Rancangan kebijakan dan prosedur pengelolaan integritas data berbasis COBIT dan ISO 27001 : studi kasus Direktorat XYZ = Data integrity management policy and procedure design based on COBIT and ISO 27001 : case study Directorate XYZ

Nur Indrawati, author

Abstrak

Sertifikasi di lingkungan Direktorat XYZ sebagai salah satu aktivitas utama di lingkungan Direktorat XYZ tidak lepas dari peran SI/TI untuk mendukung layanan sertifikasi secara optimal, yang pada akhirnya dapat memberikan layanan optimal sertifikasi. Agar dapat memberikan layanan prima sertifikasi, diperlukan adanya data yang berkualitas, yang dapat memenuhi kriteria, reliabilitas, integritas, dan ketersediaannya.

COBIT 4.1 dan SNI ISO/IEC 27001:2009 merupakan kerangka kerja tata kelola TI dan standar keamanan informasi yang merupakan praktik terbaik. Pengkombinasian keduanya dalam penyusunan kebijakan tata kelola TI digunakan dalam penelitian sebagai dasar dalam penyusunan rancangan kebijakan dan prosedur pengelolaan data, dengan harapan dapat menghasilkan kebijakan dan prosedur yang komprehensif dan memberikan manfaat pengelolaan keamanan informasi bagi organisasi yang menerapkan keduanya.

Metode yang digunakan dalam penelitian ini adalah observasi, kuisioner dan wawancara berdasarkan COBIT 4.1 dan SNI ISO/IEC 27001:2009. Selain itu, digunakan metode Delphi untuk validasi rancangan kebijakan dan prosedur. Berdasarkan hasil penilaian dan analisis risiko, dipilih kontrol-kontrol yang dapat diterapkan untuk meningkatkan keamanan informasi. Kontrol-kontrol tersebut dimasukkan dalam rancangan kebijakan dan prosedur keamanan informasi. Berdasarkan hasil kuisioner dan wawancara, dilakukan identifikasi dan analisis hasil pengukuran kematangan, analisis kesenjangan tingkat kinerja dan tingkat kematangan, analisis hasil penilaian risiko, identifikasi dan analisis dampak, identifikasi dan analisis kelemahan kontrol. Berdasarkan COBIT 4.1 dipilih proses-proses yang menghasilkan masukan (input) dalam proses pengelolaan data dan memastikan keamanan sistem sebagai aktivitas dan proses dalam rancangan kebijakan dan prosedur pengelolaan data.

Hasil pengukuran kinerja berdasarkan COBIT 4.1 menunjukkan bahwa kinerja DS5 dann DS11 masih kurang. Sedangkan hasil pengukuran kematangan menunjukkan proses pengelolaan data dan memastikan keamanan sistem berada pada tingkat 2 (dua), dengan harapan tingkat kematangan berada pada tingkat 4 (empat). Berdasar hasil penilaian kematangan disusun rekomendasi tindakan perbaikan untuk peningkatan kematangan, antara lain penyusunan kebijakan dan prosedur pengelolaan data dengan memperhatikan aspek keamanan sistem serta tim/kelompok kerja yang bertugas mengevaluasi dan mengawasi pelaksanaan kebijakan dan prosedur. Pengendalian dalam kebijakan dan prosedur keamanan informasi sesuai dengan ISO/IEC 27001:2005 meliputi pengendalian: organisasi keamanan informasi,pengelolaan aset informasi, keamanan SDM, keamanan fisik dan lingkungan, pengelolaan komunikasi dan operasional, pengaturan akses, keamanan informasi dalam pengadaan dan pemeliharaan sistem informasi, pengelolaan gangguan keamanan informasi, keamanan informasi dalam pengelolaan kealngsungan kegiatan, dan kepatuhan.

Dalam rancangan kebijakan dan prosedur pengelolaan data dengan memperhatikan aspek keamanan informasi, COBIT 4.1 digunakan sebagai payung kebijakan tata kelola TI khususnya pada pengelolaan data; sedangkan dan ISO/IEC 27001:2005 digunakan sebagai acuan dalam penyusunan kebijakan keamanan informasi. Keduanya saling melengkapi menghasilkan kebijakan dan prosedur yang komprehensif mencakup people, process, dan technology untuk mencapai kerahasiaan, ketersediaan, dan integritas informasi. Kerahasiaan, ketersediaan, dan integritas data dan informasi dicapai melalui aktivitas dan proses serta kontrol yang sesuai untuk diterapkan.
.....Certification in Directorate XYZ as one of the main activities of the Directorate XYZ can't be separated from the role of IS / IT to support optimal certification services, which in turn can provide excellent service in certification. In order to provide excellent service certification, that is required a high-quality data, which can meet the criteria, reliability, integrity, and availability.

COBIT 4.1 and ISO / IEC 27001:2009 is an IT governance framework and information security standards that are best practices. Combine both in policy making IT governance is used in this research as a basis for drafting policies and procedures of data management, with the hope of producing a comprehensive policy and procedures and provide the benefits of information security management for organizations that implement them. The method used in this study is the observation, questionnaires and interviews based on COBIT 4.1 and ISO / IEC 27001:2009. In addition, the Delphi method was used to validate the design of policies and procedures. Based on the results of risk assessment and analysis, controls that can be applied to improve information security are selected. The controls are incorporated in the draft of information security policies and procedures. Based on the results of questionnaires and interviews, to identify and analyze the results of the measurement of maturity, gap analysis and the maturity level of performance, analysis of the results of risk assessment, identification and impact analysis, identification and analysis of control weaknesses. This selection is based on COBIT 4.1 processes that produce inputs to the data management process and ensure the security of the system as activities and processes in the design of data management policies and procedures.

The results of performance measurements based on COBIT 4.1 shows that the performance of DS5 and DS11 is still lacking. While the results of measurements show the maturity of data management and ensure the security of the system is at the level of 2 (two), in the hope of maturity level is at level 4 (four). Based on maturity assessments prepared recommendations for the improvement of the maturity of remedial actions, including design of policies and procedures for data management by taking into account the security aspects of the system and the team / work group charged with evaluating and overseeing the implementation of policies and procedures. Control the information security policies and procedures in accordance with ISO/IEC 27001:2005 covers control: the organization of information security, asset management information, human resources security, physical and environmental security, communications and operations management, access arrangements, the security of information in the procurement and maintenance of information systems, management of information security threats, business continuity management, and compliance.

In the design of policies and procedures with respect to data management aspects of information security,

COBIT 4.1 is used as a reference policy governance of IT especially in data management; while and ISO / IEC 27001:2005 is used as a reference for information security policy. Both complement each other producing a comprehensive policy and procedures covering people, process, and technology to achieve confidentiality, availability, and integrity of information. Confidentiality, availability and integrity of data and information are achieved through the activities and processes and controls that are appropriate to be applied.