# ABSTRAK

Sistem pemerintahan sekarang sudah mengimplementasikan elektronik pada proses nya atau biasa disebut Sistem Pemerintahan Berbasis Elektronik (SPBE), dengan SPBE ini membuat aset rahasia/sensitif yang disimpan di sistem elektronik tersebut sangat rentan untuk dilakukan penyerangan menurut data dari laporan BSSN tahun 2022 sektor administrasi pemerintahan adalah bidang paling banyak serangan dan aduan siber. Hal tersebut membuat aset harus dijaga dengan baik, instansi XYZ memiliki tugas berfokus untuk merancang dan menjalankan SPBE maka instansi XYZ memerlukan sistem manajemen keamanan informasi (SMKI) yang baik agar aset tetap aman. Penelitian ini bertujuan untuk meningkatkan SMKI dengan cara kualitatif yaitu mewawancarai dan observasi pihak terkait dan menentukan tingkat kematangan SMKI yang standar SNI ISO/IEC 27001:2022 menggunakan *maturity level* COBIT 2019 kemudian dilakukan analisa untuk memberikan rekomendasi perbaikan berdasarkan SNI ISO/IEC 27002:2022 sebagai referensi pengendalian keamanan pada SMKI SNI ISO/IEC 27001:2022. Hasil dari penelitian ini ditemukan bahwa tingkat kematangan SMKI instansi XYZ yaitu tingkat 2 kematangan COBIT 2019, dimana pada saat ini kontrol keamanan sudah berhasil mencapai tujuan melalui kegiatan dasar, namun detail, yang dapat disebut sebagai suatu hasil kerja tetapi masih belum ada dokumentasi terkait penerapan terhadap aset organisasi dan ditemukan ada satu kontrol tidak terpenuhi terkait *web filtering*. Tingkat kematangan yang diharapkan pimpinan instansi XYZ yaitu tingkat 4, dimana hasil implementasi pada aset dilakukan audit diukur implementasinya apakah sudah sesuai prosedur. Dari kesenjangan tingkat kematangan tersebut penelitian ini memberikan rekomendasi yaitu pembuatan dokumentasi penerapan prosedur pada aset yang mengacu pada SNI ISO/IEC 27002:2022 kemudian dilakukan audit penerapannya.

**Kata Kunci**: Keamanan Informasi, ISO 27001, ISO 27002, Tingkat Kematangan, SPBE, SMKI, COBIT.