

Bab I Pendahuluan

I.1 Latar Belakang

Pemerintah Indonesia mencanangkan penyelenggaraan pemerintahan berbasis teknologi informasi dan komunikasi. Hal ini tertuang pada Peraturan Presiden No. 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Sistem pemerintahan berbasis elektronik diselenggarakan dengan prinsip efektivitas, keterpaduan, kesinambungan, efisiensi, akuntabilitas, interoperabilitas, dan keamanan. Prinsip-prinsip tersebut menjadi pedoman bagi pihak-pihak yang terlibat dalam penyelenggaraan SPBE. SPBE perlu diselenggarakan baik oleh Instansi Pusat maupun Pemerintah Daerah sesuai dengan koordinasi yang diberikan oleh Tim Koordinasi SPBE Nasional. Termasuk di dalamnya, Pemerintah Kabupaten Bandung Barat. Pemerintah Kabupaten Bandung Barat memiliki Dinas Komunikasi, Informatika, dan Statistik (Diskominfotik) sebagai koordinator dan pelaksana teknis SPBE.

Dalam Perpres No. 95 tahun 2018 tercantum ketentuan mengenai keamanan informasi SPBE. Ketentuan ini menerangkan bahwa adanya keperluan untuk melaksanakan manajemen keamanan informasi demi menjamin keberlangsungan SPBE dengan cara meminimalkan risiko-risiko berkenaan dengan keamanan informasi. Terdapat kebijakan keamanan informasi yang sudah menjelaskan lebih lanjut, bagaimana seharusnya keamanan informasi dikelola. Kebijakan tersebut adalah Peraturan Menteri Komunikasi dan Informatika No. 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Dalam peraturan ini, disebutkan bahwa terdapat dua jenis pedoman yang dapat digunakan untuk melakukan pengamanan informasi yaitu standar SNI ISO/IEC 27001 atau kerangka kerja Indeks Keamanan Informasi (KAMI) yang disusun oleh Badan Siber dan Sandi Negara.

Peraturan perundang-undangan yang mengatur tentang keamanan informasi telah dibuat untuk menghadapi perkembangan tren ancaman dalam keamanan informasi. Sebagaimana survei yang dilakukan oleh *European Union Agency for Network and Information Security* (ENISA) (dikutip melalui ISACA, 2017) yang menunjukkan tentang tentang 15 ancaman terbanyak yang terjadi pada bidang keamanan informasi. Ancaman-ancaman tersebut berurutan dari jumlah tertinggi

berupa *malware*, serangan berbasis web, serangan aplikasi web, *botnets*, *denial of service*, serangan fisik atau kehilangan, ancaman dari dalam, *phising*, *spam*, *exploit kits*, pelanggaran hak akses data, pencurian identitas, kebocoran informasi, *ransomware*, dan spionase.

Dampak yang mungkin muncul ketika terjadi ancaman terhadap keamanan informasi dapat berupa hilangnya data, pengaksesan sistem dan informasi oleh pihak yang tidak berwenang, pengambilan data dan informasi oleh pihak yang tidak berwenang, berhentinya sistem aplikasi dan tidak dapat memberikan layanan yang semestinya, atau bahkan kerusakan pada infrastruktur yang digunakan untuk menjalankan sistem aplikasi. Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat sendiri sudah mengalami beberapa risiko seperti yang sudah disebutkan sebelumnya. Timmy Sampurna Irawan, Kepala Seksi Manajemen Data dan Pengembangan Aplikasi, menyatakan bahwa risiko keamanan informasi yang sudah pernah terjadi pada Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat adalah serangan berbasis web, *denial of service*, dan *malware*.

Untuk membantu Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat dalam menghadapi regulasi yang perlu dipatuhi terutama dalam bidang pengelolaan keamanan informasi serta untuk mengetahui dan meminimalkan risiko-risiko keamanan informasi yang ada pada dinas tersebut, lingkup dari penelitian ini adalah penggunaan standar ISO 27001:2013 untuk melakukan penilaian dan perancangan rekomendasi mengenai pengelolaan keamanan informasi SPBE Pemerintah Kabupaten Bandung Barat yang penyelenggaraannya dilakukan oleh Dinas Komunikasi, Informatika, dan Statistik.

Hasil dari penelitian ini adalah rancangan untuk meningkatkan kualitas tata kelola keamanan informasi. Rancangan sistem manajemen keamanan informasi tersebut dapat digunakan oleh Pemerintah Kabupaten Bandung Barat terkhusus Dinas Komunikasi, Informatika, dan Statistik sebagai referensi dalam mengelola keamanan informasi SPBE Pemerintah Kabupaten Bandung Barat, demi mengikuti peraturan perundang-undangan yang berlaku serta meminimalkan risiko keamanan informasi yang dapat mengganggu berjalannya SPBE.

I.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah yang diangkat pada penelitian ini adalah:

- a. Bagaimana risiko dan penanganan risiko keamanan informasi dari SPBE milik Pemerintah Kabupaten Bandung Barat yang dikelola oleh Dinas Komunikasi, Informatika, dan Statistik?
- b. Bagaimana estimasi pengaruh rekomendasi dalam meningkatkan kualitas tata kelola keamanan informasi jika rekomendasi diimplementasikan pada SPBE Kabupaten Bandung Barat yang dikelola oleh Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat?

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

- a. Mengidentifikasi dan meminimalkan risiko-risiko terkait keamanan informasi yang ada pada SPBE yang dikelola Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat.
- b. Mengetahui estimasi pengaruh rekomendasi dalam meningkatkan kualitas tata kelola keamanan informasi dalam mengelola SPBE Pemerintah Kabupaten Bandung Barat apabila rekomendasi diimplementasikan oleh Dinas Komunikasi, Informatika, dan Statistik.

I.4 Manfaat Penelitian

I.4.1 Manfaat bagi Instansi

Manfaat dari penelitian ini bagi instansi adalah:

- a. Tertanganinya sebagian risiko-risiko terkait keamanan informasi karena adanya rekomendasi mengenai pengelolaan keamanan informasi dalam penyelenggaraan SPBE milik Pemerintah Kabupaten Bandung Barat.
- b. Meningkatkan kualitas tata kelola keamanan informasi Kabupaten Bandung Barat dalam menyelenggarakan SPBE terutama dalam hal kebijakan, prosedur, dan pembagian tugas pokok dan fungsi berkenaan dengan pengelolaan keamanan informasi.

I.4.2 Manfaat bagi Akademik

Manfaat dari penelitian ini bagi akademik adalah membantu perkembangan ilmu pengetahuan dengan menjadi referensi penelitian berikutnya terutama dalam bidang keilmuan sistem informasi untuk menyusun tata kelola keamanan informasi bagi Sistem Pemerintahan Berbasis Elektronik.

I.5 Ruang Lingkup

Ruang lingkup dalam penelitian ini adalah:

1. *Assessment* tata kelola keamanan informasi serta rekomendasi untuk meningkatkan kualitas tata kelola keamanan informasi tersebut.
2. Alat yang digunakan untuk melakukan *assessment* dan acuan dalam memberikan rekomendasi adalah klausa-klausa yang terdapat pada SNI/ISO 27001:2013 bagian Kontrol Annex. Klausa PDCA (*Plan – Do – Check – Act*) bukan merupakan bagian dari penelitian ini.
3. Penyusunan rekomendasi dilakukan berdasarkan analisis risiko. Risiko yang digunakan pada penelitian ini adalah risiko negatif. Hal tersebut dilakukan karena penggunaan SNI/ISO 27001:2013 lebih berfokus pada ancaman (*Threat*) dibandingkan kesempatan (*Opportunities*).
4. Penelitian ini menggunakan obyek penelitian berupa Sistem Pemerintahan Berbasis Elektronik yang dimiliki oleh Pemerintah Kabupaten Bandung Barat dalam pengelolaan Dinas Komunikasi, Informatika, dan Statistik.
5. Hasil akhir dari penelitian ini adalah rekomendasi berupa rancangan kebijakan, rancangan teknologi, dan rancangan posisi, tugas, dan fungsi pegawai yang berkaitan dengan pengelolaan keamanan informasi.