

DAFTAR PUSTAKA

- [1] A. Kornelia and D. Irawan, “Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1,” 2021.
- [2] R. Sinaga, “Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala.” [Online]. Available: <https://journal.fkom.uniku.ac.id/ilkom>
- [3] PT. Akebono Brake Astra Indonesia, “About PT. Akebono Brake Astra Indonesia,” <https://www.akebono-astra.co.id/>. Accessed: Jul. 15, 2025. [Online]. Available: <https://www.akebono-astra.co.id/>
- [4] Alicia Hope (Staff Correspondent at CPO Magazine), “Toyota’s Supply Chain Cyber Attack Stopped Production, Cutting Down a Third of Its Global Output.” Accessed: Jul. 15, 2025. [Online]. Available: <https://www.cpomagazine.com/cyber-security/toyotas-supply-chain-cyber-attack-stopped-production-cutting-down-a-third-of-its-global-output/#:~:text=Toyota%20Motor%20suspended%20operations%20in%2028%20production%20lines,electronic%20components%20supplier%20Kojima%20Industries%20on%20February%202024.>
- [5] Teju Shyamsundar, “Ransomware supply chain threats: What made a global automotive company shut their plants this past spring?,” <https://veza.com/blog/ransomware-supply-chain-threats-what-made-a-global-automotive-company-shut-their-plants-this-past-spring/>. Accessed: Jul. 15, 2025. [Online]. Available: <https://veza.com/blog/ransomware-supply-chain-threats-what-made-a-global-automotive-company-shut-their-plants-this-past-spring/>
- [6] Keagan Gay, “Throwback Attack: WannaCry ransomware takes Renault-Nissan plants offline,” <https://www.controleng.com/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline/>. Accessed: Jul. 15, 2025. [Online]. Available: <https://www.controleng.com/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline/>
- [7] CISA, “Black Basta ransomware affiliates have breached over 500 organizations between April 2022 and May 2024, FBI and CISA reported.,” <https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware>. Accessed: Jul. 15, 2025. [Online]. Available: <https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware>
- [8] Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), Federal Bureau of Investigation (FBI),

- and Multi-State Information Sharing and Analysis Center (MS-ISAC), “#StopRansomware: Black Basta,” <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a>. Accessed: Jul. 15, 2025. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a>
- [9] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, “The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector,” *Sustainability (Switzerland)*, vol. 15, no. 7, Apr. 2023, doi: 10.3390/su15075828.
- [10] SOCRadar® Cyber Intelligence Inc., “Ransomware Attacks - Distribution by Industries,” <https://socradar.io/biggest-manufacturing-industry-attacks-2024/##post-gallery-6>. Accessed: Jul. 15, 2025. [Online]. Available: <https://socradar.io/biggest-manufacturing-industry-attacks-2024/##post-gallery-6>
- [11] Badan Siber dan Sandi Negara (BSSN), “Indeks Keamanan Informasi (INDEX KAMI),” <https://www.bssn.go.id/indeks-kami/>. Accessed: Jul. 15, 2025. [Online]. Available: <https://www.bssn.go.id/indeks-kami/>
- [12] D. E. R. Hidayatullah, R. Kunthi, and R. Harwahu, “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.
- [13] S. Rif'atul Musyarofah¹ and R. Bisma², “Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun.”
- [14] Kristofel Santa, Enjelita Radjakore, Rikna Aresta Lahutung, Ravila Putri Pangalila, and Tresya Veronika Deil, “Ethical Hacking Sebagai Strategi Keamanan Cyber di Era Digital: Studi Pustaka dan Implementasi Dasar,” *Jurnal Ilmiah Teknik Informatika dan Komunikasi*, vol. 5, no. 2, pp. 548–553, Jun. 2025, doi: 10.55606/juitik.v5i2.1183.
- [15] J. Manajemen Pendidikan Islam, T. Digital Dalam Pengembangan Diklat Untuk Peningkatan Kualitas Sumber Daya Manusia Aulia Sari Damanik, and A. Fattah Nasution, “IMAMAH.” [Online]. Available: <https://ejournal.edutechjaya.com/index.php/imamah>