REFERENCES

Adam Shostack. (2014). *【AdamShostack】Threat Modeling : Designing for Security*.

Alberts, C. J., & Dorofee, A. J. (2001). *OCTAVE Method Implementation*. *1*(June).

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research*, *3*(1). https://doi.org/10.5430/elr.v3n1p39

BSI Standards Publication. (2018). BS ISO 31000 : 2018 BSI Standards Publication Risk management — Guidelines. *BSI Standards Publication*, *ISO31000*, 26. https://www.ashnasecure.com/uploads/standards/BS ISO 31000-2018.pdf

Chapple, M., Stewart, J., & Gibson, D. (2018). *Certified Information System Security Professional, Official Study Guide*.

Direktorat Jendral Prasarana dan Sarana Pertanian, K. P. (2020). *02-Pedoman-Premi-Bantuan-Asuransi-Usahatani-Padi-Tahun-2020.pdf*.

Dokumen risk. (n.d.).

FIRST. (2019). *Common Vulnerability Scoring System version 3.1 Specification Document Revision 1*. 1–24. https://www.first.org/cvss/

Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A Fair Approach*. https://books.google.co.uk/books/about/Measuring_and_Managing_Information_Risk.html?id=OkOwoAEACAAJ&pgis=1

Gregory, P. H. (2017). All in One is All You Need - CISM all in one. In *Journal of Chemical Information and Modeling* (Vol. 53, Issue 9).

Hathaway, T., & Hathaway, A. (2015). *Data Flow Diagramming by Example: Process Modeling Techniques for Requirements Elicitation*. 75.

SWISS GERMAN UNIVERSITY

How to Use DREAD Analysis with FAIR. (n.d.). Retrieved November 25, 2020, from https://www.fairinstitute.org/blog/how-to-use-dread-analysis-with-fair

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. *Sci.Int.(Lahore)*, *26*(4), 1607–1609.

ISACA. (2010). RISK IT BASED ON COBIT. *Exchange*, *32*(2), 61–64. http://search.ebscohost.com.idpproxy.reading.ac.uk/login.aspx?direct=true&AuthType=ip,shib,uid&db=eax&AN=508147495&site=ehost-live

ISACA. (2011). *ISACA, Certified Risk and Information Systems Control*. Information Systems Audit and Control. www.fgv.br/editora

ISACA. (2015). Cybersecurity Fundamentals Study Guide. *CyberSecurity Nexus*, xvii–xviii.

Jerzy, L. B., & Wilimowska, Z. (2017). Information Systems Architecture and Technology_ Proceedings of 39th International Conference on Information Systems Architecture and Technology. In *Information Systems Architecture And Technology: Proceedings of 38th International Conference on Information Systems Architecture And Technology - ISAT 2017 - Part II*.

Kementerian Pertanian Republik Indonesia. (n.d.). Retrieved November 25, 2020, from https://www.pertanian.go.id/

Khan, R., Mclaughlin, K., Laverty, D., & Sezer, S. (2017). *STRIDE-based Threat Modeling for Cyber-Physical Systems*. 0–5.

Komisioner, D., & Jasa, O. (2015). *Otoritas jasa keuangan republik indonesia*.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, *8*(6). https://doi.org/10.3390/app8060898

Landoll, D. (2016). The Security Risk Assessment Handbook. In *The Security Risk Assessment Handbook*. https://doi.org/10.1201/b10937

SWISS GERMAN UNIVERSITY

LAPORAN KINERJA AUTP. (n.d.).

Lientz, B. P. (2011). Information Technology Project Management. In *Information Technology Project Management*. https://doi.org/10.1007/978-0-230-34500-3

Ltd, A. T. (2003). Creating Secure Systems through Attack Tree Modeling. *Amenaza Technologies Ltd*. http://www.amenaza.com/downloads/docs/5StepAttackTree_WP.pdf

Maheshwari, V., & Prasanna, M. (2016). *Integrating Risk assessment and Threat modeling within SDLC process*.

Marksteiner, S., Vallant, H., & Nahrgang, K. (2019). Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. *Journal of Information Security and Applications*, *49*, 102389. https://doi.org/10.1016/j.jisa.2019.102389

Martins, G., Bhatia, S., Koutsoukos, X., Stouffer, K., Tang, C., & Candell, R. (2015). Towards a systematic threat modeling approach for cyber-physical systems. *Proceedings - 2015 Resilience Week, RSW 2015*, 114–119. https://doi.org/10.1109/RWEEK.2015.7287428

Muchandi, V. (2007). Applying 4+ 1 view architecture with UML 2. *FCGSS White Paper*, 1–11. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Applying+4+++1+View+Architecture+with+UML+2#5

Nweke, L. O., & Wolthusen, S. D. (2020). A review of asset-centric threat modelling approaches. *International Journal of Advanced Computer Science and Applications*, *11*(2), 1–6. https://doi.org/10.14569/ijacsa.2020.0110201

Nyamwanza, T. (2014). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 40 TAHUN 2014 TENTANG PERASURANSIAN*. *2014*(June), 1–2. https://repositories.lib.utexas.edu/handle/2152/39127%0Ahttps://cris.brighton.ac.uk/ws/portalfiles/portal/4755978/Julius+Ojebode%27s+Thesis.pdf%0Ausir.salford.ac.uk/29369/1/Angela_Darvill_thesis_esubmission.pdf%0Ahttps://dspace.lbor

o.ac.uk/dspace-jspui/ha

O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and Evolution*, *9*(1), 20–32. https://doi.org/10.1111/2041-210X.12860

Olowu, T. O., Sundararajan, A., Moghaddami, M., Sarwat, A. I., Unigwe, O., Okekunle, D., Kiprakis, A., Latif, A., Gawlik, W., & Palensky, P. P. (2014). Financial Risk Management. *CIRED - Open Access Proceedings Journal*, *2017*(July), 1–67. http://www.eskom.co.za/CustomerCare/TariffsAndCharges/Documents/RSA Distribution Tariff Code Vers 6.pdf%0Ahttp://www.nersa.org.za/

Podeswa, H. (2010). *UML for the IT business analyst : a practical guide to object-oriented requirements gathering*.

Saitta, P., Larcom, B., & Eddington, M. (2005). Trike v. 1 methodology document. *URL: Http://Dymaxion. Org/Trike/ …*, 1–17. http://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf

Schlegel, R., Obermeier, S., & Schneider, J. (2015). Structured system threat modeling and mitigation analysis for industrial automation systems. *Proceeding - 2015 IEEE International Conference on Industrial Informatics, INDIN 2015*, 197–203. https://doi.org/10.1109/INDIN.2015.7281734

Shevchenko, N., Chick, T. A., Riordan, P. O., Scanlon, T. P., & Woody, C. (2018). Threat Modeling : a Summary of Available Methods. *Research Report*, *July*, 26. https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

Shevchenko, N., Frye, B. R., Woody, C., & States, C. M. U. S. E. I. P. U. (2018). *Threat Modeling: Evaluation and Recommendations*. *September*. https://apps.dtic.mil/sti/pdfs/AD1083907.pdf

Sion, L., Yskout, K., Van Landuyt, D., & Joosen, W. (2018a). Risk-based design security analysis. *Proceedings - International Conference on Software*

Engineering, *i*, 11–18. https://doi.org/10.1145/3194707.3194710

Sion, L., Yskout, K., Van Landuyt, D., & Joosen, W. (2018b). Solution-aware data flow diagrams for security threat modeling. *Proceedings of the ACM Symposium on Applied Computing*, 1425–1432. https://doi.org/10.1145/3167132.3167285

Soares Cruzes, D., Gilje Jaatun, M., Bernsmed, K., & Tondel, I. A. (2018). Challenges and experiences with applying microsoft threat modeling in agile development projects. *Proceedings - 25th Australasian Software Engineering Conference, ASWEC 2018*, 111–120. https://doi.org/10.1109/ASWEC.2018.00023

Souppaya, M., & Scarfone, K. (2016). *[Draft] NIST Special Publication 800-154: Guide To Data-Centric System Threat Modeling*. 25. http://csrc.nist.gov/publications.%0Ahttp://csrc.nist.gov/publications/PubsSPs.html%5Cnhttp://csrc.nist.gov/publications/PubsDrafts.html#SP-800-154%5Cnhttp://csrc.nist.gov/publications/drafts/800-154/sp800_154_draft.pdf

Suprihanto, D., Prahasto, T., & Sugiharto, A. (2013). Penilaian Risiko Aplikasi Web Menggunakan Model DREAD. *Jurnal Sistem Informasi Bisnis*, *3*(2). https://doi.org/10.21456/vol3iss2pp59-66

There is Nothing Simple About FAIR | SimpleRisk. (n.d.). Retrieved November 25, 2020, from https://www.simplerisk.com/blog/there-is-nothing-simple-about-fair

Three Tenets of Information Security Defined | LBMC Security. (n.d.). Retrieved November 24, 2020, from https://www.lbmc.com/blog/three-tenets-of-information-security/

Torkura, K. A., Sukmana, M. I. H., Meinig, M., Cheng, F., Meinel, C., & Graupner, H. (2018). A threat modeling approach for cloud storage brokerage and file sharing systems. *IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*, 1–5. https://doi.org/10.1109/NOMS.2018.8406188

Tseng, T. W., Wu, C. T., & Lai, F. (2019). Threat Analysis for Wearable Health

SWISS GERMAN UNIVERSITY

Devices and Environment Monitoring Internet of Things Integration System. *IEEE Access*, *7*, 144983–144994. https://doi.org/10.1109/ACCESS.2019.2946081

Ucedavélez, T., & Morana, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. In *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. https://doi.org/10.1002/9781118988374

Visual. (2019). *What is Data Flow Diagram?* Lucidchart.Com. https://www.visual-paradigm.com/guide/data-flow-diagram/what-is-data-flow-diagram/

Withers, R. (2018). Software and attack centric integrated threat modeling for quantitative risk assessment. *Slate*, 99–108. https://slate.com/arts/2018/01/seth-meyers-looks-into-trumps-declining-work-hours-and-mental-capacity.html

Zeinali, M., & Hadavi, M. A. (2018). Threat Extraction Method Based on UML Software Description. *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology, ISCISC 2018*, 1–8. https://doi.org/10.1109/ISCISC.2018.8546868

SWISS GERMAN UNIVERSITY