ABSTRAK

Manajemen insiden keamanan informasi merupakan salah satu aspek krusial dalam menjaga keberlangsungan operasional dan perlindungan aset informasi suatu organisasi, khususnya pada instansi pemerintah yang mengelola data strategis. Penelitian ini bertujuan untuk menganalisis tingkat kematangan manajemen insiden keamanan informasi pada Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta dengan mengacu pada standar ISO/IEC 27002:2022.

Metode yang digunakan dalam penelitian ini melibatkan pendekatan deskriptif kualitatif dengan teknik pengumpulan data melalui wawancara, observasi, dan studi dokumentasi. Penilaian kematangan dilakukan dengan memetakan kondisi eksisting terhadap kontrol dan panduan praktik terbaik yang tercantum dalam ISO/IEC 27002:2022, khususnya pada domain pengelolaan insiden keamanan informasi. Kemudian dilakukan perhitungan nilai kematangan berdasarkan SSE-CMM.

Hasil penelitian menunjukkan bahwa tingkat kematangan manajemen insiden keamanan informasi di instansi tersebut berada pada level 4 atau Manage and Measurable, yang berarti bahwa prosedur penanganan insiden telah terdokumentasi namun masih memerlukan peningkatan pada aspek monitoring berkelanjutan dan evaluasi pasca insiden. Rekomendasi perbaikan disusun berdasarkan kesenjangan antara kondisi saat ini dan praktik ideal menurut ISO/IEC 27002:2022, sehingga diharapkan dapat mendukung peningkatan efektivitas manajemen insiden di masa mendatang.

Kata kunci : Manajemen Insiden, Keamanan Informasi, ISO/IEC 27002:2022, Dinas Komunikasi dan Informatika DIY, SSE-CMM

ABSTRACT

Information security incident management is one of the crucial aspects in maintaining the operational continuity and protection of an organization's information assets, especially in government agencies that manage strategic data. This study aims to analyze the maturity level of information security incident management at the Yogyakarta Special Region Communication and Information Service by referring to the ISO/IEC 27002:2022 standard.

The method used in this study involves a qualitative descriptive approach with data collection techniques through interviews, observations, and documentation studies. The maturity assessment is carried out by mapping existing conditions against the controls and best practice guidelines listed in ISO/IEC 27002:2022, especially in the domain of information security incident management. Then the maturity value is calculated based on SSE-CMM.

The results of the study indicate that the maturity level of information security incident management in the agency is at level 4 or Manage and Measurable, which means that the incident handling procedure has been documented but still requires improvement in the aspects of continuous monitoring and post-incident evaluation. Recommendations for improvement are prepared based on the gap between current conditions and ideal practices according to ISO/IEC 27002:2022, so that it is expected to support increasing the effectiveness of incident management in the future.

Keyword : Incident Management, Information Security, ISO/IEC 27002:2022, DIY Communication and Informatics Department, SSE- CMM