ABSTRACT

The government as users of information technology today must always be ready to face various types of information security incidents. The continuity of business processes must be maintained from all the impacts caused by the incident. However, there are still many problems encountered in handling information security incidents. In terms of human resources, technology, as well as from the policy and procedural side, it has not focused on the aspects of information security incidents. Therefore we need an incident management system as a systematic solution to ensure the continuity of information services and IT systems.

The method used in this research is a qualitative method through case studies. Data were analyzed through the stages of identification, analysis of existing conditions, and determination of the objectives of the policies and procedures to be designed. Document preparation is carried out by referring to the assessment result approach between the current (existing) condition of the business process and the information security incident management that has been carried out with the clauses required by ISO / IEC 27035.

The results of this study are in the form of policy documents and information security incident management procedures that are adjusted to ISO / IEC 27035, the formation of an incident response team, and an incident recording form. Based on the results of verification and testing, the results show that the documents compiled can be implemented, but it still takes time for them to be fully implemented. It is also necessary to develop specific technical procedures for each type of incident in order to improve the performance of the response team in handling incidents.

Keywords: incidents, information security, ISO/IEC 27035, management

INTISARI

Pemerintah sebagai pengguna teknologi informasi saat ini harus selalu siap menghadapi berbagai macam jenis insiden kemanan informasi. Keberlangsungan proses bisnis harus tetap terjaga dari segala dampak yang diakibatkan oleh terjadinya insiden. Namun masih banyak ditemukan permasalahan dalam penanganan insiden keamanan informasi yang dihadapi. Dari sisi sumber daya manusia, teknologi, maupun dari sisi kebijakan dan prosedural belum fokus pada aspek insiden keamanan informasi. Oleh karena itu diperlukan suatu sistem manajemen insiden sebagai salah satu solusi sistematis untuk menjamin keberlangsungan layanan informasi dan sistem TI.

Metode yang digunakan dalam penelitian ini adalah metode kualitatif melalui studi kasus. Data dianalisis melalui tahapan indentifikasi, analisis terhadap kondisi yang ada, serta penentuan tujuan kebijakan dan prosedur yang akan dirancang. Penyusunan dokumen dilakukan mengacu pada pendekatan hasil assesmen antara kondisi saat ini dari proses bisnis dan manajemen insiden keamanan informasi yang telah dilakukan dengan klausul yang dipersyaratkan oleh ISO/IEC 27035.

Hasil dari penelitian ini berupa dokumen kebijakan dan prosedur maanajemen insiden keamanan informasi yang disesuaikan dengan ISO/IEC 27035, pembentukan tim respon insiden, serta formulir pencatatan insiden. Berdasarkan hasil verifikasi dan pengujian didapatkan hasil bahwa dokumen yang disusun dapat diimplementasikan, namun masih membutuhkan waktu agar dapat diimplementasikan secara menyeluruh. Dibutuhkan juga penyusunan prosedur teknis spesifik dari masing-masing jenis insiden agar dapat meningkatkan kinerja tim respon dalam menangani insiden.

Kata kunci – insiden, keamanan informasi, ISO 27001, manajemen