DAFTAR PUSTAKA

Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluations (OCTAVE(SM)) Framework, Version 1.0. Carnegie Mellon Software Engineering Institute,. *Network Systems Survivability Program*, (June).

Gary Stonebumer, Alice Goguen, A. F. (2002). Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology, *30*(July).

Hayes, D. F., & Stevens, D. K. (2004). OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation.

Lipol, L. S., & Haq, J. (2011). Risk analysis method : FMEA / FMECA in the organizations. *International Journal of Basic & Applied Sciences*, *11*(5), 5–74.

Nawangsih, N. (2017). Pembuatan Standar Operasional Prosedur Kontrol Akses Physical Dan Logical Pada Aplikasi Sistem Informasi Rumah Sakit (SIMRS) Menggunakan Kerangka Kerja OCTAVE , FMEA dan Kontrol ISO 27002 : 2013 (Studi Kasus : Instalasi Pengelola Data Elektronik Rumah.

Obrand, L., Augustsson, N.-P., Holmstrom, J., & Mathiassen, L. (2012). The Emergence of Information Infrastructure Risk Management in IT Services. *2012 45th Hawaii International Conference on System Sciences*, 4904–4913. https://doi.org/10.1109/HICSS.2012.565

Paul Hopkin. (2010). *Fundamentals of Risk Management Understanding, evaluating and implementing effective risk management*.

QAPI. (2006). Guidance for Performing Failure Mode and Effects Analysis with Performance Improvement Projects.

Rachmawan, D. I. (2017). *Pembuatan Dokumen Sop Prosedur) Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja Iso 27002 : 2013 (Studi Kasus : Cv Cempaka Tulungagung) Developing Standard Operational Procedure (Sop) Document for Asset Information Security Refer To*.

Scangas, A. (n.d.). FMEA F ailure Mode and Effects Analysis.

Software, S. P. L. M. (2016). How to conduct a failure modes and effects analysis. *A White Paper Issued by: Siemens PLM Software*. Retrieved from www.siemens.com/polarion

Supradono, B. (2009). Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat , Asset , and Vulnerability Evaluation). *Media Elektrika*, *2*(1), 4–8.

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus : Sistem Informasi Akademik Universitas XYZ). *CoreIT*, *2*(2), 8–13.

Symantec. (2008). IT RIs k Management. *Strategy*, *2*(December 2007), 52.

Wiranata, I. P. A. (2017). Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 Pada Ruang Server STIE Perbanas Surabaya, 177.