# EVALUASI KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI KOTA XYZ

**I Gede Putu Krisna Juliharta[1)] I Putu Cikal Taruna[2)] Tiawan[3)]**
Program Studi Sistem Informasi [1)2)3)]
Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Primakara, Denpasar, Bali[1) 2) 3)]
krisna@primakara.ac.id[1)] cikaltaruna@gmail.com[2)] tiawan@primakara.ac.id[3)]

***ABSTRACT***

*The Electronic-Based Government System (SPBE) is a form of E-Government implementation in Indonesia which is expected to be able to harmonize information technology and government administration. XYZ City as an area that has implemented SPBE, has evaluated the SPBE in 2021. Based on this evaluation, XYZ City Government received a score of 3.19 (good). However, if we look at the details of the audit results, SPBE Management Domain gets the lowest score. This domain has a key role, because in that domain there are indicators related to information security which should have a high value because it is related to information security in the regions that administer the SPBE.*

*This study evaluates or re-audits the implementation of SPBE in the XYZ City Government, especially in the implementation of information security. The evaluation method is carried out using the Information Security Management System (ISMS) standard through the Indeks KAMI combined with COBIT 5 APO13 Manage Security to obtain the maturity level of information security. Based on the reassessment, it was found that the SPBE of the XYZ City Government was at a value of 3.17 (good), with the maturity level value being at level 1 (stub).*

***Keywords****: E-Government, SPBE, Audit, Information Security, ISMS, Indeks KAMI, COBIT 5 APO13.*

**ABSTRAK**

Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah bentuk penyelenggaraan *E-Government* di Indonesia yang diharapkan mampu menyelaraskan teknologi informasi dan penyelenggaraan pemerintahan. Kota XYZ sebagai daerah yang telah menerapkan SPBE, telah melakukan evaluasi terhadap SPBE pada tahun 2021. Berdasarkan evaluasi tersebut, Pemerintah Kota XYZ mendapatkan nilai 3,19 (baik). Namun, jika melihat secara rinci mengenai hasil audit tersebut, Domain Manajemen SPBE mendapat nilai terendah. Domain ini memiliki peran kunci, karena pada domain tersebut terdapat indikator-indikator terkait dengan keamanan informasi yang seharusnya memiliki nilai tinggi karena terkait dengan keamanan informasi pada daerah yang penyelenggara SPBE. Penelitian ini melakukan evaluasi atau audit kembali terhadap penerapan SPBE pada Pemerintah Kota XYZ, khususnya dalam penyelenggaraan keamanan informasi. Metode evaluasi dilakukan dengan menggunakan standar Sistem Manajemen Keamanan Informasi (SMKI) melalui Indeks KAMI yang dipadukan dengan COBIT 5 APO13 *Manage Security* untuk mendapatkan tingkat kematangan keamanan informasi. Berdasarkan penilaian ulang didapatkan bahwa SPBE Pemerintah Kota XYZ berada pada nilai 3,17 (baik), dengan nilai tingkat kematangan berada pada level 1 (rintisan).

**Kata Kunci :** *E-Government*, SPBE, Audit, Keamanan Informasi, SMKI, Indeks KAMI, COBIT 5 APO13.

## PENDAHULUAN

Perkembangan teknologi berperan penting dalam menjalankan roda pemerintahan. Pemerintah sebagai roda kehidupan bangsa tentu harus dapat memberikan pelayanan yang terbaik bagi masyarakat. Oleh karena itu, implementasi teknologi informasi di sektor pemerintahan atau *E-Government* memiliki dampak yang sangat besar bagi proses jalannya pemerintahan. *E-Government* adalah proses pemanfaatan perkembangan teknologi informasi yang membantu menjalankan proses pemerintah khususnya dalam menjalankan fungsi pemerintahannya [1]. Pelaksanaan *E-Government* ini diharapkan dapat membantu meningkatkan pelayanan publik yang efektif serta efisien kepada masyarakat [2].

Penerapan *E-Government* yang saat diterapkan pada lembaga-lembaga pemerintahan adalah Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE adalah penyelenggaraan pemerintahan yang diselaraskan dengan penerapan teknologi informasi. Penyelenggaraan SPBE sendiri didasari oleh Perpres Nomor 95 Tahun 2018 yang mengatur tentang SPBE. Peran SPBE sendiri terhadap jalannya pemerintahan adalah untuk mewujudkan tata kelola pemerintahan yang bersih dan transparan. Selain itu, dengan penerapan SPBE, jalannya proses pemerintahan dapat lebih efektif dan akuntabel. Hal ini sesuai dengan RPJP Nasional 2005-2025 dimana diharapkan SPBE mampu menjadi sistem pemerintahan yang terpadu dan berkinerja tinggi.

Keamanan Informasi yang terdapat dalam SPBE haruslah terjaga kerahasiaannya, keutuhan, ketersediaan, dan keasliannya [3]. Oleh karena itu, salah satu bagian dari proses audit SPBE adalah audit keamanan SPBE. Audit keamanan SPBE berguna untuk mewujudkan standar keamanan informasi yang terdapat dalam SPBE itu sendiri. Standar yang dapat digunakan dalam proses audit keamanan SPBE adalah Sistem Manajemen Keamanan Informasi (SMKI) [4]. SMKI adalah proses audit yang berfokus pada proses manajemen risiko keamanan informasi terhadap sistem informasi, orang yang terlibat, hingga proses yang terdapat pada sistem informasi tersebut [3]. Penerapan SMKI pada dasarnya sejalan dengan penerapan standar ISO/IEC 27001 yang dimana ISO/IEC 27001 membahas tentang standar manajemen keamanan sistem informasi. Hal ini dikarenakan SMKI memiliki dasar atau berbasis ISO/IEC 27001. Pelaksanaan SMKI sendiri mengacu pada konsep manajemen *Plan-Do-Check-Action* (PDCA). Dengan menggunakan SMKI sebagai *tools* audit keamanan SPBE, maka setiap proses bisnis SPBE dan aset-aset yang terdapat dalam proses bisnis SPBE itu sendiri dapat ter standarisasi dan terkelola.

Terkait dengan pemantauan dan evaluasi dari SPBE yang tertuang dalam Permen PANRB Nomor 59 Tahun 2020 [5], Kota XYZ telah melakukan evaluasi dan pengukuran terkait tentang tingkat kematangan implementasi SPBE pada tahun 2021 [6]. Berdasarkan hasil evaluasi dan pengukuran SPBE tahun tersebut, Kota XYZ mendapatkan nilai 3,19 dengan kategori baik. Namun, jika melihat secara rinci mengenai hasil audit tersebut, Domain Manajemen SPBE mendapat nilai terendah. Domain ini memiliki peran kunci, karena pada domain tersebut terdapat indikator-indikator terkait dengan keamanan informasi yang seharusnya memiliki nilai tinggi karena terkait dengan keamanan informasi pada daerah yang penyelenggara SPBE.

Untuk dapat membantu meningkatkan hasil dari evaluasi SPBE, khususnya dalam aspek SMKI dimana hal tersebut sesuai dengan domain yang terkait dengan manajemen SPBE, salah satu *tools* yang dapat digunakan untuk mengukur proses manajemen SPBE adalah Indeks Keamanan Informasi (KAMI). Indeks KAMI adalah *tools* untuk mengukur serta menganalisis tingkat kesiapan keamanan informasi yang digunakan oleh sebuah organisasi [7]. Aspek penilaian indeks KAMI berfokus pada sistem informasi, orang yang terlibat, hingga proses yang terdapat pada sistem informasi tersebut. Indeks KAMI berjalan lurus pada penerapan Sistem Manajemen Keamanan Informasi (SMKI) dan ISO/IEC 27001 yang membahas tentang membahas tentang standar keamanan sistem informasi [8]. Selain itu, penilaian dengan menggunakan indeks KAMI juga mengacu pada konsep manajemen *Plan-Do-Check-Action* (PDCA).

Penerapan manajemen keamanan informasi dari SPBE memerlukan sebuah standar atau *framework* sebagai *best practice*. *Framework* tersebut diharap dapat membantu menyediakan kerangka kerja khususnya dalam pengelolaan keamanan informasi. Salah satu *framework* yang dapat menyediakan hal tersebut adalah COBIT 5. Dalam COBIT 5 terdapat domain dalam ruang lingkup *Align, Plan, Organize* (APO) dimana proses APO13 yang mampu mengatur keamanan TI (*Management Security*)[9]. Penggabungan antara penggunaan Indeks KAMI dan COBIT 5 diharapkan mampu memberikan gambaran tentang bagaimana memanajemen keamanan informasi dalam SPBE.

Berdasarkan permasalahan yang terjadi, maka dalam penelitian ini akan melakukan evaluasi terhadap aspek keamanan atau SMKI yang diterapkan pada SPBE Kota XYZ dengan menggunakan Indeks KAMI. Penerapan manajemen SPBE mampu menjawab berbagai permasalahan serta kebutuhan organisasi-organisasi terkait dalam pemenuhan nilai dari indikator baik dari segi aspek hingga domain pada nilai indeks SPBE. Penggunaan *framework* COBIT 5 dalam evaluasi SPBE juga memberikan hasil berupa gambaran rekomendasi khususnya dalam pembuatan Standar Operasional Prosedur yang dipadukan dengan penerapan dari SMKI. Hasil evaluasi SMKI ini nantinya akan menghasilkan rekomendasi-rekomendasi yang dapat diterapkan oleh Kota XYZ guna meningkatkan aspek manajemen keamanan serta peningkatan dalam nilai SPBE.

## TINJAUAN PUSTAKA

### Sistem Pemerintahan Berbasis Elektronik (SPBE)

Sistem Pemerintahan Berbasis Elektronik atau SPBE adalah penyelenggaraan pemerintahan dengan memanfaatkan teknologi informasi [1]. Penyelenggaraan SPBE sendiri diharapkan dapat mewujudkan tata kelola pemerintahan yang efektif serta efisien. Hal ini sesuai dengan tujuan pengembangan dan penerapan *E-Government*. SPBE didasari pada Perpres Nomor 95 Tahun 2018 dengan harapan terselenggaranya teknologi informasi dalam pemerintahan yang dapat meningkatkan pelayanan bagi masyarakat [9].

### Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) adalah runtutan pengetahuan yang dirancang untuk menentukan area yang memengaruhi organisasi dan distribusi kontrol keamanan yang dapat digunakan untuk melindungi informasi sebagai aset dan memastikan kerahasiaan organisasi itu sendiri [11]. SMKI menganut skema *Plan-Do-Check-Action* (PDCA). Skema PDCA sendiri merupakan metode yang terdapat pada standar ISO 27001 [7]. Dalam SMKI, terdapat tiga kategori kebijakan yang mengatur kontrol keamanan informasi yaitu:

1. Enterprise Information Security Policy (EISP)
   Kebijakan yang menentukan wewenang bagian, bagaimana cara menciptakan keamanan informasi di setiap bagian organisasi.
2. Issue Specific Security Policy (ISSP)
   Kebijakan yang menentukan peraturan serta menjelaskan apa saja yang dapat diterima atau dikirim dalam sebuah keamanan sistem informasi.
3. System Specific Policy (SSP)
   Kebijakan yang mengatur pengendalian dan konfigurasi perangkat baik dari sisi manajerial hingga teknikal.

### Indeks KAMI

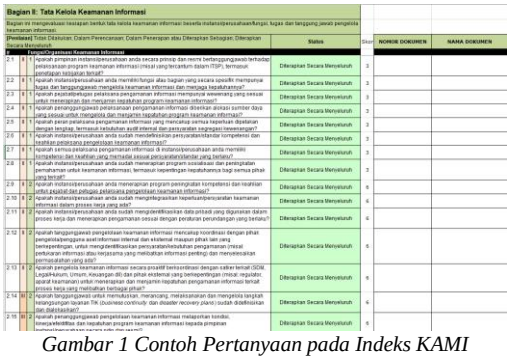
Indeks KAMI adalah sebuah *tools* atau alat yang disusun oleh Tim Direktorat Keamanan Informasi Kominfo. *Tools* ini digunakan untuk menganalisis, mengukur, dan mengevaluasi tingkat kematangan keamanan informasi dalam suatu organisasi [10]. Dengan menggunakan Indeks KAMI, sebuah organisasi akan mampu mengendalikan serta memanajemen keamanan terhadap informasi baik dari sisi aset hingga sistem yang dimilikinya.

Versi Indeks KAMI yang terbaru adalah versi 4.2. Versi ini dirilis pada 25 Mei 2021 dengan revisi yang dikeluarkan oleh BSSN. Secara umum, Indeks KAMI berfokus pada tujuh kategori penilaian, yaitu kategori SE, tata kelola, risiko, kerangka kerja, pengelolaan aset, teknologi, dan suplemen.

1. Bagian I: Kategori Sistem Elektronik
   Mengevaluasi tingkat atau kategori sistem elektronik yang dipakai, mulai dari nilai investasi, anggaran, pengelolaan, hingga penggunaan dari sistem elektronik yang dipakai.
2. Bagian II: Tata Kelola Keamanan Informasi
   Mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

3. Bagian III: Pengelolaan Risiko Keamanan Informasi
   Mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
4. Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi
   Mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
5. Bagian V: Pengelolaan Aset Informasi
   Mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.
6. Bagian VI: Teknologi dan Keamanan Informasi
   Mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.
7. Bagian VII: Suplemen
   Mengevaluasi keterlibatan pihak ketiga dalam rantai pasok (*supply chain*) layanan suatu instansi/perusahaan menimbulkan risiko terkait keberadaan/keterlibatan pihak eksternal tersebut.

Masing-masing kategori penilaian memiliki pertanyaan-pertanyaan terkait dengan penerapan dari masing-masing kategori penilaian tersebut seperti yang terdapat pada Gambar 1.

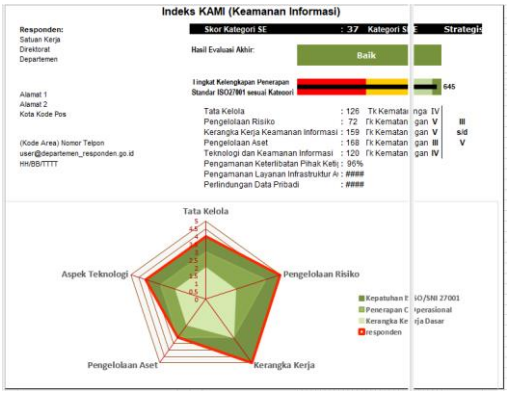



*Gambar 1 Contoh Pertanyaan pada Indeks KAMI*

Setiap pertanyaan pada kategori penilaian di Indeks KAMI, terdapat kategori kontrol yang menjadi landasan penilaian. Kategori kontrol pada setiap kategori penilaian dibagi menjadi tiga, yaitu kontrol 1 (kerangka kerja dasar keamanan informasi), kontrol 2 (efektivitas dan penerapan keamanan informasi), dan kontrol 3 (kemampuan untuk meningkatkan kinerja keamanan informasi).

Nilai akhir dalam penilaian masing-masing kategori pada Indeks KAMI berupa tingkat kematangan. Tingkat kematangan penerapan keamanan informasi pada Indeks KAMI berada pada lima tingkat, yaitu Tingkat I (Tidak Layak), Tingkat II (Perlu Perbaikan), Tingkat III (Cukup), Tingkat IV (Baik), dan Tingkat V (Sangat Baik). Untuk membantu memberikan uraian lebih detail dari masing-masing tingkatan, tingkatan ini ditambah dengan tingkatan antara I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Tambahan empat tingkat kematangan tersebut memiliki arti bahwa penerapan keamanan berada di tingkatan sesuai dengan huruf awal, namun nilai tambah (plus) yang setelah nilai tingkat kematangan memiliki arti penerapan sudah melebihi tingkatan pada huruf awal, namun belum sesuai untuk dikatakan berada pada tingkat selanjutnya.

Hasil akhir penilaian Indeks KAMI secara keseluruhan berisi *brief* penilaian terhadap penerapan keamanan informasi.




*Gambar 2 Hasil Penilaian Indeks KAMI versi 4.2*

Selain memberikan *brief* secara keseluruhan terkait penerapan keamanan informasi, Indeks KAMI juga memberikan gambaran mengenai rentang tingkat kematangan serta rentang kelengkapan penganan. Gambaran ini berfungsi sebagai landasan dasar sebuah organisasi untuk kesiapan sertifikasi ISO 27001 ISMS (Sumber: Dokumen Indeks KAMI V 4.2) [8].


*Gambar 3 Rentang Tingkat Kesiapan Sertifikasi ISO 27001 Dalam Indeks KAMI*

**COBIT 5 APO 13**

COBIT (*Control Objective for Information and related Technology*) adalah *framework* kerangka kerja sebagai panduan dalam tata kelola TI[12]. COBIT sendiri berfungsi sebagai penghubung antara GAP kebutuhan dan teknis dalam pelaksanaan dalam pemenuhan tersebut dalam sebuah organisasi. Dengan menggunakan COBIT, memungkinkan sebuah organisasi untuk mengembangkan kebijakan serta meningkatkan kualitas dan nilai dalam pelaksanaan alur proses pada bagian IT.

Dalam COBIT 5, proses yang mengatur mengenai keamanan informasi adalah APO13 (*Manage Security*)[13]. Dalam COBIT, untuk mengukur seberapa tingkatan kapabilitas dan maturitas dapat digunakan dengan *Capability Maturity Model Integration* (CMMI) dengan menentukan aktivitas proses dari *level* 0 hingga *level* 5 yang menjelaskan seberapa baik suatu proses diimplementasikan dan berkinerja[14]. Proses APO13 dalam COBIT 5 bertujuan untuk mengendalikan dampak dari insiden keamanan informasi[9]. COBIT 5 sendiri memiliki enam tingkatan kematangan yang dimulai dari Level 0 (incomplete), Level 1 (*Initialized*), Level 2 (*Managed*), Level 3 (*Defined*), Level 4 (*Quantitatively Managed*), dan Level 5 (*Optimized*).

**Metode *Plan-Do-Check-Action* (PDCA)**

Metode *Plan-Do-Check-Action* (PDCA) adalah digunakan untuk mengatur penilaian risiko, evaluasi risiko, kontrol perlindungan keamanan, desain dan manajemen keamanan dengan ISO 27001 yang sesuai dengan kebutuhan ruang lingkup analisis SMKI [7]. Pada SMKI, skema PDCA dijabarkan sebagai berikut:

1. *Plan*, menetapkan sasaran, kebijakan, serta target prosedur SMKI.
2. *Do*, menetapkan, mengidentifikasi, serta menerapkan prosedur risiko dari permasalahan keamanan sesuai dengan tujuan organisasi.
3. *Check*, melakukan pemeriksaan terhadap pelaksanaan penerapan SMKI sesuai dengan kebijakan dan sasaran manajemen organisasi.
4. *Action*, melakukan tindakan sesuai dengan hasil audit SMKI dan hasil GAP dimana mengeluarkan hasil berupa rekomendasi.

**METODE PENELITIAN**

Penelitian ini menggunakan metode *Plan-Do-Check-Action* (PDCA) pada tahap evaluasi manajemen keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) dengan melakukan pengisian kuesioner kepada staf Pemerintah Kota XYZ mengenai pelaksanaan manajemen keamanan informasi dengan menggunakan Indeks KAMI versi 4.2. Dalam penelitian ini, hasil yang akan didapatkan adalah hasil berupa angka dalam tingkat kematangan keamanan informasi mulai dari rentang tidak layak, pemenuhan kerangka kerja dasar, cukup baik, dan baik [8].

**Instrumen Penelitian**

Instrumen-instrumen yang digunakan dalam penelitian ini adalah:

1. Observasi
   Observasi dilakukan penulis dengan melakukan pengamatan langsung mengenai penerapan SPBE dalam lingkup SMKI di lingkungan Kota XYZ.
2. Wawancara
   Tahapan wawancara yang diakukan peneliti adalah untuk mendapatkan informasi mengenai penyelenggaraan SPBE di lingkungan Kota XYZ.
3. Pengumpulan Bukti
   Pada penelitian ini, peneliti melakukan pengumpulan bukti guna sebagai indikator pemenuhan dalam kebutuhan dokumen dalam Indeks KAMI versi 4.2 yang dimiliki oleh Pemerintah Kota XYZ.
4. Kuesioner
   Pada penelitian ini, kuesioner berupa Indeks KAMI versi 4.2 digunakan untuk

mendapatkan hasil GAP dan tingkat kematangan penerapan manajemen keamanan informasi dalam pelaksanaan SPBE Kota XYZ.

**Jenis dan Sumber Data**

Penelitian ini menggunakan jenis data kuantitatif yang diperoleh dari hasil kuesioner didapatkan dari kuesioner dan penghitungan GAP angka serta tingkat kematangan. Sumber data yang digunakan dalam penelitian ini adalah data-data hasil dari wawancara kepada pihak Pemerintah Kota XYZ serta pengumpulan bukti-bukti pemenuhan dari pelaksanaan manajemen keamanan informasi dalam SPBE.

**Alur Penelitian**

Penelitian ini menggunakan alur penelitian dari metode *Plan-Do-Check-Action* sebagai berikut:

1. *Plan*
   Tahapan *plan* dimulai dengan melakukan observasi di Kota XYZ untuk melihat bagaimana penerapan SPBE khususnya dalam lingkup SMKI. Kemudian, dilanjutkan dengan melakukan tanya jawab kepada beberapa staf Pemerintah Kota XYZ untuk mengetahui sejauh mana penerapan keamanan informasi pada SPBE. Berdasarkan observasi tersebut, ditemukan permasalahan bahwa penerapan SPBE di Kota XYZ berada pada angka 3,19 yang tergolong baik. Namun, jika melihat Domain Manajemen SPBE mendapat nilai terendah yaitu 2,18 yang tergolong cukup. Domain ini memiliki peran kunci, karena pada domain tersebut terdapat aspek-aspek terkait dengan manajemen keamanan informasi yang seharusnya memiliki nilai tinggi karena terkait dengan keamanan informasi pada Kota XYZ.
2. *Do*
   Tahapan *do* dimulai dengan melakukan pengumpulan bukti terkait penerapan SMKI dalam SPBE dengan bentuk dokumen-dokumen yang telah dimiliki oleh Pemerintah Kota XYZ. Seluruh bukti dokumen baik yang masih dalam bentuk draft hingga dokumen yang sudah disahkan disusun sesuai dengan kategori-kategori yang terdapat pada Indeks Kami versi 4.2.
3. *Check*
   Tahapan *check* dilakukan dengan melakukan penilaian keamanan Informasi dengan menggunakan Indeks KAMI versi 4.2 yang didasarkan pada bukti dokumen-dokumen yang telah dimiliki oleh Kota XYZ. Pada tahapan ini, peneliti menggunakan lima kategori penilaian dalam Indeks KAMI versi 4.2 untuk mendapatkan tingkat kematangan penerapan SMKI pada pelaksanaan SPBE di Kota XYZ. Setelah mendapatkan tingkat kematangan dari lima kategori penilaian dalam Indeks KAMI versi 4.2, dilanjutkan dengan penentuan *maturity level* dengan menggunakan tabel *Capability Maturity Model Integration* (CMMI) dari COBIT 5 APO 13 dan kapabilitas proses SPBE. Selanjutnya, dilakukan penilaian penerapan SPBE untuk mendapatkan hasil asli (*real*) terhadap penerapan SPBE dalam lingkup SMKI. Penilaian penerapan SPBE berdasarkan Permen PANRB Nomor 59 Tahun 2020 diberikan pada setiap struktur penilaian SPBE sesuai dengan tingkat prioritas dan kepentingan masing-masing.
4. *Action*
   Pada tahapan *action*, data berupa angka dan tingkat kematangan dari hasil dari kuesioner Indeks KAMI versi 4.2, tingkat kematangan *maturity level*, serta hasil asli (*real*) terhadap penerapan SPBE digunakan sebagai landasan dasar penyusunan rekomendasi-rekomendasi terkait dengan pemenuhan standar SMKI yang dibutuhkan oleh Kota XYZ.

## HASIL DAN PEMBAHASAN

**Plan**

1. Observasi
   Proses observasi dilakukan berdasarkan Laporan Akhir Evaluasi SPBE Pemerintah Kota XYZ Tahun 2021, dimana berfokus pada indikator-indikator penerapan SPBE terkait dengan SMKI. Berdasarkan observasi tersebut didapatkan bahwa penilaian

melingkupi pada indikator 8, 9, 21, 22, 23, 24, 25, 29, 30, dan 31. Lalu, metode penilaian pada penelitian ini menggunakan Indeks KAMI dengan versi terbaru yaitu Indeks KAMI 4.2 yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) Republik Indonesia, dengan aspek penilaian manajemen keamanan informasi terkait dengan penerapan SMKI dalam SPBE.

*Tabel 1 Bagian Penggunaan Indikator Penilaian Indeks KAMI*

| **Bagian** | **Tujuan** |
|---|---|
| Bagian II: Tata Kelola Keamanan Informasi | Mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. |
| Bagian III: Pengelolaan Risiko Keamanan Informasi | Mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. |
| Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi | Mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. |
| Bagian V: Pengelolaan Aset Informasi | Mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. |
| Bagian VI: Teknologi dan Keamanan Informasi | Mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. |

2. Wawancara

Pengisian Indeks KAMI dilakukan dengan wawancara tanya jawab kepada tim audit SPBE Kota XYZ. Pengumpulan informasi untuk pemenuhan Indeks KAMI dilakukan secara bertahap. Pemaparan informasi mengenai Indeks KAMI dilakukan terlebih dahulu untuk memberikan informasi terkait pemenuhan dari kuesioner yang akan dilakukan. Lalu setelahnya, dilaksanakan pengumpulan bukti terkait kuesioner Indeks KAMI. Lalu dilakukan pengisian kuesioner berdasarkan bukti dokumen yang telah dikumpulkan.

3. Penentuan Ruang Lingkup Penilaian SPBE

SPBE memiliki 47 indikator tingkat kematangan penerapan dimana memiliki kegiatan proses bisnis yang membantu mewujudkan tujuan dari masing-masing indikator tersebut. Hasil pengumpulan bukti dipaparkan kepada Pemerintah Kota XYZ, dengan merujuk kepada dokumen-dokumen terkait SMKI. Dalam lingkup SMKI, didapatkan 10 indikator yang sesuai dengan keamanan informasi yaitu indikator 8, 9, 21, 22, 23, 24, 25, 29, 30, dan 31.

**Do**

Pengumpulan Bukti Terkait Penerapan SPBE dilakukan dengan mengumpulkan berbagai dokumen-dokumen terkait dengan penilaian terhadap Indeks KAMI yang didapat dari dokumen penerapan manajemen keamanan informasi pada Pemerintah Kota XYZ.

**Check**

1. Penilaian Keamanan Informasi

Kumpulan data hasil wawancara serta pengumpulan bukti berupa dokumen dilakukan kepada informan serta pengisian Indeks KAMI terkait dengan pelaksanaan SPBE dalam lingkup SMKI. Hal ini dilakukan untuk dapat mengelompokkan sistem elektronik ke kategori rendah, tinggi, atau strategis melalui beberapa pertanyaan terkait penerapan SPBE dalam lingkup SMKI. Hasil berupa data nilai angka yang mengindikasi total nilai evaluasi dari masing-masing bagian Indeks KAMI.

1) Tata Kelola Keamanan Informasi

*Tabel 2 Penilaian Bagian II Indeks KAMI*

| **Bagian II: Tata Kelola Keamanan Informasi** | | | |
|---|---|---|---|
| Jumlah Pertanyaan | | | 22 |
| **Jawaban Bagian II** | | | |
| **Status Pengamanan** | **Kategori Kontrol** | | |
| | **1** | **2** | **3** |
| Tidak Dilakukan | 0 | 2 | 6 |
| Dalam Perencanaan | 1 | 5 | 0 |

| | | | |
|---|---|---|---|
| Dalam Penerapan / Penerapan Sebagian | 5 | 1 | 0 |
| Diterapkan Secara Menyeluruh | 2 | 0 | 0 |
| **Total Nilai Bagian II** | | | **31** |
| **Tingkat Kematangan** | | | **I+** |

Tata Kelola Keamanan Informasi mengukur seberapa jauh Kota XYZ dalam tata kelola keamanan informasinya. Hasilnya dalam kategori kontrol tiga seluruh tata kelola keamanan informasi tidak dilakukan. Sehingga total nilai dari bagian ini sebesar 31 sehingga dapat dikatakan **Tidak Valid**.

2) Pengelolaan Risiko Keamanan Informasi

*Tabel 3 Penilaian Bagian III Indeks KAMI*

| **Bagian III: Pengelolaan Risiko Keamanan Informasi** | | | |
|---|---|---|---|
| Jumlah Pertanyaan | | | 16 |
| **Jawaban Bagian III** | | | |
| **Status Pengamanan** | **Kategori Kontrol** | | |
| | **1** | **2** | **3** |
| Tidak Dilakukan | 6 | 4 | 2 |
| Dalam Perencanaan | 4 | 0 | 0 |
| Dalam Penerapan / Penerapan Sebagian | 0 | 0 | 0 |
| Diterapkan Secara Menyeluruh | 0 | 0 | 0 |
| **Total Nilai Bagian III** | | | **4** |
| **Tingkat Kematangan** | | | **I** |

Pengelolaan Risiko Keamanan Informasi memberikan gambaran Kota XYZ belum memiliki pengelolaan risiko keamanan informasi yang terstruktur, sehingga mendapatkan nilai empat dimana dapat dikatakan **Tidak Valid**.

3) Kerangka Kerja Pengelolaan Keamanan Informasi

*Tabel 4 Penilaian Bagian IV Indeks KAMI*

| **Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi** | | | |
|---|---|---|---|
| Jumlah Pertanyaan | | | 29 |
| **Jawaban Bagian IV** | | | |
| **Status Pengamanan** | **Kategori Kontrol** | | |
| | **1** | **2** | **3** |
| Tidak Dilakukan | 10 | 8 | 7 |
| Dalam Perencanaan | 2 | 2 | 0 |
| Dalam Penerapan / Penerapan Sebagian | 0 | 0 | 0 |
| Diterapkan Secara Menyeluruh | 0 | 0 | 0 |
| **Total Nilai Bagian IV** | | | **6** |
| **Tingkat Kematangan** | | | **I** |

Kerangka Kerja Pengelolaan Keamanan Informasi memberikan gambaran mengenai kerangka kerja pengelolaan keamanan informasi di SMKI Kota XYZ. Seluruh status pengamanan terkait tata kelola belum dilakukan secara sepenuhnya di SPBE Kota XYZ. Oleh karena itu, total nilai untuk bagian ini mendapat nilai enam, dimana termasuk **Tidak Valid**.

4) Pengelolaan Aset Informasi

*Tabel 5 Penilaian Bagian V Indeks KAMI*

| **Bagian V: Pengelolaan Aset Informasi** | | | |
|---|---|---|---|
| Jumlah Pertanyaan | | | 38 |
| **Jawaban Bagian V** | | | |
| **Status Pengamanan** | **Kategori Kontrol** | | |
| | **1** | **2** | **3** |
| Tidak Dilakukan | 9 | 6 | 4 |
| Dalam Perencanaan | 8 | 3 | 0 |
| Dalam Penerapan / Penerapan Sebagian | 7 | 1 | 0 |
| Diterapkan Secara Menyeluruh | 0 | 0 | 0 |
| **Total Nilai Bagian V** | | | **18** |
| **Tingkat Kematangan** | | | **I+** |

Pengelolaan Aset Informasi Pengelolaan aset terlihat gambaran bahwasanya dalam SMKI di SPBE Kota XYZ, belum melakukan pengelolaan aset dan hanya sampai pada proses dalam perencanaan dan penerapan secara sebagian (belum menyeluruh). Sehingga pendataan dan pengelolaan terkait aset yang mereka miliki belum terukur dengan baik dengan nilai 18 yang termasuk **Tidak Valid**.

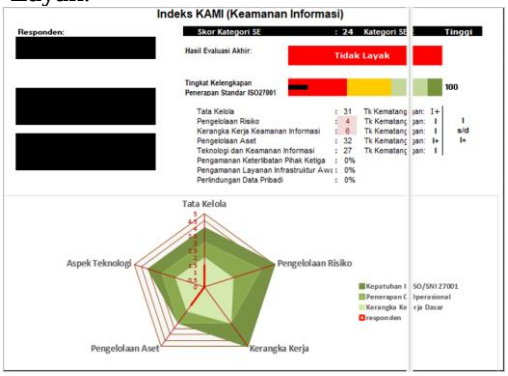
5) Teknologi dan Keamanan Informasi

*Tabel 6 Penilaian Bagian VI Indeks KAMI*

| **Bagian VI: Teknologi dan Keamanan Informasi** | | | |
|---|---|---|---|
| Jumlah Pertanyaan | | | 26 |
| **Jawaban Bagian VI** | | | |
| **Status Pengamanan** | **Kategori Kontrol** | | |
| | **1** | **2** | **3** |
| Tidak Dilakukan | 5 | 8 | 2 |
| Dalam Perencanaan | 0 | 0 | 0 |
| Dalam Penerapan / Penerapan Sebagian | 7 | 1 | 0 |
| Diterapkan Secara Menyeluruh | 1 | 2 | 0 |
| **Total Nilai Bagian V** | | | **27** |
| **Tingkat Kematangan** | | | **I** |

Teknologi dan Keamanan Informasi memberikan gambaran bahwasanya sebagian besar langkah pengamanan untuk tata kelola keamanan informasi pada SPBE Kota XYZ. Dengan nilai yang didapatkan 27, Kota XYZ belum secara seluruhnya menerapkan teknologi dan khususnya keamanan informasi. Oleh karena itu, pada bagian ini dikatakan **Tidak Valid**.

Dari hasil akhir penilaian yang dilakukan pada lima kategori kuesioner, ditemukan bahwa Kota XYZ dalam level penerapan serta tingkat kematangan seluruh aspek yang dijadikan penilaian berada di Tingkat I, dengan level penerapan masih terbatas pada **Penerapan Kerangka Kerja**. Oleh karena itu, tingkat kematangan seluruh bagian penilaian berada dalam tingkat **Tidak Layak**.




*Gambar 4 Hasil Penilaian Indeks KAMI Kota XYZ*

2. Penilaian *Maturity Level* dan *Capability Level*

Penentuan *Maturity Level* dilakukan untuk mengetahui tingkat kematangan penerapan keamanan informasi dalam organisasi. Untuk Pemerintah Kota XYZ. Berdasarkan hasil penilaian terhadap Indeks KAMI, yang selanjutnya akan menentukan tingkat *Maturity Level* pada CMMI dan SPBE.

Penilaian *capability level* CMMI COBIT 5 dengan Indeks KAMI dilakukan untuk mengetahui tingkat kematangan dari masing-masing penerapan mengenai manajemen keamanan informasi yang terdapat pada Pemerintah Kota XYZ. Dari hasil akhir penilaian, ditemukan bahwa level penerapan serta tingkat kematangan seluruh aspek yang dijadikan penilaian berada di Tingkat I, dengan level penerapan masih terbatas pada **Penerapan Kerangka Kerja**. Oleh karena itu, tingkat kematangan seluruh bagian penilaian berada dalam tingkat **Tidak Layak**.

*Tabel 7 Penilaian Tingkat Kematangan (Capability Level) Indeks KAMI*

| **Aspek Penilaian Indeks KAMI** | **Nilai Indeks KAMI** | **Level** | **Tingkat Kematangan** |
|---|---|---|---|
| Bagian 2 - Tata Kelola Keamanan Informasi | I+ | Penerapan Kerangka Kerja | Tidak Layak |
| Bagian 3 - Pengelolaan Aset | I | Penerapan Keran | Tidak Layak |

| Aspek Penilaian Indeks KAMI | Nilai Indeks KAMI | Level | Tingkat Kematangan |
|---|---|---|---|
| Informasi | | gka Kerja | |
| Bagian 4 - Teknologi dan Keamanan Informasi | I | Penerapan Kerangka Kerja | Tidak Layak |
| Bagian 5 - Pengelolaan Risiko Keamanan Informasi | I+ | Penerapan Kerangka Kerja | Tidak Layak |
| Bagian 6 - Kerangka Kerja Pengelolaan Keamanan Informasi | I | Penerapan Kerangka Kerja | Tidak Layak |

Untuk CMMI sendiri, menggunakan aspek penilaian atau bagian dari Indeks KAMI. Dari penilaian tersebut didapatkan bahwa Pemerintah Kota XYZ belum mampu menerapkan *best practice* dari COBIT 5 APO13 *Manage Security*. Hal ini ditandai dengan keseluruhan bagian *Capability Level* CMMI *Practice Name* APO13 berada pada **Level 0 (*Incomplete*)** yang berarti Pemerintah Kota XYZ belum atau hanya menerapkan sebagian dari proses SMKI dalam penerapan SPBE.

*Tabel 8 Penilaian CMMI Berdasarkan Nilai Indeks KAMI*

| *Practice Name* APO13 | Aspek Penilaian Indeks KAMI | Nilai Indeks KAMI | Nilai CMMI |
|---|---|---|---|
| APO13.01 - Membangun dan memelihara SMKI | Tata Kelola Keamanan Informasi | I+ | Level 0 |
| | Pengelolaan Aset Informasi | I | Level 0 |
| | Teknologi dan Keamanan Informasi | I | Level 0 |
| APO13.02 - Menentukan dan mengelola rencana perlakuan risiko keamanan informasi | Pengelolaan Risiko Keamanan Informasi | I+ | Level 0 |
| APO13.03 - Memonitor dan meninjau SMKI | Kerangka Kerja Pengelolaan Keamanan Informasi | I | Level 0 |

3. Penilaian Penerapan SPBE

Untuk mengetahui tingkat kematangan penerapan SPBE di Pemerintah Kota XYZ dilakukan evaluasi indikator SPBE yang didasarkan pada Permen PANRB Nomor 59 Tahun 2020. Penilaian ini dilakukan dengan mengumpulkan bukti dukung berupa dokumen-dokumen yang telah ada. Lalu, sesuai dengan seminar "[LIVE] Sosialisasi Permen PANRB No. 59 Tahun 2020 tentang Pemantauan dan Evaluasi SPBE" yang diselenggarakan oleh Kementerian PANRB pada 19 November 2020 di kanal Youtube Kementerian PANRB[16], dilakukan penilaian dengan bukti dokumen yang telah dikumpulkan agar penilaian berjalan secara objektif. Hasil penilaian ulang menunjukkan bahwa Pemerintah Kota XYZ mendapat nilai rata-rata sebesar **3,17 (Baik)**. Hasil ini tentu berbeda dengan penilaian yang dilakukan pada tahun 2021, dimana sebelumnya pada tahun 2021 mendapat nilai **3,19** dan pada tahun 2019 mendapat **3,33**.

**Action**

Penyelenggaraan SPBE dalam lingkup SMKI di lingkungan Kota XYZ membutuhkan panduan atau pedoman umum terhadap penyelenggaraan keamanan informasinya. Rekomendasi yang dapat diberikan untuk pemenuhan tersebut adalah

berupa dokumen antara lain dokumen Pedoman Audit TIK dan Dokumen SMKI atau Manual SMKI.

Penyusunan rekomendasi disusun berdasarkan berbagai kebutuhan terkait penerapan SMKI terhadap jalannya SPBE. Rekomendasi disusun sesuai dengan aturan-aturan terkait dengan penerapan SMKI hingga penerapan SPBE. Landasan hukum atas penyusunan rekomendasi tersebut adalah:

- Peraturan BSSN Nomor 8 Tahun 2021.
- Peraturan BSSN Nomor 4 Tahun 2021.
- Peraturan ANRI Nomor 11 Tahun 2021.
- Permenpan RB Nomor 59 Tahun 2020.
- Permenpan RB Nomor 5 Tahun 2020.
- Peraturan Kominfo Nomor 4 Tahun 2016.

## SIMPULAN

Penerapan Sistem Manajemen Keamanan Informasi (SMKI) oleh Kota XYZ dalam penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) berada pada level paling rendah, dimana seluruh aspek penilaian terkait manajemen keamanan informasi berada pada tingkatan kematangan I sampai I+ dengan kategori tingkat tergolong Tidak Layak. Hal ini mengindikasikan bahwa Pemerintah Kota XYZ perlu meninjau kembali penerapan manajemen keamanan informasi yang telah berjalan saat ini.

Untuk dapat memenuhi kebutuhan dari Manajemen keamanan SPBE, Kota XYZ perlu menyediakan atau menyusun dokumen-dokumen terkait dengan pemenuhan SMKI. Dokumen-dokumen tersebut harus dapat menyesuaikan dengan hasil terkait dengan penilaian dari Indeks KAMI.

Rekomendasi yang dapat diberikan oleh peneliti adalah agar dapat melakukan penyusunan sebuah dokumen keamanan informasi, khususnya dokumen Manual SMKI yang pada dasarnya sudah memuat seluruh standar keamanan informasi pada sebuah organisasi.

## DAFTAR PUSTAKA

A. A. Bouty, M. Hidayat Koniyo, and D. Novian, "Evaluasi Sistem Pemerintahan Berbasis Elektronik Menggunakan E-Government Maturity Model (Kasus di Pemerintah Kota Gorontalo)," *Jurnal Penelitian Komunikasi dan Opini Publik*, vol. 23, no. 1, pp. 16–24, 2019.

[2] O. Somantri and I. D. Hasta, "Implementasi E-Government Pada Kelurahan Pesurungan Lor Kota Tegal Berbasis Service Oriented Architecture (SOA)," *Jurnal Pengembangan IT(JPIT)*, vol. 2, no. 1, pp. 23–29, 2017.

[3] I. Gede Putu Krisna Juliharta, "Analisa Tingkap Kesiapan Penerapan Keamanan Teknologi Informasi Dalam Pelaksanaan E-Government Berbasis Indeks Keamanan Informasi (Kami) Studi Kasus Pemerintah Kota Kediri," *Jurnal Teknologi Informasi dan Komputer*, vol. 5, no. 1, pp. 21–26, 2019.

[4] Badan Standardisasi Nasional, "SMKI: Standar Keamanan Informasi yang Diakui Dunia - BSN - Badan Standardisasi Nasional - National Standardization Agency of Indonesia - Setting the Standard in Indonesia ISO SNI WTO," Aug. 19, 2020. https://bsn.go.id/main/berita/detail/11356/smki-standar-keamanan-informasi-yang-diakui-dunia (accessed Apr. 04, 2022).

[5] Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, "Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020," Jakarta, Sep. 2020.

[6] Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, "Keputusan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 1503 Tahun 2021," Jakarta, Dec. 2021.

[7] Nurul Fadhyalah Octariza, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Pusat PT Jasa Marga," Thesis, Universitas Islam Negeri Syarif Hidayatullah, Jakarta, 2019.

[8] BSSN, "Indeks KAMI Versi 4.2," 4.2, May 25, 2021

[9] Faridl Mughoffar, M. K. Ir.Ahmad Holil Noor Ali, and S. K. M. S. Anisah Herdiyanti, "Penyusunan Template Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005 dan Patuh Terhadap Cobit 5 Management Processes Apo13 Manage Security," *JURNAL TEKNIK POMITS* , vol. 2, no. 1, pp. 1–6, 2013.

[10] B. Adi Purnomo, L. Abdurrahman, and R. Fauzi, "Perancangan Keamanan Informasi Menggunakan Metode Analisis Risiko Cobit 5 Pada Layanan Bisnis PT POS Indonesia," *e-Proceeding of Engineering*, vol. 8, no. 2, pp. 2851–2864, 2021.

[11] Tim Direktorat Keamanan Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik," Jakarta, Sep. 2011.

[12] Y. Megasyah and A. A. Arifnur, "Academic Information System Security Audits Using Cobit 5 Framework Domains APO12, APO13 and DSS05," *Journal of Applied Engineering and Technological Science*, vol. 1, no. 2, pp. 124–135, 2020.

[13] ISACA, *COBIT5 A Business Framework for the Governance and Management of Enterprise IT*, vol. 1. Illinois: ISACA, 2012.

[14] Luis Gorgona, "Building a Maturity Model for COBIT 2019 Based on CMMI," Nov. 2021. [Online]. Available: https://www.isaca.org/resources/cobit

[15] A. Calder, *ISO27001/ISO27002 A Pocket Guide: 2013*, Second Edition. IT Governance Publishing, 2013.

[16] Kementerian PANRB, Indonesia. *[LIVE] Sosialisasi Permen PANRB No. 59 Tahun 2020 tentang Pemantauan dan Evaluasi SPBE*, (Nov. 19, 2020). Accessed: Oct. 23, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=l-e6gpw6puU