

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Utilisasi sistem informasi dalam membantu operasi bisnis merupakan hal yang umum dilakukan di organisasi atau perusahaan. Salah satu bentuk penggunaan sistem informasi yang digunakan di organisasi atau perusahaan adalah sistem absensi digital. Tidak terkecuali Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat, yang juga ikut memanfaatkan kemajuan sistem informasi dengan menerapkan sistem absensi digital melalui aplikasi Sistem Monitoring Aparatur Sipil Negara *Realtime* (SMART), yang dirilis pada tahun 2020 lalu. Aplikasi SMART memiliki fungsi utama sebagai alat absensi digital yang beroperasi dengan mengumpulkan dan memproses informasi data pribadi pegawainya. Data pribadi yang dikumpulkan mencakup data pribadi bersifat umum seperti nama dan Nomor Induk Pegawai (NIP), lokasi serta data pribadi bersifat sensitif yakni foto wajah. Kehadiran aplikasi SMART absensi ini mempermudah Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat dalam memproses absensi dan melakukan evaluasi kinerja pegawainya.

Namun, disamping kemudahan yang ditawarkan, utilisasi sistem informasi tanpa adanya penerapan kontrol keamanan yang tepat, hanya akan membuat organisasi atau perusahaan tersebut menjadi rentan terhadap kejahatan siber (Hamdi, Norman, Molok, & Hassandoust, 2019). Kebocoran data, manipulasi absensi dan penghapusan data merupakan salah satu kerentanan yang terdapat pada suatu sistem yang tidak terlindungi dengan sempurna. Pada pertengahan tahun 2024 terdapat kasus kebocoran data pribadi yang disebabkan oleh *ransomware* pada Pusat Data

Nasional Sementara (PDNS), hal ini menyebabkan terhambatnya beberapa fasilitas umum, salah satunya imigrasi dikarenakan rusaknya fasilitas validasi warga yang bermigrasi (Intan, 2024). Berdasarkan dari dokumen Lanskap Keamanan Siber Indonesia, pada tahun 2023 terdapat sebanyak 403.990.813 trafik anomali yang tercatat, salah satu dampak aktivitas anomali adalah bertujuan untuk melakukan pencurian data sensitif (Direktorat Operasi Keamanan Siber, 2023).

Secara umum keamanan merupakan salah satu faktor penting yang perlu diperhatikan untuk mengetahui kualitas suatu sistem informasi (Putra, 2020). Oleh karena itu penting bagi sistem ini untuk memiliki mekanisme keamanan sistem informasi. Dalam sistem absensi digital seperti aplikasi SMART absensi, kerentanan dapat berupa kebocoran data, manipulasi absensi dan penghapusan data. Dimana hal-hal tersebut dapat menyebabkan kerugian bagi organisasi dan juga pegawainya, tidak hanya dari sisi biaya namun juga reputasi (Safa, Solms, & Futcher, 2016).

Peraturan Bupati Bandung Barat Nomor 8 Tahun 2023, menjelaskan bahwa aplikasi SMART absensi digunakan sebagai alat absensi elektronik yang juga digunakan sebagai alat untuk mengukur kinerja pegawai Aparatur Sipil Negara (ASN) (Pemerintah Kabupaten Bandung Barat, 2023). Mengutip dari peraturan tersebut, memberikan kesimpulan bahwa aplikasi SMART absensi ini merupakan salah satu aplikasi utama yang digunakan sehari-hari oleh pegawai Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat. Berdasarkan dari dokumen *Roadmap* Persandian dan Keamanan Informasi Pemerintah Daerah Kabupaten Bandung Barat, pada tahun 2024 Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat seharusnya sudah merancang dan memiliki dokumen kebijakan dan pedoman persandian dan keamanan informasi. Namun, sampai tesis ini dibuat, keamanan informasi yang diterapkan di aplikasi SMART

belum secara menyeluruh dibangun ataupun memiliki dokumen lengkap berdasarkan standar atau *best practice* yang menjadi rujukan penerapan keamanan informasi. Lebih lanjut, Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik mewajibkan Penyelenggara Sistem Elektronik untuk menerapkan SNI ISO/IEC 27001 (Badan Siber dan Sandi Negara, 2020). Hal ini berarti bahwa sudah seharusnya aplikasi SMART absensi dibangun berdasarkan ISO/IEC 27001.

Sejalan dengan peraturan tersebut, standar ISO/IEC 27001 dinilai cocok untuk digunakan sebagai dasar pengukuran keamanan informasi aplikasi SMART absensi, karena standar ini menyediakan spesifikasi dan/atau *best practice* yang dapat digunakan untuk mengelola keamanan informasi (Aminzade, 2018). ISO/IEC 27001 menerapkan kontrol-kontrol keamanan informasinya melalui kerangka kerja Sistem Manajemen Keamanan Informasi (SMKI), yang secara menyeluruh menjaga tiga pilar keamanan informasi yakni, kerahasiaan, integritas dan ketersediaan informasi (CIA) melalui penerapan proses manajemen risiko (Velasco, et al., 2018) (ISO/IEC, 2022). Standar ISO/IEC 27001, juga membantu untuk secara efektif mengembangkan dan memelihara prosedur, kontrol dan proses yang dirancang untuk melindungi keamanan informasi, dari pengaksesan, pengungkapan, modifikasi, penggunaan dan perusakan yang tidak sah (Gillies, 2011) (Fajar, Christian, & Girsang, 2018) (Hamdi, Norman, Molok, & Hassandoust, 2019). Standar ISO/IEC yang digunakan dalam tesis ini adalah ISO/IEC 27001 versi 2022, dari empat *annex* yang ada pada ISO/IEC 27001:2022 kontrol A.6 *People controls* dan A.7 *Physical controls* tidak digunakan karena tesis ini berfokus pada evaluasi keamanan pengembangan dan operasional aplikasi SMART absensi. Untuk mengevaluasi aplikasi SMART absensi *annex* yang digunakan adalah A.5

*Organizational controls* dan A.8 *Technological controls* dengan jumlah kontrol keamanan yang digunakan sebanyak 69 kontrol yang terbagi pada A.5 *Organizational controls* sebanyak 36 kontrol, terdapat satu kontrol yang tidak digunakan yakni 5.23 *Information security for use of cloud services* karena aplikasi SMART absensi tidak menggunakan layanan *cloud*. Sementara terdapat 34 kontrol dari A.8 *Technological controls*, dan terdapat satu kontrol yang tidak digunakan yakni 8.30 *Outsourced development* karena aplikasi SMART absensi dikelola dan dibangun oleh pegawai internal.

Peningkatan keamanan informasi diinisiasikan dalam tesis ini, khususnya untuk pengembangan dan operasional aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat. Dengan mengacu pada standar ISO/IEC 27001 versi tahun 2022, penerapan keamanan informasi aplikasi SMART absensi akan dinilai dengan menggunakan nilai *maturity level* yang mengadopsi tingkat kematangan dari *Capability Maturity Model Integration* (CMMI) yakni, Level 0 *Nonexistent*, Level 1 *Initial*, Level 2 *Repeatable*, Level 3 *Defined*, Level 4 *Managed*, dan Level 5 *Optimized*. Penilaian tingkat kematangan ini memiliki tujuan untuk mengevaluasi dan memetakan tingkat keamanan informasi yang diterapkan di aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat. Setelah melakukan evaluasi, rekomendasi perbaikan pengelolaan keamanan informasi akan dirancang berdasarkan tingkat dan/atau susunan organisasi, sesuai dengan kebutuhan Sistem Manajemen Keamanan Informasi (SMKI) aplikasi SMART absensi berdasarkan standar ISO/IEC 27001:2022.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang yang sudah dijabarkan sebelumnya, maka rumusan masalah yang dirumuskan dalam tesis ini adalah:

1. Bagaimana menentukan kontrol keamanan berdasarkan ISO/IEC 27001:2022 yang efektif diterapkan untuk aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat
2. Bagaimana tingkat kematangan keamanan aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat
3. Apa saja rekomendasi dan saran terhadap keamanan aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat berdasarkan ISO/IEC 27001:2022

### **1.3 Tujuan Penelitian**

Penelitian ini bertujuan untuk membantu Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat dalam meninjau kondisi keamanan sistem informasi aplikasi SMART absensi berdasarkan standard ISO/IEC 27001:2022. Kebutuhan bagi pegawai Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat untuk dapat menggunakan aplikasi SMART absensi secara aman memberikan tujuan bagi tesis ini yaitu:

1. Menentukan kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022 yang efektif untuk diterapkan di aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat.
2. Menentukan tingkat kematangan keamanan aplikasi SMART absensi berdasarkan *Capability Maturity Model Integration (CMMI)*
3. Memberikan rekomendasi perubahan dan/atau perbaikan Sistem Manajemen Keamanan Informasi (SMKI) yang disesuaikan dengan kebutuhan aplikasi SMART absensi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat.

#### **1.4 Manfaat Penelitian**

Penelitian yang dilakukan diharapkan memberikan beberapa manfaat bagi Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat untuk dapat memiliki aplikasi absensi yang lebih aman dan dapat diandalkan, selain itu akan membaca hasil penelitian ini. Berikut adalah beberapa manfaat yang dapat digunakan dari hasil penelitian ini:

1. Mengetahui tata cara melakukan penilaian tingkat kematangan dengan menggunakan *Capability Maturity Model Integration (CMMI)* untuk ISO/IEC 27001:2022.
2. Mengetahui dan memahami cara meningkatkan keamanan sistem informasi dengan menggunakan ISO/IEC 27001:2022 untuk aplikasi absensi.
3. Memberikan hasil berupa laporan penilaian tingkat kematangan dan rekomendasi sesuai dengan susunan organisasi dan tanggung jawabnya terhadap aplikasi SMART absensi di Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat.

#### **1.5 Batasan Masalah**

Berikut ini adalah beberapa batasan masalah yang dibahas di dalam penelitian ini:

1. Penelitian dibatasi pada masalah keamanan sistem informasi yang relevan terhadap aplikasi SMART absensi.
2. Sistem informasi yang diteliti merupakan sistem informasi yang digunakan bagi aplikasi absensi pegawai di Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat.
3. Standar yang menjadi rujukan penilaian tingkat kematangan adalah ISO/IEC 27001:2022.

4. Tingkat kematangan yang digunakan merujuk kepada tingkat kematangan yang didefinisikan oleh *Capability Maturity Model Integration (CMMI)*.
5. Penelitian dilakukan dengan berdasarkan sumber data yang diperoleh melalui wawancara dan kuesioner terhadap *User Aplikasi*, *Pengelola Aplikasi*, dan *Pihak Manajerial*. Serta peninjauan dokumen yang berkaitan dengan pengembangan, penggunaan, peraturan dasar aplikasi SMART absensi.
6. Proses *self-assessment* yang berperan sebagai *internal auditor* dengan tujuan untuk memberikan fleksibilitas kepada pegawai Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat dan tidak menimbulkan disrupti di lingkungan tersebut.

## 1.6 Sistematika Penulisan

Sistematika penulisan akan diuraikan menjadi lima bab, yaitu:

**Bab I Pendahuluan:** bab ini berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

**Bab II Kajian Pustaka:** bab ini secara umum berisikan uraian dari berbagai teori yang menjadi penunjang bagi penelitian ini. Dalam bab ini juga berisikan mengenai penelitian terdahulu yang memiliki kesamaan topik agar dapat menentukan fokus penelitian dan memberikan hasil penelitian yang berbeda. Beberapa teori yang dibahas pada bab ini antara lain, sistem informasi, keamanan informasi, perlindungan privasi, sistem manajemen keamanan informasi (SMKI), ISO/IEC 27001:2022 dan ISO/IEC 27002:2022, *maturity level* dan membuat kajian terhadap penelitian sebelumnya yang relevan dengan topik penelitian ini.

**Bab III Metodologi Penelitian:** bab ini berisi terkait persiapan penelitian

dengan menjelaskan objek penelitian, alasan penelitian dan ruang lingkup yang diteliti. Selain itu pada bab ini dijelaskan juga pemilihan kontrol dan/atau persyaratan keamanan yang didefinisikan oleh ISO/IEC 27001:2022.

**Bab IV Hasil Penelitian dan Pembahasan:** bab ini berisi analisa terhadap nilai kematangan aplikasi SMART absensi, dan rekomendasi strategi peningkatan keamanan sistem informasi.

**Bab V Kesimpulan:** bab ini berisi kesimpulan dari hasil penelitian yang diperoleh dari penelitian ini dan saran bagi penelitian selanjutnya.

**Daftar Pustaka:** pada bagian ini berupa daftar dari seluruh sumber kepustakaan yang digunakan dalam penelitian. Penulisan daftar pustaka merujuk kepada kaidah yang berlaku dan/atau ditentukan dalam tata naskah di lingkungan Universitas Komputer Indonesia.