Abstrak

Di era teknologi informasi, masyarakat semakin mendambakan pelayanan pemerintahan yang cepat dan tidak terbatas jarak, ruang, dan waktu. Untuk itu, pemerintah menjawab kebutuhan tersebut dengan mengimplementasikan Sistem Pemerintahan Berbasis Elektronik (SPBE).SIPP merupakan salah satu pelayanan yang pengadilan berikan sebagai pemberi pelayanan pada masyarakat. Dalam pemberian layanan yang baik diperlukannya integrasi antar informasi yang baik pula agar pelayanan yang diberikan cepat dan tepat . selain sebagai layanan pemberi informasi SIPP juga berfungsi sebagai salah satu alat yang digunakan Mahkamah Agung Republik Indonesia dalam mengawasi kinerja pengadilan di seluruh pelosok Indonesia. Dalam *Road Map* 2015 Mahkamah Agung tahun SIPP merupakan bagian dari salah satu program *Quick Win* Mahkamah Agung yang telah disesuaikan dengan Cetak Biru Mahkamah Agung tahun 2010-2035 yaitu pada program Pengembangan Teknologi Informasi .

Pada tahun 2020 Pengadilan mengalami banyak masalah dalam bidang keamanan informasi terutama pada *website* pengadilan di seluruh Indonesia termasuk SIPP. Terdapat lebih dari 20 pengadilan yang mengalami serangan *hacker* berdasarkan data dari sumber internal pengadilan, kerusakan yang dialami yaitu baik pada *website*, fitur *web* SIPP maupun fitur perpustakaan pengadilan.

Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 pasal 7, setiap penyelenggara SPBE harus menerapkan keamanan informasi mengikuti standar keamanan informasi yang dijelaskan oleh Kementerian Komunikasi dan Informasi. Karena peraturan ini disusun untuk meminimalkan risiko pelanggaran keamanan pada SPBE, dan terdapat banyak pelanggaran keamanan pada tahun 2020, oleh karena itu ini menunjukkan penerapan peraturan yang buruk. Maka perlu dilakukannya asesmen keamanan informasi pada SIPP di pengadilan untuk menyelidiki area mana yang diabaikan. Dalam mencapai hal tersebut, penelitian ini menggunakan analisis kesenjangan menggunakan ISO/IEC 27001 dan tingkat kematangan untuk mengungkapkan area yang diabaikan dalam keamanan informasi.

Dalam Penelitian ini Metode yang digunakan adalah metode kualitatif, pengumpulan data dan validasi data dengan teknik triangulasi yaitu melalui wawancara, observasi, dan dokumentasi. *Gap analysis* di gunakan dalam analisis data dan untuk mengukur tingkat kematangan menggunakan CMMI(*Capability Maturity Model for Integration*).

Hasil penelitian menunjukkan dari sepuluh annex yang di uji tingkat keamanan informasi SIPP di Pengadilan berada pada level 3 (*Defined*) yang berarti Pengadilan mengetahui adanya permasalahan yang harus diatasi, terdapat beberapa proses yang belum ter standarisasi dan di dokumentasi serta lebih menangani masalah per kasus yang ada saja.

Kata kunci : ISO 27001, asesmen , keamanan informasi, CMMI , SIPP