 2022 IEEE International*

- Conference on Cybernetics and Computational Intelligence, CyberneticsCom 2022*, 58–62.
<https://doi.org/10.1109/CyberneticsCom55287.2022.9865640>
- Bavaresco, M. V., D'Oca, S., Ghisi, E., & Lamberts, R. (2020). Methods used in social sciences that suit energy research: A literature review on qualitative methods to assess the human dimension of energy use in buildings. *Energy and Buildings*, 209, 109702.
<https://doi.org/10.1016/j.enbuild.2019.109702>
- Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 63(4), 531–540. <https://doi.org/10.1016/j.bushor.2020.03.010>
- Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management*. 97–104. <https://doi.org/10.1145/508171.508187>
- Bouziani, M., Merbah, M., Tiskar, M., Et-tahir, A., & Chaouch, A. (2022). When can we talk about implementing an Information Security Management System, according to ISO 27001? *Turkish Journal of Computer and Mathematics Education*, 13(02), 394–401.
- Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *Iberian Conference on Information Systems and Technologies, CISTI, 2019-June(June)*, 19–22.
<https://doi.org/10.23919/CISTI.2019.8760870>
- Carvalho, C. A. B. de, Andrade, R. M. de C., Castro, M. F. de, Coutinho, E. F., & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. *Computers and Electrical Engineering*, 59, 141–152. <https://doi.org/10.1016/j.compeleceng.2016.12.030>
- Chaeikar, S. S., Jafari, M., & Taherdoost, H. (2012). Definitions and Criteria of CIA Security. *International Journal of Advanced Computer Science and Information Technology*, 1(1), 14–23.
- Chaganti, R., Varadarajan, V., Gorantla, V. S., Gadekallu, T. R., & Ravi, V. (2022). Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet*, 14(9), 1–20. <https://doi.org/10.3390/fi14090250>
- Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT In Education*, 8(2), 34–42.
<https://doi.org/10.37134/jictie.vol8.2.4.2021>
- Coss, D., & Samonas, S. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, 10(3), 21–45.
www.jissec.org
- Deng, S., Hu, Q., Wu, D., & He, Y. (2023). BCTC-KSM: A blockchain-assisted threshold cryptography for key security management in power IoT data sharing. *Computers and Electrical Engineering*, 108, 108666.

<https://doi.org/10.1016/J.COMPELECENG.2023.108666>

- Denzin, N. K., & Lincoln, Y. S. (2018). The SAGE Handbook of Qualitative Research. In *Synthese* (Vol. 195, Nomor 5). <https://doi.org/10.1007/s11229-017-1319-x>
- Doni. (2021). *10 Sektor Prioritas untuk Memacu Transformasi Digital*. Kementerian Komunikasi dan Informatika. <https://www.kominfo.go.id/content/detail/36895/10-sektor-prioritas-untuk-memacu-transformasi-digital/0/artikel>
- Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinouidakis, C., Cook, A., & Janicke, H. (2020). A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, 1641–1646. <https://doi.org/10.1109/COMPSAC48688.2020.00-20>
- Dronov, V. Y., & Dronova, G. A. (2022). Principles of information security management system. *Journal of Physics: Conference Series*, 2182(1). <https://doi.org/10.1088/1742-6596/2182/1/012092>
- Echeverría, A., Cevallos, C., Ortiz-Garces, I., & Andrade, R. O. (2021). Cybersecurity model based on hardening for secure internet of things implementation. *Applied Sciences (Switzerland)*, 11(7). <https://doi.org/10.3390/app11073260>
- Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, 1(1), 1–11. <https://doi.org/10.25008/bcsee.v1i1.2>
- Gadelha, A. L. L., Gouveia, L. B., & Sarmiento, A. M. (2023). Essential internal control: evidence from the executive branch of the State of Ceará. *Revista de Gestao*, 30(1), 32–46. <https://doi.org/10.1108/REGE-08-2020-0073>
- Gao, H. (2023). Design of Network Data Information Security Monitoring System Based on Big Data Technology. *Procedia Computer Science*, 228, 348–355. <https://doi.org/10.1016/J.PROCS.2023.11.040>
- Godejord, P., & Godejord, B. (2023). Computer Games as a Pedagogical Tool for Creating Cyber Security Awareness. *Proceedings of the European Conference on Games-based Learning, 2023-October*, 220–224. <https://doi.org/10.34190/ecgbl.17.1.1407>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST cybersecurity framework via the gordon-loeb model. *Journal of Cybersecurity*, 6(1), 1–8.

<https://doi.org/10.1093/CYBSEC/TYAA005>

- Gourisetti, S. N. G., Mylrea, M., Ashley, T., Kwon, R., Castleberry, J., Wright-Mockler, Q., McKenzie, P., & Brege, G. (2019). Demonstration of the Cybersecurity Framework through Real-World Cyber Attack. *Proceedings - 2019 Resilience Week, RWS 2019*, 19–25. <https://doi.org/10.1109/RWS47064.2019.8971822>
- Guccio, C., Lisi, D., Martorana, M., & Mignosa, A. (2017). On the role of cultural participation in tourism destination performance: an assessment using robust conditional efficiency approach. *Journal of Cultural Economics*, 41(2), 129–154. <https://doi.org/10.1007/s10824-017-9295-z>
- Gupta, B. B., Gaurav, A., & Kumar Panigrahi, P. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, 162, 113859. <https://doi.org/10.1016/J.JBUSRES.2023.113859>
- Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access*, 9, 94723–94747. <https://doi.org/10.1109/ACCESS.2021.3093952>
- Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: An introduction. *Psychiatry Research*, 280(April). <https://doi.org/10.1016/j.psychres.2019.112516>
- Hanifah, F., Budiyo, A., & Widjajarto, A. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault Dan Docker Bench For Security Dengan Acuan Framework CIS Control. *e-Proceeding of Engineering*, 8(5), 8879–8885. <https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15914>
- Huang, Y., Debnath, J., Iorga, M., Kumar, A., & Xie, B. (2019). CSAT: A User-interactive Cyber Security Architecture Tool based on NIST-compliance Security Controls for Risk Management. *2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2019*, 0697–0707. <https://doi.org/10.1109/UEMCON47517.2019.8993090>
- Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *Journal of Supercomputing*, 74(10), 5171–5186. <https://doi.org/10.1007/s11227-018-2479-2>
- Ivanov, D., Kalinin, M., Krundyshev, V., & Orel, E. (2020). Automatic security management of smart infrastructures using attack graph and risk analysis. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 295–300. <https://doi.org/10.1109/WorldS450073.2020.9210410>

- Kamel, S. O. M., & Hegazi, N. H. (2018). A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security. *International Journal of Scientific and Engineering Research*, 9(9), 1227–1244. https://www.researchgate.net/profile/Samah_Kamel3/publication/328163339_A_Proposed_Model_of_IoT_Security_Management_System_Based_on_A_study_of_Internet_of_Things_IoT_Security/links/5bbc74254585159e8d8f245a/A-Proposed-Model-of-IoT-Security-Management-System
- Kavak, A., & Odabaş, H. (2023). The impact of information security management guide utilization on technological and institutional information security measures in university libraries in Türkiye. *The Journal of Academic Librarianship*, 49(6), 102800. <https://doi.org/10.1016/J.ACALIB.2023.102800>
- Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian Decision Network-Based Security Risk Management Framework. *Journal of Network and Systems Management*, 28(4), 1794–1819. <https://doi.org/10.1007/s10922-020-09558-5>
- Ključnikov, A., Mura, L., & Sklenár, D. (2019). INFORMATION SECURITY MANAGEMENT IN SMES: FACTORS OF SUCCESS Aleksandr Ključnikov¹, Ladislav Mura², David Sklenár^{2,3}. *Entrepreneurship and Sustainability Issues*, 6(4), 2081–2094.
- Kobezak, P., Marchany, R., Raymond, D., & Tront, J. (2018). Host inventory controls and systems survey: Evaluating the CIS critical security control one in higher education networks. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2018-Janua*, 4742–4751. <https://doi.org/10.24251/hicss.2018.597>
- Kwon, R., Ashley, T., Castleberry, J., McKenzie, P., & Gourisetti, S. N. G. (2020). Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. *IEEE Xplore*, 75, 106–112.
- Lartey, P. Y., Kong, Y., Bah, F. B. M., Santosh, R. J., & Gumah, I. A. (2020). Determinants of Internal Control Compliance in Public Organizations; Using Preventive, Detective, Corrective and Directive Controls. *International Journal of Public Administration*, 43(8), 711–723. <https://doi.org/10.1080/01900692.2019.1645689>
- Li, W., Stidsen, C., & Adam, T. (2023). A blockchain-assisted security management framework for collaborative intrusion detection in smart cities. *Computers and Electrical Engineering*, 111, 108884. <https://doi.org/10.1016/J.COMPELECENG.2023.108884>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egy.2021.08.126>
- Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR

- Compliance. *Iberian Conference on Information Systems and Technologies, CISTI, 2019-June*(June), 1–6. <https://doi.org/10.23919/CISTI.2019.8760937>
- Lubis, M., & Safitra, M. F. (2023). Conceptual Model Tree Of Research. In *Repository.Uin-Suska.Ac.Id*. [http://repository.uin-suska.ac.id/26740/1/Haki Buku Genealogi Intelektual Melayu Tradisi Pemikiran Islam Abad ke 19 di Kerajaan Riau Lingga.pdf](http://repository.uin-suska.ac.id/26740/1/Haki%20Buku%20Genealogi%20Intelektual%20Melayu%20Tradisi%20Pemikiran%20Islam%20Abad%20ke%2019%20di%20Kerajaan%20Riau%20Lingga.pdf)
- Mekarisce, A. A. (2020). Teknik Pemeriksaan Keabsahan Data pada Penelitian Kualitatif di Bidang Kesehatan Masyarakat. *JURNAL ILMIAH KESEHATAN MASYARAKAT: Media Komunikasi Komunitas Kesehatan Masyarakat*, 12(3), 145–151. <https://doi.org/10.52022/jikm.v12i3.102>
- Menezes, B. C., Kelly, J. D., Leal, A. G., & Le Roux, G. C. (2019). Predictive, Prescriptive and Detective Analytics for Smart Manufacturing in the Information Age. *IFAC-PapersOnLine*, 52(1), 568–573. <https://doi.org/10.1016/J.IFACOL.2019.06.123>
- Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez, G., & Quiroz, D. (2019). Information Security Management Frameworks in Higher Education Institutions: An Overview. *2019 3rd Cyber Security in Networking Conference, CSNet 2019*, 63–65. <https://doi.org/10.1109/CSNet47905.2019.9108845>
- Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). Efficient estimation of word representations in vector space. *1st International Conference on Learning Representations, ICLR 2013 - Workshop Track Proceedings*, 6–7.
- Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, 68(1), 87–100. <https://doi.org/10.1109/TEM.2020.2977815>
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., Altman, D., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J. A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J. J., Devreux, P. J., Dickersin, K., Egger, M., Ernst, E., ... Tugwell, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, 6(7). <https://doi.org/10.1371/journal.pmed.1000097>
- Mortazavi, S. A. R., & Safi-Esfahani, F. (2019). A checklist based evaluation framework to measure risk of information security management systems. *International Journal of Information Technology (Singapore)*, 11(3), 517–534. <https://doi.org/10.1007/s41870-019-00302-0>
- Moshinsky, M. (2021). ISO 27001 Standardization of the existing ISMS in a Software Industry SME. *Nucl. Phys.*, 13(1), 104–116.

- Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science*, 217, 1406–1415. <https://doi.org/10.1016/J.PROCS.2022.12.339>
- Mylrea, M., Gourisetti, S. N. G., Larimer, C., & Noonan, C. (2018). Insider threat cybersecurity framework webtool & methodology: Defending against complex cyber-physical threats. *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, 207–216. <https://doi.org/10.1109/SPW.2018.00036>
- Najib, M. (2021). *IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS ECAMPUZ MENGGUNAKAN CIS BENCHMARK*. 1–6.
- Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security*, 135, 103525. <https://doi.org/10.1016/J.COSE.2023.103525>
- Nath N, R., & V Nath, H. (2022). Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. *Computers and Electrical Engineering*, 100, 107997. <https://doi.org/10.1016/J.COMPELECENG.2022.107997>
- Nawa, E.-L. T., Chitauro, M., & Bhunu Shava, F. (2023). Developing a Cybersecurity Framework for the Namibian Banking Institutions. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4332733>
- Nugroho, A. S. A., & Winarno, W. W. (2018). “Jurnal TRANSFORMASI (Informasi & Pengembangan Iptek)” (STMIK BINA PATRIA) METODE SILOGISME AND UNTUK VALIDITAS JAWABAN DARI RESPONDEN DALAM ANALISIS MATURITY LEVEL KEAMANAN INFORMASI BERBASIS SNI ISO 27001:2013 PADA DINAS KEPENDUDUKAN DAN PENCATATAN SIPI. *Jurnal TRANSFORMASI*, 14(2), 167–177.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., & Moher, D. (2021). Updating guidance for reporting systematic reviews: development of the PRISMA 2020 statement. *Journal of Clinical Epidemiology*, 134, 103–112. <https://doi.org/10.1016/j.jclinepi.2021.02.003>
- Parihar, A., Prajapati, J. B., Prajapati, B. G., Trambadiya, B., Thakkar, A., & Engineer, P. (2024). Role of IOT in healthcare: Applications, security & privacy concerns. *Intelligent Pharmacy*. <https://doi.org/10.1016/J.IPHA.2024.01.003>
- Paul, P. C., Loane, J., McCaffery, F., & Regan, G. (2021). Towards design and development of a

- data security and privacy risk management framework for wban based healthcare applications. *Applied System Innovation*, 4(4), 704–710. <https://doi.org/10.3390/asi4040076>
- Paya, A., Cotarelo, A., & Redondo, J. M. (2022). Egida: Automated security configuration deployment systems with early error detection. *Computers and Security*, 116(2022). <https://doi.org/10.1016/j.cose.2022.102638>
- Piech, H., & Grodzki, G. (2017). Audit expert system of communication security assessment. *Procedia Computer Science*, 112, 147–156. <https://doi.org/10.1016/J.PROCS.2017.08.188>
- Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A., & Popoola, J. (2023). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, Challenges and Solutions. *Blockchain: Research and Applications*, 100178. <https://doi.org/10.1016/J.BCRA.2023.100178>
- Rehman, Z., Gondal, I., Ge, M., Dong, H., Gregory, M., & Tari, Z. (2024). Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. *Computers & Security*, 139, 103685. <https://doi.org/10.1016/J.COSE.2023.103685>
- Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*, 53, 27001–27003. <https://doi.org/10.1109/NCETSTEA48365.2020.9119914>
- Saputra, B. B. B., & Krisnadi, I. (n.d.). *No Title*. 0(5), 5–9.
- Sas, M., Reniers, G., Ponnet, K., & Hardyns, W. (2021). The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. *Safety Science*, 144, 105447. <https://doi.org/10.1016/J.SSCI.2021.105447>
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974. <https://doi.org/10.1016/J.COSE.2022.102974>
- Simonova, A. (2020). *an Analysis of Factors Influencing National Institute of Standards and Technology Cybersecurity Framework Adoption in Financial Services: a Correlational Study*. May, 1–56.
- Soegiyono. (2011). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*.
- Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178–188. <https://doi.org/10.1016/j.future.2018.09.063>

- Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of Cybersecurity Standard and Framework Components. *International Journal of Communication Networks and Information Security*, 12(3), 417–432. <https://doi.org/10.17762/ijcnis.v12i3.4817>
- Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*, 11(14). <https://doi.org/10.3390/electronics11142181>
- Tyagi, H., Kumar, R., & Pandey, S. K. (2023). A detailed study on trust management techniques for security and privacy in IoT: challenges, trends, and research directions. *High-Confidence Computing*, 3(2), 100127. <https://doi.org/10.1016/J.HCC.2023.100127>
- Van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE*, 12(7), 1–17. <https://doi.org/10.1371/journal.pone.0181689>
- Viegas, V., & Kuyucu, O. (2022). IT Security Controls. In *IT Security Controls*. <https://doi.org/10.1007/978-1-4842-7799-7>
- Xie, Z., Zhang, D., Han, X., & Hu, W. (2023). Power system transient stability preventive control optimization method driven by Stacking Ensemble Learning. *Energy Reports*, 9, 757–765. <https://doi.org/10.1016/J.EGYR.2023.05.106>
- Yang, J.-M., & Kwak, S. W. (2024). Robust corrective control against fundamental and non-fundamental mode attacks with application to an asynchronous digital system. *Information Sciences*, 120145. <https://doi.org/10.1016/J.INS.2024.120145>
- Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, 8, 131723–131740. <https://doi.org/10.1109/ACCESS.2020.3009876>
- Yasin, M., Akhmad Arman, A., Edward, I. J. M., & Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020*, 2013(95), 3–7. <https://doi.org/10.1109/TSSA51342.2020.9310875>
- Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers and Security*, 104, 102221. <https://doi.org/10.1016/j.cose.2021.102221>
- Zhou, C., & Jiang, Z. (2023). Computer Network Communication Security Encryption System Based on Ant Colony Optimization Algorithm. *Procedia Computer Science*, 228, 38–46. <https://doi.org/10.1016/J.PROCS.2023.11.006>