Desain dan analisis kerangka kerja keamanan informasi berdasarkan kombinasi NIST CSF Versi 1.1, ISO/IEC 27002: 2013 dan COBIT 2019 sebagai instrumen pengukuran tingkat kematangan keamanan siber: (Studi kasus: Pusat Data dan Teknologi, Informasi Komunikasi, Badan XYZ) = Design and analysis of information security frameworks based on the combination of NIST CSF Version 1.1, ISO/IEC 27002: 2013 and COBIT 2019 as instruments for measuring cybersecurity maturity level: (Case study: Data and Technology Center, Information Communication of XYZ Agency).

Diah Sulistyowati, author

Abstrak

Tren digitalisasi yang semakin meningkat pada situasi pandemi Covid-19 saat ini telah mempengaruhi gaya hidup masyarakat baik individu maupun organisasi dan mengubah perilaku konvensional menjadi digital. Era digital menawarkan berbagai kemudahan, namun disisi lain terdapat tantangan berupa ancaman siber yang mempengaruhi keamanan siber suatu negara. Dalam rangka meningkatkan keamanan siber secara lebih efektif dan efisien pada salah satu Instansi Pemerintah di Indonesia, Pusat Data dan Teknologi Informasi Komunikasi (TIK) yang merupakan salah satu unsur pendukung di Badan XYZ menjadi obyek penelitian dalam rencana implementasi pengukuran kematangan keamanan siber. Berdasarkan kondisi saat ini, dapat diketahui bahwa implementasi pengelolaan keamanan TIK belum diterapkan secara optimal. Mengacu hal tersebut, maka dibutuhkan kerangka kerja keamanan secara komprehensif yang akan membantu dalam pengelolaan TIK secara lebih aman dalam mengantisipasi adanya ancaman siber yang semakin meningkat. Dalam penelitian ini, akan melakukan perancangan kerangka kerja kematangan keamanan siber dengan melakukan integrasi berdasarkan kerangka kerja, standar NIST CSF, ISO 27002 dan COBIT 2019. Hasil dari penelitian ini diantaranya: Kerangka kerja (framework) kematangan keamanan siber yang dihasilkan terdiri dari 201 aktivitas yang dapat diimplementasikan oleh organisasi, dan terbagi dalam 38 kategori pada framework kematangan keamanan siber. Selain itu, distribusi aktivitas dalam framework terdiri dari 21.56% berasal dari NIST CSF Model, 14.59% berasal dari ISO 27002, dan 63.85% berasal dari COBIT 2019 Model. Melalui konsep kerangka kerja kematangan keamanan siber yang dihasilkan diharapkan dapat menjadi masukan dalam penyusunan instrumen tingkat kematangan keamanan siber dan sandi secara organisasi.

.....The increasing trend of digitization in the current Covid-19 pandemic situation has affected the lifestyles of both individuals and organizations and changed conventional behavior to digital. The digital era offers various conveniences, but on the other hand, there are challenges in the form of cyber threats that affect the cybersecurity of a country. To improve cybersecurity more effectively and efficiently at one of the Government Agencies in Indonesia, the Center for Data and Information and Communication Technology (ICT), one of the XYZ Agency’s supporting elements, is the research object in implementing cybersecurity maturity. Based on current conditions, it can be seen that the implementation of ICT security management has not been implemented optimally. A comprehensive security framework is needed that will assist in managing ICT more securely in anticipating the increasing cyber threats. This research/ will design a

cybersecurity maturity framework by integrating based on the framework, the NIST CSF standard, ISO 27002, and COBIT 2019. The results of this study include: The resulting cybersecurity maturity framework consists of 201 activities that can be implemented by the organization/ and is divided into 38 categories in the cybersecurity maturity framework. In addition, the distribution of activities in the frameworks consists of 21.56% derived from the NIST CSF Model, 14.59% comes from ISO 27002, and 63.85% comes from the COBIT 2019 Model. Through the concept of cybersecurity maturity framework produced, it is hoped that it becomes an input for preparing an organizational cybersecurity maturity level instrument.