EVALUASI PENILAIAN MANDIRI PENERAPAN SMKI DI SALAH SATU LINGKUNGAN K/L

Irwan Suryono

Program Studi S2 Teknologi Informasi Universitas Pamulang
Jl. Raya Puspitek No.46, Buaran, Serpong 15310
isusaja@gmail.com

Abstract

In the context of managing the information security management system (SMKI), ministries/agencies (K/L) have committed to participate in maintaining the confidentiality and security of information on all data managed in each K/L so that aspects of confidentiality, integrity, and availability of All and information assets belonging to the company from threats from internal and external parties can be properly maintained. The existence of the Perpim, Perkom, and SMKI policies as information security management system (SMKI) policies and standards within the K/L environment makes them a guideline to protect confidential data and information belonging to the Institution from various forms of threats both from within and outside the K/L environment. Furthermore, the most important thing in the implementation of an information security management system is to evaluate the implementation of the ISMS, which is termed monitor and review. Evaluation is needed to guarantee the implementation of the ISMS so that the selected security control system can protect data and information from various risks and provide confidence in the level of security for the institution. Evaluation in this study was carried out using the ISMS self-assessment evaluation tool which is a derivative of the KAMI Index tool. This tool is used to measure the implementation of ISMS within the Institution. Evaluation is carried out on various areas that are the target of implementing information security with a scope of discussion that also meets all security aspects defined by the ISO/IEC 27001:2005 standard. The results of this study are evaluations to obtain an assessment of the understanding and implementation of IT security management, determine the maturity level of information technology security management and obtain recommendations on the results of information security management analysis.
Keywords*: evaluation, information security, KAMI Index, ISO 27001, ISMS*

Abstrak

Dalam rangka mengelola sistem manajemen keamanan informasi (SMKI), di kementerian/lembaga (K/L) sudah berkomitmen ikut menjaga kerahasian dan keamanan informasi seluruh data yang di kelola di masing-masing K/L sehingga aspek kerahasiaan, integritas, dan ketersediaan dari seluruh dan aset informasi milik perusahaan dari ancaman dari pihak internal maupun eksternal dapat terjaga dengan baik. Hadirnya Perpim, Perkom, dan kebijakan SMKI sebagai kebijakan dan standar sistem manajemen keamanan informasi (SMKI) di lingkungan K/L menjadikannya sebagai pedoman dalam rangka melindungi data dan informasi rahasia milik Lembaga dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan K/L. Selanjutnya hal yang paling penting di dalam pelaksanaan implementasi sistem manajemen keamanan informasi adalah melakukan evaluasi terhadap pelaksanaan SMKI yang diistilahkan monitor and review. Evaluasi diperlukan dalam rangka menjamin pelaksanaan SMKI agar kontrol sistem keamanan yang dipilih mampu melindungi data dan informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi institusi. Evaluasi pada penelitian ini dilakukan dengan menggunakan tool evaluasi SMKI penilaian mandiri yang merupakan turunan dari tool Indeks KAMI. Tool ini digunakan untuk mengukur penerapan SMKI di lingkungan Lembaga. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC

27001:2005. Hasil dari penelitian ini adalah evaluasi untuk mendapatkan penilaian mengenai pemahaman dan penerapan pengelolaan keamanan TI, mengetahui tingkat kematangan pengelolaan keamanan teknologi informasi dan mendapatkan rekomendasi atas hasil analisis pengelolaan keamanan informasi.
Kata kunci: evaluasi, keamanan informasi, indeks KAMI, ISO 27001, SMKI

I. PENDAHULUAN

Hadirnya Peraturan Pimpinan mengenai system manajemen keamanan informasi selain memperkuat fungsi manajemen risiko, kebijakan ini juga merupakan wujud pelaksanaan rencana strategis analisis regulasi standar manajemen yang Digunakan Lembaga dalam Penentuan Strategi Peningkatan serta Implementasi Manajemen Risiko dan Implementasi Sistem Manajemen Keamanan Informasi (SMKI) (p.48, hal 63) yang tertuang di dalam IT Blueprint Tahun 2020-2024 terkait perencanaan implementasi arsitektur (architecture implementation planning) di area "kebijakan pengelolaan keamanan di organisasi pemerintah" .

Hal yang paling penting di dalam pelaksanaan SMKI adalah melakukan evaluasi terhadap pelaksanaan dan penerapan SMKI yang diistilahkan *monitoring and review of ISMS (secara terus menerus)*. Dalam siklus PDCA (Plan-Do-Check-Action) atau biasa juga di kenal dengan internal audit check, evaluasi penerapan SMKI ini merepresentasikan proses *Check*. Dalam perkembangannya, evaluasi pengelolaan keamanan informasi bagi penyelenggara pelayanan didasarkan pada Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik dengan alat evaluasi berupa penggunaan Indeks Keamanan Informasi (Indeks KAMI). Tujuan utamanya adalah membandingkan seberapa jauh persyaratan klausul-klausul ISO 27001 terkait keamanan informasi telah dipenuhi, baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun aspek penerapannya.

Tujuan dari evaluasi penerapan SMKI ini selain sebagai tindak lanjut dari nota dinas (280/PID.00/30-32/10/2022) yang diturunkan dari Tim Inspektorat, adalah untuk mendapatkan penilaian mengenai pengelolaan keamanan TI di lingkungan Lembaga, mengetahui tingkat pemahaman dan kematangan pengelolaan keamanan TI dan mendapatkan rekomendasi berdasarkan hasil analisis pengelolaan keamanan informasi pada Lembaga Awdx.

Analisis hasil survei akan menentukan apakah kuisioner ini dapat digunakan dalam memaksimalkan peran dan tugas Komite SMKI untuk membantu pencapaian tujuan institusi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien pada tahun berikutnya dan secara berkelanjutan.

Landasan Teori

SMKI merupakan suatu framework atau kerangka kerja kebijakan dan prosedur untuk mengelola data sensitif organisasi secara sistematis, umumnya kita mengenal dengan istilah sistem manajemen pengelolaan keamanan yang bertujuan mencegah dan melindungi sistem informasi dari tindakan ilegal.

Informasi di sini harus kita anggap aset harus dilindungi keamanannya. Dan informasi bisa dikatakan aman jika terpenuhinya 3 elemen dasar keamanan informasi yaitu confidentiality, integrity, dan availability.

Sebagai dasar survei dan alat evaluasi penilaian mandiri dalam penerapan dan pelaksanaan keamanan informasi, sudah dilaksanakan 2 (dua) kegiatan yang berkaitan dengan penerapan SMKI di Lembaga.

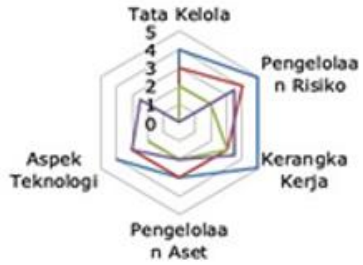
a) Indeks Keamanan Informasi

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan snapshot indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya. Untuk implementasinya, indeks KAMI meliputi VII (tujuh) area, sebagai berikut:

1. Kategori Sistem Elektronik, terkait dengan evaluasi tingkat atau kategori sistem elektronik yang digunakan.
2. Tata Kelola Keamanan Informasi, terkait dengan evaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
3. Pengelolaan Risiko Keamanan Informasi, terkait dengan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
4. Kerangka Kerja Pengelolaan Keamanan Informasi, terkait dengan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya
5. Pengelolaan Aset Informasi, terkait dengan evaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.
6. Teknologi dan Keamanan Informasi, terkait dengan evaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.
7. Suplemen, terkait dengan evaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Dari tujuh area tersebut, hanya lima area yang di ukur tingkat kematangannya untuk tindakan evaluasi selanjutnya yaitu Tata Kelola, Pengelolaan Risiko (manajemen risiko), Kerangka Kerja (kebijakan, pedoman, prosedur), Pengelolaan Aset TI, dan Aspek Teknologi.



Gambar 1. Diagram hasil penilaian Indeks Kami

Hasil keseluruhan terhadap lima area indeks KAMI ditampilkan pada diagram jaring laba-laba skor Indeks KAMI di bawah ini:

- Level kepatuhan paling signifikan di dapat pada area *Pengelolaan Aset* karena di anggap telah melampaui atau memenuhi bagian Kerangka Kerja Dasar atau Tingkat Kematangan III.
- Pada area *Pengelolaan Risiko dan Teknologi* dinyatakan butuh peningkatan karena jawaban responden terhadap Kerangka Kerja hanya pada Tingkat Kematangan II.
- Untuk menuju pada jaring Kepatuhan ISO 27001/SNI yang lebih baik maka Direktorat Manajemen Informasi harus memperhatikan semua area baik aspek kerangka kerja dasar, konsistensi penerapan dan tindakan peningkatan kinerja keamanan.

Langkah-langkah perbaikan pengelolaan keamanan informasi unit Direktorat Manajemen Informasi diantaranya :

1. Melaksanakan dan menerapkan semua kebijakan dan prosedur keamanan informasi pada semua area pengamanan.
2. Memonitoring segala aktivitas teknologi informasi meliputi kinerja pegawai, kinerja hardware, kinerja software, dan pengimplementasian penerapan regulasi terkait pengelolaan keamanan informasi.
3. Mengevaluasi setiap penerapan kebijakan dan prosedur terkait keamanan informasi untuk menilai efektifitas dan efisiensi kinerja terhadap segala aktivitas teknologi informasi.

b) Assessment Cyber Security Maturity (CSM)

CSM merupakan instrumen yang dikembangkan oleh BSSN untuk menilai tingkat kematangan keamanan Siber bagi organisasi, mengidentifikasi GAP antara kondisi pengelolaan keamanan siber saat ini dengan kondisi ideal, dimana outputnya berupa nilai maturitas keamanan siber organisasi beserta laporan yang memuat penjelasan.

Hasil pengisian dalam dokumen ini menggambarkan kondisi pengelolaan siber yang saat ini terjadi pada institusi responden.

Untuk implementasinya, pengisian tool CSM meliputi V (lima) area, sebagai berikut:

1. Tata Kelola, terkait dengan Aspek tata kelola terdiri dari sub aspek kesadaran, audit, kontrol, pemenuhan, kebijakan, dan proses.
2. Identifikasi, terkait dengan Aspek identifikasi terdiri dari sub aspek manajemen aset, inventaris,

manajemen risiko, prioritas, pelaporan, dan klasifikasi.
3. Proteksi, tekait dengan Aspek proteksi terdiri dari sub aspek jaringan, aplikasi, pengguna, manajemen identitas dan akses, cloud, dan data.
4. Deteksi, terkait dengan Aspek deteksi terdiri dari sub aspek perubahan, monitor, peringatan, pemberitahuan, intelijen, dan pelaporan.
5. Respon, terkait dengan Aspek respon terdiri dari penahanan, penanggulangan, pemulihan, Kegiatan Paska Insiden, dan pelaporan.

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
3,60		3,75		3,70		3,82		3,22	
Kesadaran	3,24	Manajemen Aset	3,25	Jaringan	4,00	Perubahan	2,00	Penahanan	3,50
Audit	3,67	Inventaris	3,80	Aplikasi	3,60	Monitor	4,36	Penanggulangan	4,60
Kontrol	4,09	Manajemen Risiko	4,00	Pengguna	3,89	Peringatan	4,38	Pemulihan	3,00
Pemenuhan	3,11	Prioritas	3,80	Manajemen Identitas dan Aset	4,15	Pemberitahuan	5,00	Kegiatan Paska Insiden	2,00
Kebijakan	3,60	Pelaporan	3,67	Cloud	2,86	Intelijen	4,18	Pelaporan	3,00
Proses	3,93	Klasifikasi	4,00	Data	3,71	Pelaporan	3,00		

Tabel 1 , Akumulasi dari hasil penilaian Cyber Security maturity

Berdasarkan penilaian instrumen CSM tersebut diperoleh bahwa: **Total Score Indeks Kematangan: 3.62**

Dengan demikian, secara kualitatif dapat digambarkan bahwa penerapan keamanan siber prosesnya sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat formal, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini dapatterukur dengan baik.

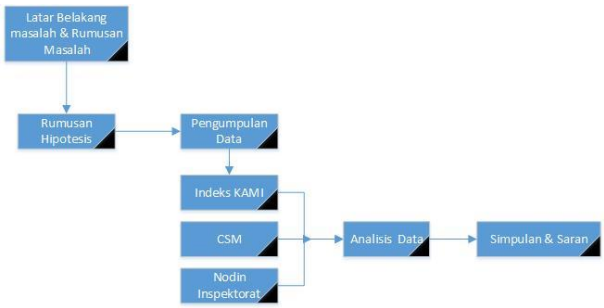
II. METODE PENELITIAN

Metode yang digunakan adalah mengumpulkan, menggolongkan, dan menganalisis data yang berupa angka untuk mendapatkan informasi dalam mengukur pemahaman struktur dan implementasi SMKI. Metode ini merupakan metode kuantitatif survei berangkat dari permasalahan, yang terdiri atas latar belakang masalah, identifikasi masalah, dan rumusan masalah. Permasalahan tersebut selanjutnya dijelaskan dan dijawab dengan teori.

Bagian yang diukur meliputi :

1. Pemahaman SMKI yang terdiri dari 3 komponen (kepemimpinan, perencanaan, informasi terdokumentasi).
2. Pengendalian SMKI yang terdiri dari 4 komponen (Kebijakan Keamanan Informasi, Pengendalian Akses, Keamanan Fisik dan Lingkungan, Keamanan Operasi).
3. Pemahaman mengenai struktur dan peran dalam SMKI yang terdiri dari 2 komponen (Struktur Organisasi, Tugas dan Tanggung Jawab.

Metodologi pekerjaan survei ini secara garis besar terdiri atas tahapan-tahapan berikut.



Gambar 2. Alur proses evaluasi, alur ini bisa didesain sesuai kebijakan di lembaga masing-masing.

III. HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas mengenai hasil perbandingan penilaian aspek kepatuhan, hasil kondisi peran TIK, dan hasil status kesiapan keamanan informasi di internal Lembaga.

a) *Penentuan Skoring*

Penentuan dan perhitungan skoring pada survei ini tidak berpedoman pada aturan tertentu karena pertanyaan pada kuisioner merupakan persyaratan pemahaman yang dipilih berdasarkan kebutuhan untuk pengukuran secara garis besar saja.

Rumus penilaian skoring menggunakan fungsi perhitungan statistik, nilai dihasilkan dari perhitungan berapa jumlah responden yang menjawab “tidak” dan “ya”. Kriteria nilai pemahamam mengenai SMKI sebagai berikut :

1. Angka 0% – 19,99% = Kurang sekali
2. Angka 20% – 39,99% = Kurang
3. Angka 40% – 59,99% = Cukup
4. Angka 60% – 79,99% = Baik
5. Angka 80% – 100% = Sangat Baik

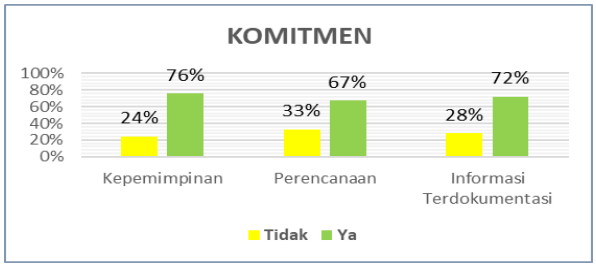
Deskripsi pilihan :
"tidak" : apakah menurut responden penerapan persyaratan/pengendalian belum memenuhi.
"ya" : artinya apakah menurut responden Persyaratan/pengendalian telah dijalankan.

b) *Penilaian Aspek Kepemimpinan*
Penilaian Aspek Kepemimpinan dilakukan secara garis besar dengan menganalisis isian item pertanyaan pada Tool KAMI, item isian berdasarkan kondisi eksisting.
Sasaran Penilaian Aspek Kepemimpinan:
1. Pemahaman dalam penerapan komitmen keamananan informasi yang didukung oleh atasan pad unit kerja di Kedeputian Inda. (ada peran CISO dalam penerapan SMKI)
2. Pemahaman pihak-pihak yang berkepentingan, dan menentukan risiko dan peluang yang perlu ditangani.
3. Pemahaman dan kesadaran dalam mengelola aset informasi organisasi yang terdokumentasi.

Penghitungan komparasi sederhana *self assestment* (penilaian secara personal) dengan jawaban "tidak" atau "ya" dapat terlihat sebagai berikut:

No Klausul	Persyaratan	Tidak	Ya	Capaian
1	Kepemimpinan & Komitmen	24%	76%	88%
2	Perencanaan	33%	67%	83%
3	Informasi Terdokumentasi	28%	72%	86%

Tabel 2.hasil penilaiaan pada aspek komitmen



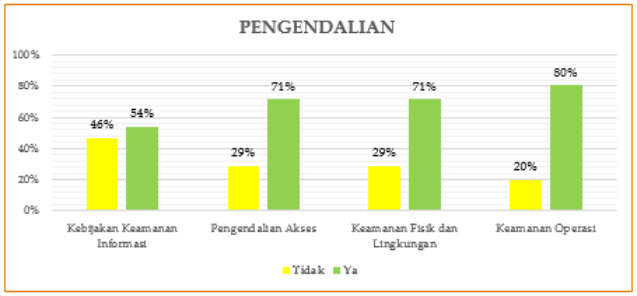
Gambar persentase hasil penilaian pada aspek komitmen

- Perhitungan nilai persentase di dapat dengan membandingkan antara nilai jawaban responden yaitu tidak dengan ya, nilai rata-rata yang dihasilkan adalah **86%** (sangat baik).
- Nilai pemahaman responden dengan jawaban "ya" cenderung lebih tinggi. Selanjutnya perlu dilakukan proses penilaian assessment aspek masing-masing komponen secara rinci untuk mengetahui apakah isian responden sesuai dengan ketersediaan bukti atau tidak.
- Pada penilaian komponen **perencanaan** jawaban responden memiliki nilai **67%** artinya dari sisi identifikasi dan perencanaan penanganan risiko masih menjadi komponen yang harus di maksimalkan.
- Hasil perbandingan tersebut menjelaskan mengenai kondisi pemahaman pegawai terhadap kepemimpinana & komitmen, perencanaan, dan informasi terdokumentasi sudah baik namun perlu kegiatan lanjutan untuk assessment secara rinci.

c) *Penilaian Aspek Pengendalian*
Komponen dari penilaian Aspek Pengendalian antara lain pemahaman mengenai kebijakan, kondisi pengendalian akses, keamanan fisik, dan penerapan prosedur keamanaan. Item isian berdasarkan kondisi eksisting.
Sasaran Penilaian Aspek Pengendalian :
1. Pemahaman responden mengenai kebijakan keamanaan informasi.
2. Pemahaman pembatasan akses terhadap informasi dan fasilitas pemrosesan informasi.
3. Pemahaman rule keamanan yang diterapkan dalam mencegah akses fisik yang tidak sah, kerusakan, dan gangguan ke organisasi akibat impact dari insiden.
4. Pemahaman mengenai Prosedur dan tanggung jawab operasional.

No Seksi	Kendali	Tidak	Ya	Capaian
1	Kebijakan Keamanan Informasi	46%	54%	77%
2	Pengendalian Akses	29%	71%	86%
3	Keamanan Fisik dan Lingkungan	29%	71%	86%
4	Keamanan Operasi	20%	80%	90%

Tabel 3. Penilaian Aspek Pengendalian



Grafik persentase hasil pengendalian

- Perhitungan nilai persentase di dapat dengan membandingkan antara nilai jawaban responden

yaitu tidak dengan ya, nilai rata-rata yang dihasilkan adalah **85%** (sangat baik).

- Nilai pemahaman responden dengan jawaban "ya" cenderung lebih tinggi. Selanjutnya perlu dilakukan proses penilaian assessment aspek masing-masing komponen secara rinci untuk mengetahui apakah isian responden sesuai dengan ketersediaan bukti atau tidak.
- Hasil perbandingan tersebut menjelaskan mengenai kondisi pemahaman pegawai terhadap kebijakan keamanan informasi, pengendalian akses, keamnaan fisik dan lingkungan, dan keamanan operasional sudah baik namun perlu kegiatan lanjutan untuk assessment secara rinci.

d) *Penilaian Aspek Peran Tugas di Struktur OKI*

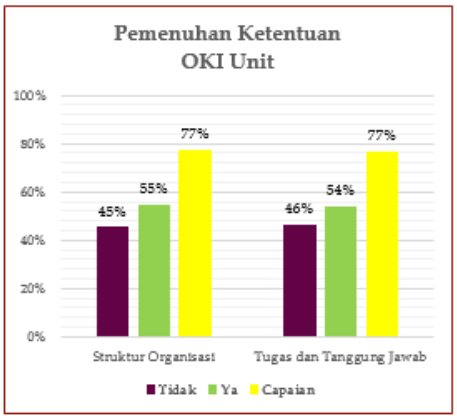
Komponen dari penilaian aspek organisasi keamanan informasi unit kerja antara lain pemahaman mengenai peran dan tugas pada struktur keamanan informasi. Item isian berdasarkan kondisi eksisting.

Sasaran Penilaian Aspek Organisasi Keamanan Informasi :

1. Mengukur pemahaman peran dan tugas CISO menurut struktur OKI pada perpim SMKI no 4 tahun 2018
2. Mengukur pemahaman tugas dan tanggung jawab PIC unit menurut struktur OKI pada perpim SMKI no 4 tahun 2018

No	Seksi	Kendali	Tidak	Ya	Capaian
1		Struktur Organisasi	45%	55%	77%
2		Tugas dan Tanggung Jawab	46%	54%	77%

Tabel 2.hasil penilaiaan pada aspek komitmen



Grafik persentase hasil persentase OKI

- Perhitungan nilai persentase di dapat dengan membandingkan antara nilai jawaban responden yaitu tidak dengan ya, nilai rata-rata yang dihasilkan adalah **77%** (baik).
- Perlu peningkatan pada komponen penilaian peran tugas pada struktur keamanan informasi, mengingat nilai pada komponen ini masuk area cukup yakni **55% dan 54%** → (Cukup).
- Nilai pemahaman responden dengan jawaban "ya" cenderung lebih tinggi namun sedikit. Sehingga sangat perlu dilakukan proses penilaian assessment aspek masing-masing komponen secara rinci untuk mengetahui apakah isian responden sesuai dengan ketersediaan bukti atau tidak.
- Hasil perbandingan tersebut menjelaskan mengenai kondisi pemahaman pegawai terhadap fungsi struktur Organisasi Keamanan Informasi sudah baik secara rata-rata namun perlu assessment ulang dan kegiatan lanjutan untuk assessment secara rinci.

IV. KESIMPULAN

Pada bagian ini menjelaskan kesimpulan dan saran untuk pengelolaan keamanan informasi di Lembaga.

Kesimpulan

a) Nilai rata-rata hasil kuisioner

Hasil penilaian persentase kuisioner dari 3 aspek , hasilnya masuk dalam kategori baik

1. Aspek Kepemimpinanan **(86%) → Sangat Baik**
2. Aspek Pengendalian Keamanan Informasi **(85%) → Baik**
3. Aspek Organisasi Keamanan Informasi Unit **(77%) → Baik** *dengan catatan*

b) Komponen yang memiliki kinerja baik

Empat komponen yang memiliki indeks kinerja terbaik adalah:

1. Aspek kepemimpinan
   a) Pemahaman definisi SMKI **(89%)**
   b) Pengelolaan pengamanan asset informasi **(82%)**
2. Aspek pengendalian
   a) SOP di unit kerja sudah terdokumentasi **(80%)**
3. Aspek Organisasi Keamanan Informasi Unit
   a) Perlu adanya peran PIC/Pejabat/Pelaksana di masing-masing unit kerja **(80%)**

c) Komponen yang perlu di evaluasi

Sedangkan **tiga komponen** yang merupakan bagian dari aspek yang perlu di evaluasi adalah:

1. Aspek pengendalian
   a) Perkom klasifikasi keamanan akses arsip dinamis **(54%)** dan;
   b) Perpim Sistem Manajemen Keamanan Informasi **(54%)**

2. Aspek Organisasi Keamanaan Informasi
   a) Peran, tugas dan tanggung jawab komite SMKI **(41% dan 38%)**
   b) Kegiatan sosialisasi security awareness **(38%)**

V. SARAN

a) Saran pada area pengendalian

Kesimpulan yang dapat diambil secara menyeluruh dari hasil penilaian survei pemahaman SMKI antara lain :

a.1. Perlu dilakukan pembahasan pada level OKI, khususnya forum komite SMKI untuk melakukan evaluasi beberapa komponen pada aspek pengendalian dan aspek organisasi keamanan informasi.

a.2. Kegiatan penilaian atau evaluasi harus dilakukan berkelanjutan minimal setahun sekali sebagai bentuk kontrol system manajemen.

b) Saran pada area organisasi keamanan informasi unit.

b1. Perlu adanya pembahasan pada forum komite SMKI mengenai strategi sosialiasi yang dapat menjangkau seluruh pegawai KOMISI.

b2. Perlu adanya pembahasan pada forum komite SMKI mengenai strategi sosialiasi Peraturan Pimpinan tekait Keamanan Informasi.

b3. Peran serta dan dukungan komite SMKI dalam penyusunan revisi Perpim SMKI.

b4. Perlu adanya pembahasan pada forum komite SMKI mengenai pengaktifkan kembali Komite SMKI.

VI. UCAPAN TERIMA KASIH

Alhamdulillah, puji dan syukur saya panjatkan kepada Tuhan yang maha esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan penulisan jurnal ini, tak lupa saya ucapan terima kasih kepada pihak-pihak di instansi K/L tempat saya bekerja yang telah membantu terlaksananya kegiatan evaluasi implementasi SMKI, hingga bisa saya tuangka juga menjadi tulisan artikel ini, semoga artikel jurnal ini bisa membawa manfaat bagi semuanya.

VII. DAFTAR PUSTAKA

[1] PDCA: An Implementation Guide to ISO 27001:2013. (2020, december 8). Retrieved from bestpractice.biz: https://bestpractice.biz/pdca-an-implementation-guide-to-iso-270012013/

[2] CEC. (2018). Perpim No.4 tentang Sistem Manajemen Keamanan Informasi.

[3] Dutton, J. (2021, August 23). What is an Information Security Management System. Retrieved from itgovernanceusa: https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2

[4] Kominfo. (2020, January 31). Sistem Manajemen Pengamanan Informasi (SMPI). Retrieved from https://aptika.kominfo.go.id/2020/01/sistem-manajemen-pengamanan-informasi-smpi/

[5] RI, P. n. (2020). Kebijakan dan standar Sistem Manajemen Keamanan Informasi. Retrieved from https://jdih.perpusnas.go.id/file_peraturan/Kebijakan_dan_Standar_SMKI.pd