DAFTAR PUSTAKA

[1] A. Mas dan A. Lluı, "Implementing information security best practices on software lifecycle processes : The ISO / IEC 15504 Security Extension," vol. 8, 2014.

[2] M. Andries *et al.*, "The risks associated with cloud computing," *IDEAS Work. Pap. Ser. from RePEc*, hal. 20, 2013.

[3] I. A. Tondel, M. B. Line, dan M. G. Jaatun, "Information security incident management : Current practice as reported in the literature," *Comput. Secur.*, vol. 45, no. September, hal. 42–57, 2014.

[4] V. R. Palilingan dan J. R. Batmetan, "Incident Management in Academic Information System using ITIL Framework," in *IOP conferences Series : materials Science and Engineering*, 2018, hal. 0–9.

[5] A. D. Nugraha dan N. Legowo, "Implementation of incident management for data services using ITIL V3 in telecommunication operator company," in *Proceedings - 2017 International Conference on Applied Computer and Communication Technologies, ComCom 2017*, 2017, vol. 2017-Janua, hal. 1–6.

[6] N. Azizah, Y. Kusumawati, dan R. R. Sani, "Perancangan Manajemen Insiden pada Layanan Teknologi Informasi Inventory Menggunakan Framework ITIL Versi3 (Studi Kasus : PT. Genta Semar Mandiri Semarang)," *JOINS (Journal Inf. Syst.*, vol. 5, no. 1, hal. 136–146, 2020.

[7] D. S. Ilvarianto dan N. Legowo, "Incident management implementation using continual service improvement method at PT AOP," in *Proceedings - 2017 International Conference on Applied Computer and Communication Technologies, ComCom 2017*, 2017, vol. 2017-Janua, hal. 1–7.

[8] Richard, F. L. Gaol, harco L. hendric S. Warnars, E. Abdurachman, dan B. Soewito, "Development of Web Application based on ITIL – Incident Management Framework In Computer," *2019 Int. Conf. Inf. Manag. Technol.*, vol. 1, no. August, hal. 120–125, 2019.

[9] L. Lema-Moreta dan J. Calvo-Manzano, "A proposal for implementation of ITIL incident management process in SMEs," *2017 IEEE 2nd Ecuador Tech. Chapters Meet. ETCM 2017*, vol. 2017-Janua, hal. 1–5, 2018.

[10] O. Ogunyebi, B. Swar, dan S. Aghili, "An Incident Handling Guide for Small Organizations in the Hospitality Sector," in *WorldCIST'18*, 2018, vol. 206, hal. 232–241.

[11] Z. Fadhly, "Perbandingan Manajemen Sektor Pemerintah Dengan Sektor Swasta," *J. Public Policy*, vol. 2, no. 2, hal. 186–195, 2019.

[12] H. Syahrial, "Pengembangan Sistem Manajemen Tanggapan Insiden Keamanan Komputer (Csirms) Studi Kasus Kantor Akuntan Publik," hal. 1–12.

[13] L. Tello-Oquendo *et al.*, "A structured approach to guide the development of incident management capability for security and privacy," in *ICEIS 2019 - Proceedings of the 21st International Conference on Enterprise Information Systems*, 2019, vol. 2, no. Iceis, hal. 328–336.

[14] K. Bernsmed dan I. A. Tøndel, "Forewarned is Forearmed : Indicators for Evaluating Information Security Incident Management," *2013 Seventh Int. Conf. IT Secur. Incid. Manag. IT Forensics*, hal. 3–14, 2013.

[15] I. O. for S. (ISO), *SNI ISO/IEC 27035-1:2016 - Teknologi Informasi - Teknik Keamanan - Manajemen Insiden Keamanan Informasi - Bagian 1 : Prinsip manajemen insiden*. Badan Standardisasi Nasional, 2019, hal. 25.

[16] L. Lema, J.-A. Calvo-Manzano, R. Colomo-palacios, dan M. Arcilla, "ITIL in small to medium-sized enterprises software companies: towards an implementation sequence," *J. Softw. Evol. Process*, vol. 25, no. 7, hal. 681–709, 2015.

[17] M. B. Line, I. A. Tøndel, dan M. G. Jaatun, "Information security incident management : Planning for failure," in *Eighth International Conference on IT Security Incident Management & IT Forensics*, 2014, hal. 47–61.

[18] C. Hove, T. Marte, M. B. Line, dan K. Bernsmed, "Information security incident management : Identified practice in large organizations," in *Eighth International Conference on IT Security Incident Management & IT Forensics Information*, 2014, hal. 27–46.

[19] N. H. Ab Rahman dan K. K. R. Choo, "A survey of information security incident handling in the cloud," *Comput. Secur.*, vol. 49, hal. 45–69, 2015.

[20] R. Baskerville, P. Spagnoletti, dan J. Kim, "Incident-centered information security : Managing a strategic balance between prevention and response," *Inf. Manag.*, vol. 51, no. 1, hal. 138–151, 2014.

[21] S. Fuada, "Incident Management of Information Technology in the Indonesia Higher Education based on COBIT Framework : A Review," *EAI Endorsed Trans. Energy Web*, vol. 6, no. 21, 2019.

[22] M. Bartnes, N. Brede, dan P. E. Heegaard, "The future of information security incident management training : A case study of electrical power companies," *Comput. Secur.*, vol. 61, no. 217528, hal. 32–45, 2016.

[23] G. Tsakalidis, K. Vergidis, S. Petridou, dan M. Vlachopoulou, "A cybercrime incident architecture with adaptive response policy," *Comput. Secur.*, vol. 83, hal. 22–37, 2019.

[24] A. B. Setiawan, "Perencanaan Strategis Sistem Informasi Pada Pusat Penanganan Insiden Keamanan Informasi Sektor Pemerintah," *J. Masy. Telemat. dan Inf.*, vol. 5, no. 1, hal. 1–24, 2014.

[25] T. P. Silitonga, A. Holil, dan N. Ali, "Sistem Manajemen Insiden Pada Program Manajemen Helpdesk Dan Dukungan Ti Berdasarkan Framework Itil V3 (Studi Kasus Pada Biro Teknologi Informasi BPK-RI)," vol. 2010,

no. Seminar Nasional Informatika, hal. 210–218, 2010.

[26]   M. E. Whitman dan H. J. Mattord, *Principles of Information Security*, no. September. 2011.

[27]   I. O. for S. (ISO), *SNI ISO/IEC 27035-2:2016 - Teknologi Informasi - Teknik Keamanan - Manajemen Insiden Keamanan Informasi - Bagian 2 : pedoman perencanaan dan persiapan respon insiden*. Badan Standardisasi Nasional, 2019, hal. 72.

[28]   Peraturan Presiden RI, "Sistem Pemerintahan Berbasis Elektronik." hal. Nomor 95 Tahun 2018, 2018.

[29]   Y. E. Karabulut, G. Boylu, E. U. Kucuksille, dan M. A. Yalcinkaya, "Characteristics of Cyber Incident Response Teams in the World and Recommendations for Turkey," *Balk. J. Electr. Comput. Eng.*, vol. 3, no. 4, hal. 175–178, 2015.

[30]   R. Ruefle, K. Van Wyk, dan L. Tosic, *New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)*, no. May. 2013, hal. 86.