Desain kerangka kerja manajemen risiko keamanan informasi berdasarkan integrasi ISO/IEC 27005:2018, NIST SP 800-39, octave allegro dan COBIT 2019: studi penerapan awal di Pusat Pendidikan dan Pelatihan Badan XYZ = Information security risk management framework design based on ISO/IEC 27005:2018, NIST SP 800-39, octave allegro and COBIT 2019: initial study at Learning and Training Center of XYZ Agency

Imam Baehaki, author

Abstrak

Terdapat beberapa jenis pendekatan manajemen risiko keamanan informasi sebagai panduan dalam menerapkan program risiko keamanan. Setiap pendekatan mempunyai tujuan dan metodologi yang berbeda tergantung pada kebutuhan dan selera organisasi yang melakukannya. Jika suatu organisasi memiliki personel yang kompeten untuk mengimplementasikan manajemen risiko keamanan informasi, maka akan mudah untuk melakukannya. Namun, itu akan menjadi tantangan bagi organisasi yang tidak memiliki personil yang kompeten. Tujuan dari penelitian ini adalah untuk merancang kerangka kerja manajemen risiko keamanan informasi yang sederhana namun memenuhi prinsip-prinsip manajemen risiko keamanan informasi. Desain didasarkan pada integrasi empat pendekatan manajemen risiko keamanan informasi yang berbeda. ISO 27005 mewakili standar, Risk Management Framework (RMF) oleh NIST mewakili pedoman, OCTAVE Allegro mewakili metodologi, dan COBIT mewakili kerangka kerja. Integrasi tersebut dipenuhi dengan melakukan analisis komparatif dengan menyortir dan menggabungkan berdasarkan proses aktivitas manajemen risiko keamanan informasi. Penyortiran diterapkan untuk mendapatkan desain model sederhana, dan penggabungan digunakan untuk mendapatkan desain model lengkap. Desain model sederhana terdiri dari proses identifikasi, pengukuran, administrasi dan pemantauan. Proses identifikasi terdiri dari identifikasi konteks dan komponen risiko. Proses pengukuran meliputi pengukuran faktor risiko dan risiko. Proses administrasi menghasilkan rencana penanganan risiko dan pengambilan keputusan. Proses pemantauan dengan objek perubahan dan pertukaran informasi. Untuk memvalidasi hasil perancangan desain model sederhana, dilakukan studi penerapan awal dalam bentuk simulasi penerapan di Pusdiklat Badan XYZ. Hasil studi penerapan awal ini adalah mayoritas responden baik online maupun offline menyatakan bahwa desain sederhana namun memenuhi prinsip manajemen risiko keamanan informasi dibuktikan dengan seluruh indikator evaluasi penerapan desain bernilai di atas passing grade 50%.
.....There are several types of information security risk management (ISRM) methods as guidance in implementing a security risk program. Each method carried different goals and methodologies depending on the needs and tastes of the organization that carried it out. If an organization has personnel who are competent to implement ISRM, it will be easy to do so. However, it will be challenging for an organization that lacks skilled personnel. The purpose of this study is to design a framework for ISRM that is simple but meets the principles of ISRM. The design is based on the integration of four different ISRM methods. ISO 27005 represents the standard, RMF by NIST represents guidelines, OCTAVE represents methodology, and COBIT represents framework. The integration is fulfilled by conducting a comparative analysis by sorting and merging based on the activity processes of ISRM. The result of this study is two designs of ISRM,

namely full design and simple design. Sorting is applied to get a simple design, and merging is used to get a full design. The simple model design consists of the process of identification, measurement, administration and monitoring. The identification process consists of identifying the context and components of risk. The measurement process includes the measurement of risk and risk factors. The administrative process produces a plan for risk management and decision making. The process of monitoring with objects of change and information exchange. To validate the results of the design of a simple model, a preliminary implementation study was carried out in the form of a simulation application at the XYZ Agency Training Center. The results of this preliminary implementation study are that the majority of respondents both online and offline stated that the design was simple but met the principles of information security risk management, evidenced by all the indicators of the evaluation values above 50% passing grade.