

DAFTAR PUSTAKA
www.itk.ac.id

Adianto, T., Ali, Y. & Saptono, E., 2020. Penilaian Risiko Serangan Siber Sistem Manajemen Keamanan Informasi PT. UAV. *Manajemen Pertahanan*, 6(1), pp. 52-72.

Alghamdi, W. N. M. & Rastogi, R., 2020. *An efficient data flow material model (DFMM) for cyber security risk assessment in real time server*. s.l., Materials Today: Proceedings.

Annarelli, A., Nonino, F. & Palombi, G., 2020. Understanding the Management of Cyber Resilience Systems. *Computers & Industrial Engineering*.

APQC, 2014. *Education Process and Classification Framework*. Houston: American Productivity & Quality Center.

Ardiyanti, H., 2014. Cybersecurity dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica*, 5(1).

Arianto, A. R., 2017. Cyber Security: Geometri Politik dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21. *Jurnal PIR*, 1(2), pp. 108-118.

Arianto, A. R. & Angraini, G., 2019. Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, 9(1), pp. 13-29.

Atrinawati, L. H. et al., 2020. *Assessment of Process Capability Level in University XYZ Based on COBIT 2019*. s.l., Second International Conference on Enhanced Research and Industrial Application 2020 - Engineering.

Babiceanu, R. F. & Seker, R., 2019. Cyber Resilience Protection for Industrial Internet of Things: A Software-Defined Networking Approach. *Computers in Industry*, Volume 104, pp. 47-58.

Badan Siber dan Sandi Negara, 2019. *Laporan Tahunan 2019 : Honeynet Project BSSN - IHP*, Jakarta: Badan Siber dan Sandi Negara.

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J., 2015. New contributions in information systems and technologies. In: *Cyber resilience—fundamentals for a definition*. Cham: Springer, pp. 311-316.

Chang, L. Y. & Coppel, N., 2020. Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, Volume 97.

Chen, L., Dui, H. & Zhang, C., 2020. A resilience measure for supply chain systems considering the interruption with the cyber-physical systems. *Reliability Engineering & System Safety*, Volume 199.

Choudhury, S. et al., 2015. *Action Recommendation for Cyber Resilience*. s.l., In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense.

Cicilio, P. et al., 2020. Electrical grid resilience framework with uncertainty. *Electric Power Systems Research*, Volume 189.

CRR, 2020. *Cyber Resilience Review (CRR) : Method Description and Self-Assessment User Guide*. s.l.:U.S. Department of Homeland Security : Cybersecurity and Infrastructure Security Agency.

Fischer, E. A., 2009. *Creating a National Framework for Cybersecurity: an Analysis of Issues and Options*. New York: Nova Science Publishers, Inc..

Hagen, J., 2018. Building resilience against cyber threats in the energy sector. *International journal of critical infrastructure protection*, Volume 20, pp. 26-27.

Haque, M. A., Shetty, S. & Krishnappa, B., 2019. *ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control System*. Washington DC, The 4th IEEE International Conference on Intelligent Data and Security.

Haque, M. A., Teyou, G. K. D., Shetty, S. & Krishnappa, B., 2018. *Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights*. s.l., IEEE.

Hausken, K., 2020. Cyber Resilience in Firms, Organizations and Societies. *Internet of Things*, Volume 11.

Institut Teknologi Kalimantan, 2016. *Tentang ITK*. [Online] Available at: <https://itk.ac.id/> [Accessed 10 Desember 2020].

Islami, M. J., 2017. Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Jurnal Masyarakat Telematika dan Informasi*, 8(2), pp. 137-144.

Koelemeijer, D., 2018. *Enhancing the Cyber Resilience of Critical Infrastructures through an Evaluation Methodology Based on Assurance Cases*. s.l., Elsevier.

Linkov, I. & Kott, A., 2019. Cyber Resilience of Systems and Networks. In: *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. Cham: Springer, pp. 1-25.

Meilani, D., Arief, I. & Habibitullah, M., 2019. *Designing Disaster Recovery Plan of Data System for University*. s.l., IOP Conf. Series: Materials Science and Engineering.

Nguyen, W. P. V., Nair, A. S. & Nof, S. Y., 2019. *Advancing Cyber-Physical Systems Resilience: The Effects of Evolving Disruptions*. Chicago, 25th International Conference on Production Research Manufacturing Innovation: Cyber Physical Manufacturing.

NIAC, 2009. *Critical Infrastructure Resilience Final Report and Recommendations*, s.l.: National Infrastructure Advisory Council.

NIST, 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1 ed. s.l.: National Institute of Standards and Technology.

Peraturan Menteri Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia Nomor 62, 2017. *Tata Kelola Teknologi Informasi di Lingkungan Kementerian Riset, Teknologi dan Pendidikan Tinggi*, s.l.: Menteri Riset, Teknologi Dan Pendidikan Tinggi.

Perdani, M. D. K., Widyawan & Santosa, P. I., 2018. *Blockchain untuk keamanan transaksi elektronik perusahaan financial technology*. Yogyakarta, Universitas AMIKOM Yogyakarta.

Rahmadi, G. & Pratama, A. R., 2020. Analisis Kesadaran Cyber Security Pada Kalangan Pelaku e-Commerce di Indonesia. *Automata*, 1(2).

Rahmawati, I., 2017. Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, 7(2), pp. 51-66.

Ramadhani, M. R. & Pratama, A. R., 2020. Analisis Kesadaran Cyber Security Pada Pengguna Media Sosial Di Indonesia. *Automata*, 1(2).

Rehak, D., Senovsky, P., Hromada, M. & Lovecek, T., 2019. Complex approach to assessing resilience of critical infrastructure elements. *International journal of critical infrastructure protection*, Volume 25, pp. 125-138.

Riyandhika, R. R. & Pratama, A. R., 2020. Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia. *Automata*, 1(2).

Sepúlveda-Estay, D. A., Sahay, R., Barfod, M. B. & Jensen, C. D., 2020. A Systematic Review of Cyber-Resilience Assessment Frameworks. *Computers & Security*.

Severson, T. A. et al., 2020. A resilient framework for sensor-based attacks on cyber-physical systems using trust-based consensus and self-triggered control. *Control Engineering Practice*, Volume 101.

Sihotang, H. T., 2015. Penerapan Tata Kelola Teknologi Informasi dengan Menggunakan COBIT Framework 4.1 Studi Kasus Pada PT. Perkebunan Nusantara III Medan (PERSERO). *Jurnal Mantik Penusa*, 17(1), pp. 1-7.

Sihotang, H. T. & Sagala, J. R., 2015. Penerapan Tata Kelola Teknologi Informasi dan Komunikasi Pada Domain Align, Plan And Organise (APO) dan Monitor, Evaluate And Assess (MEA) Dengan Menggunakan Framework COBIT 5 Studi Kasus: STMIK Pelita Nusantara Medan. *Jurnal Mantik Penusa*, 18(2), pp. 90-96.

Smith, E. A., 2005. *Effects based operations. Applying network centric warfare in peace, crisis, and war..* Washington DC: Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense.

Srinivas, J., Das, A. K. & Kumar, N., 2019. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, Volume 92, pp. 178-188.

Tonhauser, M. & Ristvej, J., 2019. *Disruptive Acts in Cyberspace, Steps to Improve Cyber Resilience at National Level.* Slovak Republic, Elsevier.

Williams, P. A. H. & Manheke, R. J., 2010. *Small Business - A Cyber Resilience Vulnerability*. Perth, Western Australia, Proceedings of the 1st International Cyber Resilience Conference.

Zhu, C. et al., 2020. Cyber-physical resilience modelling and assessment of urban roadway system interrupted by rainfall. *Reliability Engineering & System Safety*, Volume 204.



www.itk.ac.id