EVALUASI DAN REKOMENDASI PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) SPBE PADA INSTANSI XYZ

I Gede Putu Krisna Juliharta[1)] Ni Kadek Sinta Febriani[2)] Ketut Queena Fredlina[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)] ixa.sintafebriani@gmail.com[2)] queena@primakara.ac.id[3)]

ABSTRACT

The use of technology, information, and communication in the field of government is known as e-Government. One of the implementations of e-Government carried out by government agencies or agencies in Indonesia is SPBE. To ensure that the SPBE runs according to the goals set, a monitoring and evaluation process is needed from the SPBE itself. The XYZ Agency itself has many systems that are intended for the community, to make it easier and to be able to reach all levels of government. To maintain and improve the quality of information security management at XYZ Agency is to evaluate the level of readiness and completeness of information security management using the KAMI Index parameters, which will later become a reference for producing recommendations in the form of ISMS guidelines.

Based on the results of an evaluation of the implementation of information security management related to the implementation of SPBE at the XYZ Agency, it is at an inappropriate level with the implementation of information security management that has been running which is still at level I to I+. To be able to adjust to these values. The XYZ Agency needs to prepare an Information Security Management System document as a standard guide in implementing SPBE.
Keywords*: SPBE, Information Security, ISMS, KAMI Index, Guidelines, E-government*

ABSTRAK

Pemanfaatan teknologi, informasi dan komunikasi di bidang pemerintahan dikenal dengan *e-Government*. Salah satu penerapan *e-Government* yang dilakukan oleh lembaga ataupun instansi pemerintah di Indonesia yaitu SPBE. Untuk menjamin jalannya SPBE tersebut agar berjalan sesuai dengan tujuan yang telah tetapkan maka diperlukan proses pemantauan dan evaluasi dari SPBE itu sendiri. Instansi XYZ sendiri memiliki banyak sistem yang diperuntukkan kepada masyarakat, guna mempermudah dan dapat menjangkau semua lapisan masyarakat. Untuk menjaga dan meningkatkan kualitas manajemen keamanan informasi pada Instansi XYZ adalah dengan mengevaluasi tingkat kesiapan dan kelengkapan dari manajemen keamanan informasi menggunakan parameter Indeks KAMI, yang nantinya akan menjadi acuan untuk menghasilkan rekomendasi berupa panduan SMKI.

Berdasarkan hasil evaluasi penerapan manajemen keamanan informasi terkait dengan penyelenggaraan SPBE pada Instansi XYZ berada pada level tidak layak dengan penyelenggaraan manajemen keamanan informasi yang telah berjalan yang masih berada pada tingkat I sampai I+. Untuk dapat menyesuaikan dengan nilai tersebut. Instansi XYZ perlu menyusun dokumen Sistem Manajemen Keamanan Informasi sebagai panduan baku dalam penyelenggaraan SPBE.
Kata Kunci : SPBE, Keamanan Informasi, SMKI, Indeks KAMI, Pedoman, *E-goverment*

PENDAHULUAN

Teknologi Informasi dan Komunikasi (TIK) tidak hanya bersifat sebagai perangkat pembantu kegiatan berorganisasi, akan tetapi merupakan bagian dari organisasi dalam upaya mencapai tujuan organisasi tersebut. Ini dilakukan untuk mewujudkan pemerintahan yang *good governance* terutama dalam pelayanan publik yang erat kaitannya dengan penggunaan informasi, komunikasi, dan teknologi[1].

Pemanfaatan teknologi, informasi dan komunikasi di bidang pemerintahan dikenal

dengan *e-Government*. Penerapan dari *e-Government* sebaiknya bukan sekedar mengikuti tren, melainkan suatu langkah strategis dalam upaya peningkatan pelayanan, meningkatkan partisipasi masyarakat, transparansi, akuntabilitas, efisiensi dan efektivitas birokrasi[2]. Salah satu penerapan *e-Governmen*t yang dilakukan oleh lembaga ataupun instansi pemerintah yaitu SPBE. Penerapan SPBE ini tercantum dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik. Pemerintahan dituntut untuk bisa sampai pada level integrasi, baik antar OPD, antar pemerintah daerah, serta antara pemerintah daerah dengan pusat[3]. Untuk menjamin jalannya SPBE tersebut agar berjalan sesuai dengan tujuan yang telah tetapkan maka diperlukan proses pemantauan dan evaluasi dari SPBE itu sendiri. Hal tersebut dituangkan ke dalam aturan Permen PANRB Nomor 59 Tahun 2020. Evaluasi ini juga berguna untuk mengetahui capaian kemajuan dari penerapan SPBE, meningkatkan kualitas penerapan SPBE dan meningkatkan kualitas pelayan publik.

Instansi pemerintahan di Indonesia juga perlu menerapkan keamanan informasi untuk menghindari adanya pencurian data dan hilangnya data secara sengaja maupun tidak sengaja[4]. Instansi XYZ sendiri memiliki banyak sistem yang diperuntukkan kepada masyarakat, guna mempermudah dan dapat menjangkau semua lapisan masyarakat. Untuk mengakses sistem-sistem tersebut tentunya diperlukan data-data pribadi pendukung lainnya untuk mempermudah akses terhadap sistem tersebut seperti nama, alamat, NIK dan informasi lainnya yang bersifat pribadi lainnya. Selaku instansi yang bertugas untuk menampung, mengelola dan memproses data-data pribadi dari masyarakat.

Terkait dengan evaluasi manajemen keamanan informasi yang tertuang ke dalam Permen PANRB No. 59 Tahun 2020. Dalam peraturan tersebut dijelaskan bahwa Pemantauan SPBE adalah proses penilaian secara sistematis melalui verifikasi informasi terhadap hasil penilaian mandiri untuk mengukur tingkat kematangan penerapan SPBE. Sebelumnya sudah dilakukan evaluasi SPBE pada instansi XYZ di tahun 2019 dan 2021 dan yang dimana hasilnya masuk ke dalam kategori Baik dengan nilai 3,19 pada tahun 2019 dan nilai 3,33 pada tahun 2021. Penurunan nilai ini dipengaruhi dengan adanya penambahan domain manajemen SPBE dan Audit TIK. Penambahan domain tersebut tercantum dalam Permen PANRB No. 5 Tahun 2020[5]. Berikut merupakan rincian evaluasi SPBE pada tahun 2021 sebagai berikut[6]:

Tabel 1. Hasil Evaluasi tahun 2021

No	Nama Indeks	Nilai
1	Kebijakan Internal terkait Tata Kelola SPBE	3,00
Domain Kebijakan SPBE		3,00
2	Perencanaan Strategis SPBE	2,75
3	Teknologi Informasi dan Komunikasi	3,75
4	Penyelenggara SPBE	3,50
Domain Tata Kelola SPBE		3,30
5	Penerapan Manajemen SPBE	2,13
6	Audit TIK	2.33
Domain Manajemen SPBE		2,18
7	Layanan Administrasi Pemerintahan Berbasis Elektronik	3,70
8	Layanan Publik Berbasi Elektronik	3,33
Domain Layanan SPBE		3,55
INDEKS SPBE		**3,19**

Dari hasil penelitian Indeks SPBE Instansi XYZ bisa dilihat hanya pada domain manajemen SPBE saja yang masih berada pada predikat (cukup). Hal ini menandakan bahwa Instansi XYZ belum mampu menerapkan manajemen SPBE sebagaimana yang disebutkan dalam Permen PANRB Nomor 59 Tahun 2020.

Tabel 2. Predikat Indeks SPBE

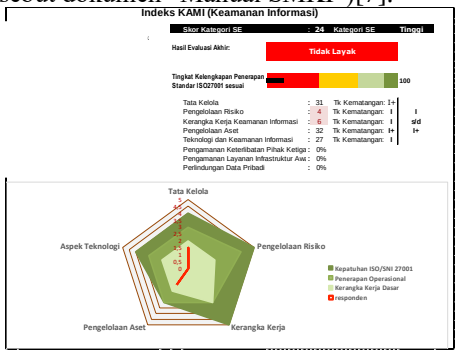
No	Nilai Indeks	Predikat
1	4,2 – 5,0	Memuaskan
2	3,5 - < 4,2	Sangat Baik
3	2,6 - < 3,5	Baik
4	1,8 - < 2,6	Cukup
5	<1,8	Kurang

Instansi XYZ memiliki banyak sistem yang diperuntukkan kepada masyarakat, guna mempermudah dan dapat menjangkau semua lapisan masyarakat. Untuk mengakses sistem-sistem tersebut tentunya diperlukan data-data

pribadi pendukung lainnya untuk mempermudah akses terhadap sistem tersebut seperti nama, alamat, NIK dan informasi lainnya yang bersifat pribadi lainnya. Selaku instansi yang bertugas untuk menampung, mengelola dan memproses data-data pribadi dari masyarakat, tentunya informasi tersebut bersifat sangat penting untuk dijaga bagi Instansi XYZ.

Contoh usaha/upaya dalam meningkatkan kualitas manajemen keamanan informasi yang dapat dilakukan oleh Instansi XYZ adalah dengan mengevaluasi tingkat kesiapan dan kelengkapan dari manajemen keamanan informasi menggunakan parameter Indeks KAMI. Hal ini termuat di dalam Peraturan BSSN Nomor 8 Tahun 2021. Hasil dari evaluasi atau pengukuran akan menghasilkan tingkat kematangan atau kesiapan manajemen keamanan informasi dari Instansi XYZ yang dimana nantinya, akan digunakan sebagai acuan untuk meningkatkan manajemen keamanan informasi pada SPBE.

Evaluasi menggunakan parameter atau *tools* indeks KAMI dilakukan pada evaluasi tahun 2022, dimana dari hasil evaluasi tersebut disimpulkan bahwa tingkat kematangan SPBE dalam lingkup manajemen keamanan informasi masih berada dalam level 1 (rintisan). Hal ini berarti Instansi XYZ sebagai penyelenggara SPBE belum menerapkan secara keseluruhan dari proses SMKI. Berdasarkan dari temuan tersebut, maka diperlukan penyusunan dan penetapan dokumen terkait SMKI guna menjadi pedoman penyelenggaraan Manajemen Keamanan Informasi (umumnya disebut dokumen "Manual SMKI")[7].



Gambar 1. Tingkat Kematangan SPBE Menggunakan *Tools* Indeks KAMI

SMKI sendiri merupakan proses yang disusun berdasarkan tahapan perencanaan, implementasi, cek evaluasi, dan meningkatkan terhadap keamanan informasi perusahaan atau yang lebih dikenal dengan metode PDCA (*Plan*, *Do*, *Check*, *Action*). Dengan disusunnya pedoman SMKI tersebut, diharapkan Instansi XYZ dapat melindungi proses bisnis, meminimalisir akibat dari insiden teknologi informasi, dapat mengelola dan mengurangi risiko keamanan informasi, serta menghindari kegagalan serius. Oleh karena itu, peneliti mengajukan judul skripsi "Evaluasi dan Rekomendasi Pedoman Sistem Manajemen Keamanan Sistem Informasi (SMKI) SPBE pada Instansi XYZ".

TINJAUAN PUSTAKA

Keamanan Informasi

Keamanan informasi merupakan suatu upaya melindungi, menjaga, mengamankan informasi beserta aset serupa dari ancaman yang mungkin terjadi sehingga dapat membahayakan informasi dan aset serupa lainnya, contohnya seperti informasi yang disalahgunakan oleh oknum yang tidak memiliki hak akses. Keamanan informasi sendiri menjadi salah satu aspek penting dalam usaha melindungi informasi beserta aset serupa bagi suatu usaha maupun organisasi. Berikut merupakan tiga aspek penting dari keamanan informasi [8], antara lain:

1. *Condentiality* (Kerahasiaan), aspek kerahasiaan informasi atau aset serupa dan memastikan hanya dapat diakses oleh orang yang berwenang.
2. *Integrity* (Integritas), Aspek yang menjamin bahwa informasi atau aset serupa tidak dirubah tanpa ijin dan sepengetahuan dari pihak yang berwenang
3. *Availability* (Ketersediaan), Aspek yang menjamin informasi atau aset serupa akan tersedia ketika dibutuhkan.

Sistem Manajemen Keamanan Informasi (SMKI)

SMKI merupakan kumpulan kebijakan/prosedur/susunan proses yang dibuat berdasarkan pendekatan risiko bisnis untuk mengelola data/informasi milik suatu

organisasi atau bisnis secara sistematis[9][10]. Tujuan dari penerapan SMKI pada suatu bisnis atau organisasi adalah untuk menjamin kelangsungan bisnis dan mengurangi risiko maupun ancaman untuk meminimalkan dari dampak pelanggaran keamanan informasi[10][11]. SMKI dapat menghasilkan prosedur keamanan informasi, manual keamanan informasi, instruksi dan formulir keamanan informasi dari penerapannya[12].

Audit Sistem Informasi

Secara umum audit merupakan kegiatan atau proses pengumpulan dan penilaian terhadap informasi sebagai satu kesatuan organisasi/instansi/perusahaan oleh para ahli[13]. Audit sistem informasi merupakan cara/aktivitas pengujian atau evaluasi bukti-bukti untuk mengetahui mampu atau tidaknya sistem dalam melindungi aset, menjaga integritas data, mendeteksi risiko dan efek potensial yang timbul , serta membantu mencapai tujuan organisasi atau perusahaan[12][13].

Dalam program audit, kontrol sistem informasi dikelompokkan ke dalam empat kategori umum[13], yakni: kontrol lingkungan, kontrol keamanan fisik, kontrol keamanan logis, *IS Operation Control.*

Indeks KAMI

Indeks Keamanan Informasi (KAMI) merupakan sebuah *tools* yang membantu dalam evaluasi pengamanan informasi dari segi tingkat kematangan dan kesiapan pengamanan informasi pada lembaga pemerintahan. Selain itu, Indeks KAMI juga bisa digunakan untuk menganalisis kesesuaian/kelengkapan aspek dari penerapan ISO 27001[10][15]. Indeks KAMI tidak diperuntukkan menganalisis efektivitas maupun kelayakan dari pengamanan informasi yang ada, namun sebagai *tools* yang memberikan bayangan mengenai kesiapan yang melingkupi kelengkapan dan kematangan kerangka kerja keamanan informasi kepada pimpinan terkait[16].

Evaluasi atau penilaian dalam Indeks KAMI dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pengaman yang termasuk di dalam standar ISO 27001[16], yang disusun menjadi 5 target antara lain: tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, teknologi dan keamanan informasi serta suplemen.

Tabel 3. Area Evaluasi Indeks KAMI

No	Area	Bagian yang Dievaluasi
1	Tata Kelola	Kesiapan bentuk tata kelola keamanan informasi beserta instansi, tugas dan tanggung jawab pengelola informasi.
2	Pengelola Risiko Keamanan Informasi	Kesiapan penerapan pengelola risiko keamanan sebagai dasar penerapan strategi keamanan informasi.
3	Kerangka Kerja Pengelolaan Keamanan Informasi	Kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
4	Pengelolaan Aset Informasi	Kelengkapan pengamanan aset informasi termasuk siklus penggunaan aset tersebut.
5	Teknologi dan Keamanan Informasi	Kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Dalam penilaian ini, pertanyaan akan dikelompokkan menjadi 2 keperluan yaitu keperluan kelengkapan dan kematangan. Dari penilaian kelengkapan, pemimpin perusahaan atau instansi terkait dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Sedangkan dari penilaian kematangan, nantinya akan digunakan sebagai media pelaporan pemetaan dan peningkatan kesiapan keamanan informasi dari suatu organisasi.

Untuk keperluan kematangan Indeks KAMI, tingkat kematangan didefinisikan sebagai berikut:

Tabel 4. Tingkatan Indeks KAMI

No	Tingkatan	Keterangan
1	Tingkat I	Kondisi awal
2	Tingkat II	Penerapan kerangka kerja dasar
3	Tingkat III	Terdefinisi dan konsisten
4	Tingkat IV	Terkelola dan Terukur
5	Tingkat V	Optimal

Untuk membantu memberikan uraian yang lebih spesifik, tingkatan diatas ditambahkan dengan tingkatan antara I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkat kematangan. Hasil penilaian tersebut akan divisualisasikan ke dalam bentuk diagram jaring laba-laba (*spider chart*).

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

Metode *Plan-Do-Check-Action* (PDCA) 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[17].

Manajemen Keamanan Informasi SPBE

Sistem Pemerintahan Berbasis Elektronik atau SPBE merupakan penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan SPBE. Manajemen keamanan informasi SPBE dilaksanakan oleh setiap instansi Pusat dan Pemerintahan Daerah berdasarkan pedoman manajemen keamanan informasi SPBE yang tertuang pada Peraturan BSSN No 4 Tahun 2021. Dalam pelaksanaan keamanan informasi SPBE terdapat area-area yang diprioritaskan oleh organisasi, dimana di antaranya:

1. Data dan informasi SPBE;
2. Aplikasi SPBE;
3. Aset infrastruktur SPBE;
4. Kebijakan keamanan informasi SPBE yang telah dimiliki.

Dalam upaya menjaga atau meningkatkan keamanan SPBE, hal yang dapat dilakukan adalah dengan menerapkan standar dan prosedur keamanan SPBE serta menguji keamanan dari aplikasi SPBE itu sendiri. Standar teknis dan prosedur keamanan aplikasi diterapkan pada aplikasi berbasis web dan *mobile*.

METODE PENELITIAN

Penelitian ini menggunakan metode *Plan*, *Do*, *Check*, *Action* (PDCA) pada tahap evaluasi Manajemen Keamanan Informasi dalam lingkup Sistem Manajemen Keamanan Informasi (SMKI).

Instrumen Penelitian

Adapun instrumen-instrumen yang digunakan dalam penelitian ini adalah:

1. Observasi
   Peneliti melakukan observasi yaitu dengan pengamatan langsung pada Instansi XYZ untuk mendapatkan informasi mengenai Sistem Manajemen Keamanan Informasi di Instansi XYZ.
2. Wawancara
   Pada tahapan wawancara ini peneliti gunakan untuk mendapat informasi mengenai penyelenggaraan sistem manajemen keamanan informasi yang diterapkan pada Instansi XYZ.
3. Pengumpulan Bukti
   Tahapan pengumpulan bukti peneliti lakukan untuk memenuhi penilaian dalam evaluasi indeks KAMI. Dimana pengumpulan bukti tersebut dilakukan pada Instansi XYZ terkait dengan pelaksanaan Sistem Manajemen Keamanan Sistem Informasi (SMKI).

Jenis dan Sumber Data

Penelitian ini menggunakan jenis data kuantitatif dan kualitatif, yang dimana data kuantitatif diperoleh dari hasil analisis Indeks KAMI dan data kualitatif diperoleh dari hasil wawancara dan pengumpulan dokumen-dokumen yang ada. Begitu pun dengan sumber data yang digunakan merupakan data primer terkait dengan penyelenggaraan SPBE pada Instansi XYZ serta data sekunder yang diperoleh dari studi literatur.

Alur Penelitian

Adapun proses dari alur penelitian di atas dapat dijabarkan sebagai berikut:

1. Identifikasi Masalah
   Langkah pertama yang dilakukan adalah perumusan masalah. Proses ini, dilakukan dengan cara observasi terkait penerapan sistem manajemen keamanan informasi pada Instansi XYZ. Berdasarkan hasil evaluasi tingkat kematangan proses SPBE Instansi XYZ dari sebelumnya,

dimana tingkat kematangannya dinyatakan “Tidak Layak". Oleh karena itu, peneliti memutuskan untuk melakukan evaluasi ulang pada lingkup keamanan informasi guna menghasilkan panduan penyusunan Sistem Manajemen Keamanan Informasi (SMKI).

2. Studi Literatur

   Pada proses ini, dilakukan pencarian informasi yang relevan dengan penelitian ini dari penelitian terkait sebelumnya. Penelitian terkait yang dikumpulkan berupa buku, jurnal, artikel maupun dokumentasi terkait yang dapat dijadikan landasan teori serta keilmuan yang baik. Hal ini bertujuan untuk menunjang keberhasilan penelitian seperti dalam halnya pemilihan metode penelitian.

3. Penerapan PDCA

   Dalam penelitian ini, peneliti membuat langkah-langkah dalam mengadopsi Metode PDCA , yang dijabarkan sebagai berikut:

   a.*Plan*

   1) Observasi

      Peneliti secara langsung melakukan observasi di Instansi XYZ untuk melihat bagaimana penerapan dari manajemen keamanan informasi yang ada. Tahapan ini dimulai pada bulan September 2022. Dari kegiatan tersebut, adapun data yang didapatkan adalah dokumen terkait dari penerapan keamanan informasi pada Instansi XYZ.

   2) Wawancara

      Kegiatan bertujuan untuk mengetahui sejauh mana penerapan dari keamanan informasi yang diterapkan pada Instansi XYZ. Wawancara ini dilakukan dengan cara melakukan sesi tanya jawab kepada beberapa staf terkait dari Instansi XYZ.

   3) Penentuan Ruang Lingkup

      Penentuan ruang lingkup pada penelitian ini meliputi bagian-bagian pengendalian dalam SMKI.

   b. *Do*

      Pada tahapan ini, peneliti melakukan pengumpulan bukti terkait penelitian. Tahapan ini dilakukan untuk mendapatkan bukti nyata berupa dokumen mengenai penerapan keamanan informasi pada Instansi XYZ. Pengumpulan bukti terkait mengikuti indikator penerapan dalam lingkup SMKI.

   c. *Check*

      Selanjutnya, pada tahap ini peneliti melakukan penilaian/evaluasi terhadap keamanan informasi pada Instansi XYZmenggunakan *tools* Indeks KAMI.

   d. *Action*

      Pada tahap ini, peneliti memberikan rekomendasi yang digunakan untuk meningkatkan tingkat kematangan dari keamanan informasi Instansi XYZ.

4. Kesimpulan

   Kesimpulan yang diberikan berupa dokumentasi mengenai tahapan yang telah dilakukan sebelumnya. Dimana kesimpulan tersebut dapat dijadikan acuan dan referensi penerapan manajemen keamanan informasi yang telah diteliti. Selain itu, pada tahapan ini juga memuat saran terkait peningkatan kematangan manajemen keamanan informasi Instansi XYZ.

HASIL DAN PEMBAHASAN

Penilaian Keamanan Informasi

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

Dari hasil penilaian pada lima kategori keamanan informasi, didapatkan bahwa kategori sistem elektronik Instansi XYZ mendapatkan nilai **27** dengan tingkat ketergantungan **Tinggi**. Hal ini mengindikasi bahwa sistem elektronik yang dikelola oleh Instansi XYZ memiliki nilai investasi cenderung tinggi, dengan tingkat klasifikasi

informasi dan dampak dari kegagalan sistem elektronik berada pada level medium-tinggi.

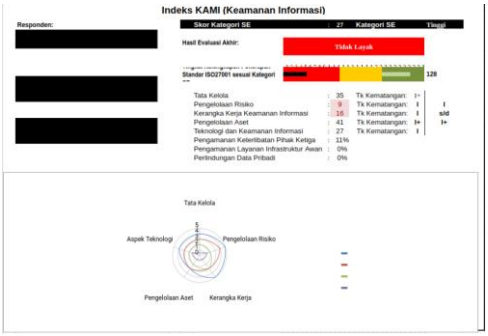
Dari segi tata kelola keamanan informasi, Instansi XYZ belum secara menyeluruh menerapkan kesiapan dalam hal tata kelola, tugas, dan tanggung jawab terhadap sistem elektronik yang dikelola. Hal ini didasarkan pada nilai evaluasi tata kelola yang berada pada nilai **35** dengan tingkat kematangan **I+** atau masih pada kondisi awal. Hal ini sangat disayangkan karena dalam pengembangan dan manajemen keamanan informasi dari sebuah elektronik, tata kelola merupakan landasan dari terbentuknya sistem elektronik itu sendiri.

Pengelolaan risiko keamanan informasi dalam sistem elektronik yang dikelola oleh Instansi XYZ mendapat nilai **9** dengan tingkat kematangan **I**. Instansi XYZ sendiri belum secara penuh melakukan perencanaan terhadap pengelolaan risiko hingga langkah-langkah mitigasi terhadap risiko yang ada. Hal ini tentu membutuhkan perhatian khusus, karena nilai investasi dari sistem elektronik yang dikelola oleh Instansi XYZ cenderung tinggi, yang dimana bertolak belakang dengan bagaimana Instansi XYZ mengelola proses risiko keamanan informasi yang terdapat pada sistem elektronik tersebut.

Dalam pengelolaan kerangka kerja keamanan informasi, Instansi XYZ masih belum secara menyeluruh menerapkan kebijakan dan prosedur keamanan informasi. Hal ini ditandai dengan masih tidak dilakukannya mekanisme pengelolaan dokumen dan prosedur keamanan informasi. Selain itu, dalam proses audit yang dilaksanakan oleh pihak internal atau pihak independen, Instansi XYZ baru hanya menerapkan secara sebagian dan belum secara menyeluruh. Oleh karena itu, pada pengelolaan kerangka kerja pengelolaan keamanan informasi, Instansi XYZ mendapat nilai **16** degan tingkat kematangan **I**.

Pengelolaan aset informasi yang dilakukan oleh Instansi XYZ secara keseluruhan belum diterapkan secara maksimal. Berdasarkan kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset yang digunakan oleh Instansi XYZ, mendapatkan nilai **41** dengan tingkat kematangan **I+**. Hal ini mengindikasikan bahwa Instansi XYZ masih secara umum merencanakan prosedur terhadap pengelolaan aset informasi.

Penggunaan teknologi dalam pengamanan aset informasi dalam penyelenggaraan SPBE yang dilaksanakan oleh Instansi XYZ secara keseluruhan belum dilakukan. Secara detail, Instansi XYZ sudah menerapkan layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan. Namun, *logging* atau pencatatan riwayat dari penggunaan teknologi tersebut belum dilakukan sama sekali. Pembatasan pengguna hingga waktu pengamanan teknologi belum diterapkan secara menyeluruh. Oleh karena itu, Instansi XYZ mendapatkan nilai **27** dengan tingkat kematangan **I**.



Gambar 2. Hasil Indeks KAMI pada Instansi XYZ

Secara keseluruhan, penyelenggaraan manajemen keamanan informasi yang dilaksanakan oleh Instansi XYZ mendapatkan nilai **128**, dengan hasil evaluasi akhir **Tidak Layak**. Hal ini menggambarkan bahwa penyelenggaraan SPBE yang dilaksanakan oleh Instansi XYZ belum memiliki kesiapan akan pengamanan informasi yang berjalan.

Rekomendasi Pedoman SMKI

Dalam penyelenggaraan SPBE dalam lingkup manajemen keamanan informasi yang dilakukan oleh Instansi XYZ, tentu membutuhkan sebuah pedoman baku. Dengan semakin meningkatnya risiko dan insiden keamanan informasi dalam penyelenggaraan sistem elektronik, upaya pengamanan terhadap

sistem elektronik yang memiliki data dan informasi strategis dan penting harus segera dilakukan.

Sehubungan dengan hal tersebut, dalam rangka keamanan data dan informasi di lingkungan Instansi XYZ, perlu menyusun sebuah standar tentang manajemen keamanan informasi, yang mengatur bagaimana informasi menjadi aman agar kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga.

Sebagai bentuk rekomendasi yang dapat diberikan terhadap penerapan manajemen keamanan informasi khususnya dalam penyelenggaraan SPBE yang dilakukan oleh Instansi XYZ, serta menyesuaikan terhadap hasil dari penilaian keamanan informasi dengan indeks KAMI, maka rekomendasi yang dapat diberikan adalah berupa dokumen pedoman Sistem Manajemen Keamanan Informasi (SMKI) yang dibagi menjadi 11 bagian.

1. Bagian I Pengendalian Umum

   Pada bagian ini, kebijakan dan standar SMKI digunakan sebagai pedoman dalam rangka melindungi aset informasi Instansi XYZ dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Instansi XYZ yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi agar selalu terjaga dan terpelihara dengan baik.

2. Bagian II Pengendalian Organisasi Keamanan Informasi

   Pada bagian ini, memberikan pedoman dalam membentuk tim keamanan informasi yang bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkungan Instansi XYZ termasuk hubungan dengan pihak luar.

3. Bagian III Pengendalian Pengelolaan Aset Informasi

   Pada bagian ini, memberikan pedoman dalam mengelola aset informasi di lingkungan Instansi XYZ untuk melindungi dan menjamin keamanan aset informasi.

4. Bagian IV Pengendalian Keamanan Sumber Daya Manusia

   Pada bagian ini, memastikan bahwa seluruh pegawai dan pihak ketiga di lingkungan Instansi XYZ memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi, serta mengetahui proses terkait keamanan informasi.

5. Bagian V Pengendalian Keamanan Fisik dan Lingkungan

   Pada bagian ini, mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan pada perangkat pengolah informasi serta gangguan pada aktivitas organisasi.

6. Bagian VI Pengendalian Pengelolaan Komunikasi dan Operasional

   Pada bagian ini, memastikan komunikasi dan operasional yang aman dan benar pada perangkat pengolah informasi, mengimplementasikan dan memelihara keamanan informasi, mengelola layanan yang diberikan pihak ketiga, meminimalkan risiko kegagalan, melindungi keutuhan dan ketersediaan informasi dan perangkat lunak, memastikan keamanan pertukaran informasi dan pemantauan terhadap proses operasional.

7. Bagian VII Pengendalian Kontrol Akses

   Pada bagian ini, memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi khususnya perangkat pengolah informasi.

8. Bagian VIII Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi

   Pada bagian ini, memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

9. Bagian IX Pengendalian Pengelolaan Gangguan Keamanan Informasi

   Pada bagian ini, memastikan kejadian dan kelemahan keamanan informasi yang terhubung, dengan sistem informasi

dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

10. Bagian X Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan

Pada bagian ini, melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

11. Bagian XI Pengendalian Kepatuhan

Pada bagian ini, bertujuan untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

SIMPULAN

Penerapan manajemen keamanan informasi pada sistem elektronik yang dikelola oleh Instansi XYZ berada pada level **Tidak Layak**. Nilai kategori sistem elektronik Instansi XYZ yang tinggi berbanding terbalik dengan penyelenggaraan manajemen keamanan informasi yang telah berjalan yang masih berada pada tingkat **I** sampai **I+**.

Untuk dapat menyesuaikan dengan nilai kategori sistem elektronik yang dimiliki, Instansi XYZ perlu menyusun pedoman Sistem Manajemen Keamanan Informasi (SMKI) sebagai sebuah panduan baku dalam penyelenggaraan sistem elektronik.

Pedoman SMKI digunakan sebagai acuan dasar penyelenggaraan sistem elektronik. Mulai dari tahapan tata kelola sebagai bentuk tanggung jawab penyelenggaraan sistem elektronik, pengelolaan risiko sebagai bentuk mitigasi terhadap berbagai ancaman yang muncul terhadap penyelenggaraan elektronik, penyusunan kebijakan dan prosedur, pengelolaan aset dan teknologi dalam jalannya sistem elektronik, hingga efektivitas terhadap penggunaan teknologi pada sistem elektronik yang berjalan pada penyelenggaraan SPBE oleh Instansi XYZ.

DAFTAR PUSTAKA

[1] Y. Novita, Y. Nurhadryani, and S. Wahjuni, "Analisis Penerapan Teknologi Informasi Dalam Mendukung Pengembangan Local E-Government Analysis of the Application of Information Technology in Supporting Local E-Government Development," *J. Penelit. Pos dan Inform.*, vol. 11, no. 1, pp. 1–19, 2021, doi: 10.17933/jppi.2021.110101.

[2] R. A. Nugroho and Y. Purbokusumo, "E-Government Readiness: Penilaian Kesiapan Aktor Utama Penerapan E-Government di Indonesia E-Government Readiness: Main Actor Readiness Assessment for E-Government Application in Indonesia," *Iptek-Kom*, vol. 22, no. 1, pp. 1–17, 2020, [Online]. Available: http://dx.doi.org/10.33164/iptekkom.22.1.2020.1-17.

[3] Khaidarmansyah and R. Saifuddin, "Optimalisasi Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Provinsi Lampung," *Deriv. J. Manaj.*, vol. 16, no. 1, pp. 85–95, 2022.

[4] D. G. A. Atmaja, I. G. P. Krisna Juliharta, and K. Q. Fredlina, "Penilaian Tingkat Keamanan Teknologi Informasi Menggunakan Metode Keamanan Informasi (KAMI) Dan Vulnerability Assessment," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 2, p. 173, 2020, doi: 10.35889/jutisi.v9i2.523.

[5] I. G. Putu, K. Juliharta, and I. P. C. Taruna, "Evaluasi keamanan sistem pemerintahan berbasis elektronik di kota xyz," pp. 210–221.

[6] Deputi Bidang Kelembagaan dan Tata Laksana Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, "Laporan Hasil Evaluasi Sistem Pemerintahan Berbasis Elektronik Pemerintah Kota Denpasar Tahun 2021," 2021.

[7] I. dan S. K. D. Dinas Komunikasi, "Laporan Audit TIK Pemerintah Kota Denpasar 2022," *Dinas Komunikasi, Inf. dan Stat. Kota Denpasar*, p. 29, 2022.

[8] A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

[9] T. Hartati, "Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001: 2013," *KOPERTIP J. Ilm. Manaj. Inform. dan Komput.*, vol. 1, no. 2, pp. 63–70, 2017, doi: 10.32485/kopertip.v1i02.24.

[10] B. A. Firzah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Berdasarkan Iso / Iec 27001 : 2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (Dptsi) Its Surabaya Evaluating Information Security Management Using Ind," vol. 6, no. 1, 2017.

[11] D. Rahmat, "Informasi Menggunakan Standar Sni Iso / Iec 27001 : 2013," vol. 06, pp. 37–41, 2019.

[12] S. R. Musyarofah and R. Bisma, "Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah," *Teknologi*, vol. 11, no. 1, pp. 1–15, 2021, doi: 10.26594/teknologi.v11i1.2152.

[13] G. A. Hanindito, "Analisis dan Audit Sistem Manajemen Keamanan Informasi (SMKI) pada Instansi Perpustakaan dan Arsip Daerah Kota Salatiga," *J. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 2, pp. 279–284, 2017, doi: 10.25077/teknosi.v3i2.2017.279-284.

[14] Y. C. Pradipta, Y. Rahardja, M. N. N. Sitokdana, U. Kristen, and S. Wacana, "Teknologi Informasi Dan Komunikasi Penerbangan Dan Antariksa (Pustikpan) Menggunakan Sni Iso / Iec 27001 : 2013," pp. 352–358, 2013.

[15] M. Siga, T. D. Susanto, and B. C. Hidayanto, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur," *Semin. Nas. Sist. Inf. Indones.*, no. 479, pp. 478–483, 2014.

[16] M. F. Husin, H. . Wowor, and S. D. . Karouw, "Implementasi Indeks Kami Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 12, no. 1, 2017.

[17] W. Apriandari and A. Sasongko, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Sni Iso / Iec 27001 : 2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus : Di Diskominfo Kota Sukabumi)," *Ilmiah SANTIKA*, vol. 8, no. 1. pp. 715–729, 2018.