DAFTAR PUSTAKA

[1] Kementerian PAN RB, "Pedoman Manajemen Risiko SPBE," pp. 1–30, 2020.

[2] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Comput. Secur.*, vol. 57, pp. 14–30, 2016, doi: 10.1016/j.cose.2015.11.001.

[3] C. Izuakor and R. White, "Critical Infrastructure Asset Identification : Policy , Methodology and Gap Analysis," 2017.

[4] B. K. Tripathy, "Risks Assessment in IT Infrastructure," *Intech*, no. tourism, p. 13, 2016, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics.

[5] L. Tsipouri *et al.*, *Risk management in the procurement of innovation*. 2010.

[6] J. W. Wairiuko, D. R. Nyonje, and D. E. O. Omulo, "Human Resource Capacity and Adoption of E-Government for Improved Service Delivery in Kajiado County, Kenya," *Int. J. Bus. Soc. Sci.*, vol. 9, no. 10, pp. 94–110, 2018, doi: 10.30845/ijbss.v9n10p10.

[7] G. F. Khan, J. Moon, C. Rhee, and J. J. Rho, "E-government skills Identification and Development: Toward a Staged-Based User-Centric Approach for Developing Countries," *Asia Pacific Journal of Information Systems*, vol. 20, no. 1. pp. 1–31, 2010.

[8] M. Hamner, D. Taha, and S. Brahimi, "Human factors in implementing e-government in developing countries," *Citizens E-Government Eval. Policy Manag.*, no. September, pp. 184–206, 2010, doi: 10.4018/978-1-61520-931-6.ch010.

[9] "Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi - Indeks SPBE 2020 Meningkat, Pemerintah Tidak Berpuas Diri." https://menpan.go.id/site/berita-terkini/indeks-spbe-2020-meningkat-pemerintah-tidak-berpuas-diri (accessed May 29, 2021).

[10] K. PAN-RB, “Hasil evaluasi SPBE 2020.pdf.” .

[11] Kementerian PAN RB, “Peraturan Menteri PAN & RB No. 59 Tahun 2020 Tentang Pemantauan dan Evaluasi SPBE,” 2020.

[12] H. I. Kure and S. Islam, “Assets focus risk management framework for critical infrastructure cybersecurity risk management,” *IET Cyber-Physical Syst. Theory Appl.*, vol. 4, no. 4, pp. 332–340, 2019, doi: 10.1049/iet-cps.2018.5079.

[13] I. Manea and I. Popa, “Risk Management in Public Procurement Process,” *Stud. Sci. Res. Econ. Ed.*, no. 15, pp. 389–396, 2010, doi: 10.29358/sceco.v0i15.145.

[14] T. Kalvet, “Risks Management in Public Procurement for Innovation: The Case of Nordic-Baltic Sea Cities,” 2013.

[15] R. G. Utomo, G. Wills, and R. Walters, “A framework for factors influencing the implementation of information assurance for e-Government in Indonesia,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 3, pp. 1025–1034, 2020, doi: 10.18517/ijaseit.10.3.9186.

[16] J. R. S. Fraser and B. J. Simkins, “The challenges of and solutions for implementing enterprise risk management,” *Bus. Horiz.*, vol. 59, no. 6, pp. 689–698, 2016, doi: 10.1016/j.bushor.2016.06.007.

[17] M. Marrone and L. M. Kolbe, “Impact of IT Service Management Frameworks on the IT Organization,” *Bus. Inf. Syst. Eng.*, vol. 3, no. 1, pp. 5–18, 2011, doi: 10.1007/s12599-010-0141-5.

[18] A. Shrestha, “Development and Evaluation of a Software-Mediated Process Assessment Approach in IT Service Management,” p. 314, 2015.

[19] K. Tiatasin, “IT Risk Management for E-Government Implementation Success,” pp. 61–72, 2015.

[20] ISO31000, “BS ISO 31000 : 2018. Risk management — Guidelines,” *BSI Stand. Publ.*, 2018.

[21] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, “Assessing information

security risks in the cloud: A case study of Australian local government authorities," *Gov. Inf. Q.*, vol. 37, no. 1, p. 101419, 2020, doi: 10.1016/j.giq.2019.101419.

[22] N. A. Sunday, "Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures," *Blekinge Inst. Technol. Sch. ...*, no. August, pp. 1–52, 2018, [Online]. Available: https://www.diva-portal.org/smash/get/diva2:831198/FULLTEXT01.pdf%0Ahttp://www.medieteknik.bth.se/fou/cuppsats.nsf/all/2cf7d7f61e47ae4ec1257514004fce3f/$file/WLAN_Security Risk Assessment and Countermeasures.pdf.

[23] A. Shrestha, A. Cater-Steel, W. G. Tan, and M. Toleman, "A model to select processes for IT service management improvement," *ACIS 2012 Proc. 23rd Australas. Conf. Inf. Syst.*, pp. 1–10, 2012.

[24] H. Al Farsi, "Factors Influencing The Effectiveness Of Enterprise Risk Management (ERM) In Publicly Listed Companies In Oman," vol. 9, no. 03, pp. 6750–6760, 2020.

[25] A. R. Otero, *Information Technology Control and Audit*. 2018.

[26] E. Jordan and L. Silcock, "Beating IT Risks," p. 292, 2005, [Online]. Available: http://books.google.com/books?id=BYWlMtM6EBYC&pgis=1%5Cnftp://pedidos.rafalim.com/Risk Management/Beating IT Risks.pdf.

[27] ISACA, *COBIT 5 Framework*. 2012.

[28] ISO/IEC, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and," vol. 2018, 2018.

[29] ISACA, *COBIT 5*. .

[30] J. Simota, J. Tupa, and F. Steiner, "Risk Management to Enhance Performance in the Construction SME Sector; Theory and Case Study," in *Risk Management Treatise for Engineering Practitioners*, 2018.

[31] C. Callahan and J. Soileau, "Does Enterprise risk management enhance

operating performance?," *Adv. Account.*, 2017, doi: 10.1016/j.adiac.2017.01.001.

[32] M. Al 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.

[33] G. Giannopoulos, B. Dorneanu, and O. Jonkeren, *Risk Assessment Methodology for Critical Infrastructure Protection*. 2012.

[34] J. Cresswell, "Research Design Qualitative, Quantitative, and Mixed Methods Approach," *Intercult. Educ.*, vol. 20, no. 2, pp. 127–133, 2009, doi: 10.1080/14675980902922143.

[35] M. A. Achachlouei and L. M. Hilty, *Progress in Information System*. 2016.

[36] V. Venkatesh and S. A. Brown, "Bridging the Qualitative–Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *J. Crit. Realis.*, vol. 17, no. 2, pp. 118–139, 2018.

[37] Meher, "Risk Assessment on IT Infrastructure," *Risk Manag.*, vol. 24, no. 4, pp. 1–7, 2018.

[38] P. I. Santosa, "Metode Penelitian Kuantitatif Pengembangan Hipotesis dan Pengujian SmartPLS," *ANDI, Yogyakarta*. Andi, Yogyakarta, p. 1, 2018.

[39] HM Treasury, "Management of Risk in Government," no. January, p. 44, 2017, [Online]. Available: https://www.gov.uk/government/publications/management-of-risk-in-government-framework.

[40] R. G. Hassan and O. O. Khalifa, "E-Government - an Information Security Perspective," *Int. J. Comput. Trends Technol.*, vol. 36, no. 1, pp. 1–9, 2016, doi: 10.14445/22312803/ijctt-v36p101.

[41] R. Munir, M. R. Mufti, I. Awan, Y. F. Hu, and J. P. Disso, "Detection, mitigation and quantitative security risk assessment of invisible attacks at

enterprise network," *Proc. - 2015 Int. Conf. Futur. Internet Things Cloud, FiCloud 2015 2015 Int. Conf. Open Big Data, OBD 2015*, pp. 256–263, 2015, doi: 10.1109/FiCloud.2015.24.

[42] R. Breu, F. Innerhofer-Oberperfler, and A. Yautsiukhin, "Quantitative assessment of enterprise security system," *ARES 2008 - 3rd Int. Conf. Availability, Secur. Reliab. Proc.*, no. September 2014, pp. 921–928, 2008, doi: 10.1109/ARES.2008.164.

[43] Sugiyono, *Metode Penelitian Kombinasi (mixed Methods)*. 2018.

[44] P. D. A. Ferdinand, *Metode Penelitian Manajemen: Pedoman Penelitian untuk Skripsi, Tesis dan Disertasi Ilmu Manajemen*. 2016.

[45] I. Ghozali and H. Latan, *Partial Least Squares : Konsep, Teknik dan Aplikasi Smart PLS 3.0 untuk Penelitian Empiris*. 2015.

[46] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, 2011, doi: 10.2753/MTP1069-6679190202.