# Perancangan Manajemen Risiko Keamanan Informasi: Studi Kasus Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara = Designing Information Security Risk Management: A Case Study of National Cyber Security Operation Center in National Cyber and Crypto Agency

Mas Merdekadyarta, author



---

Abstrak

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 12 merupakan peraturan yang mendasari tentang manajemen risiko dalam sistem elektronik. pada Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik menyebutkan bahwa Sistem Manajemen Pengamanan Informasi (SMPI) adalah pengaturan kewajiban bagi Penyelenggara Sistem Elektronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko. Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) merupakan unit kerja di Badan Siber dan Sandi Negara yang melaksanakan tugas memegang kendali operasi keamanan siber Indonesia. Adanya serangan siber yang semakin besar hingga tercatat pada tahun 2020 terdapat 495.337.202 anomali yang menyerang di jaringan Indonesia, hal ini dibutuhkan keandalan Pusopskamsinas dalam melaksanakan monitoring lalu lintas siber di Indonesia. Dalam penyelenggaraan operasi keamanan siber tentu terdapat kerawanan dan potensi ancaman yang memberikan dampak negatif/risiko terhadap organisasi di mana risiko tersebut dapat dilakukan mitigasi dengan menerapkan manajemen risiko keamanan informasi pada Pusopskamsinas. Salah satu Indikator Sasaran Kegiatan Pusopskamsinas yaitu “Meningkatnya Kualitas Pemonitoran Keamanan Siber atas Serangan dan Ancaman Siber”. Berdasarkan data Laporan Kinerja Pusopskamsinas tahun 2020, diketahui bahwa Pusopskamsinas belum dapat memenuhi target kinerja dari indikator kinerja sasaran dengan capaian nilai 65% dari target capaian 100%. Tidak tercapainya target kinerja dapat berpengaruh terhadap Indikator Kinerja Utama (IKU) organisasi sebagai penentu ukuran tingkat keberhasilan sasaran strategis sehingga diperlukan adanya evaluasi kinerja organisasi. Berdasarkan hasil analisis permasalahan digunakan Business Model for Information Security dari ISACA yaitu Organization, People, Technology, dan Process, salah satu instrumen dari segi organisasi yang belum tersedia adalah dokumen Perencanaan Manajemen Risiko Keamanan Informasi. Penelitian ini merupakan penelitian menggunakan metode kualitatif dengan metode penarikan kesimpulan berupa secara induktif dan merupakan klasifikasi penelitian studi kasus. Pengumpulan data dilakukan melalui observasi, studi dokumen, dan wawancara kepada pejabat, pengelola layanan / tim operasional, serta perwakilan stakeholder. Hasil dari penelitian ini berupa Perencanaan Manajemen Risiko yang sesuai dengan kondisi Pusopskamsinas sehingga dapat membantu pencapaian target kinerja serta meningkatkan pencapaian Rencana Strategis BSSN.

..... Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions Article 12 is an underlying regulation concerning risk management in electronic systems. Regulation of the National Cyber and Crypto Agency Number 8 of 2020 concerning Security Systems in the Operation of Electronic Systems states that the Information Security Management System (ISMS) is a regulation of obligations for Electronic System Operators in implementing information security management

based on risk principles. The National Cyber Security Operations Center (Pusopskamsinas) is a work unit in the National Cyber and Crypto Agency that carries out the task of controlling Indonesian cybersecurity operations. The existence of cyber-attacks is getting bigger until it was recorded that in 2020 there were 495,337,202 anomalies attacking the Indonesian network, this required the reliability of Pusopskamsinas in carrying out cyber traffic monitoring in Indonesia. In carrying out cyber security operations, of course there are vulnerabilities and potential threats that have a negative impact / risk on the organization where these risks can be mitigated by implementing information security risk management at Pusopskamsinas. One of the indicators of the Pusopskamsinas activity target is "Increasing the Quality of Cyber Security Monitoring of Cyber Attacks and Threats". Based on data from the 2020 Pusopskamsinas Performance Report, it is known that the Pusopskamsinas has not been able to meet the performance targets of the target performance indicators with a score of 65% of the 100% achievement target. The failure to achieve the performance targets can affect the main performance indicators (IKU) of the organization as a determinant of the level of success of strategic targets so that an evaluation of organizational performance is needed. Based on the results of the problem analysis, ISACA's Business Model for Information Security is used, namely Organization, People, Technology, and Process. One of the instruments in terms of organization that is not yet available is the Information Security Risk Management Planning document. This research is using qualitative methods such as inductive inference and the classification of a case study. Data collected through observation, study of documents and interviews of officials, managers of services / operations team, and stakeholder representatives. The results of this study are in the form of a Risk Management Planning in accordance with the conditions of the Pusopskamsinas so that it can help achieve performance targets and increase the achievement of the BSSN Strategic Plan.