EVALUASI TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI

MENGGUNAKAN INDEKS KAMI VERSI 4.1

DI LINGKUNGAN DINAS KOMUNIKASI DAN INFORMATIKA

KABUPATEN BANTUL

NO. 555/00583

DISKOMINFO KABUPATEN BANTUL

TAHUN 2022

DASAR HUKUM

1. Undang-Undang No.19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Pasal 15 ayat 1 bahwa setiap Penyelengaran Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap operasinya Sistem Elektronik sebagaimana mestinya;
2. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mendefinisikan ketentuan yang harus dipenuhi sebagai Penyelenggara Sistem Elektronik;
3. Peraturan Presiden No. 95 Tahun 2018 tentang SPBE bahwa Manajemen Keamanan Informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko Keamanan Informasi;
4. Peraturan Menteri Dalam Negeri No. 18 dan 23 Tahun 2020 dan No. 48 Tahun 2021 tentang perencanaan pembinaan dan pengawasan penyelenggarahan pemerintahan daerah;
5. Peraturan Badan BSSN No. 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik.

PENDAHULUAN

Berdasarkan Peraturan Presiden No.71 Tahun 2019 [2] Penyelenggara Sistem Elektronik Wajib menyediakan Sistem Pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan dan kerugian. Ketenuan lebih lanjut mengenai Sistem Pengamanan sebagaimana diatur dalam peraturan kepala lembaga yang melaksanakan urusan pemerintahan di bidang keamanan siber. Lembaga yang dimaksud adalah Badan Siber dan Sandi Negara (BSSN), yang telah mengeluarkan Peraturan Badan BSSN No. 8 Tahun 2020 [5] tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik. Sistem ini yang kemudian dikenal dengan Sistem Manajemen Keamanan Informasi (SMKI).

Sistem Manajemen Keamanan Informasi (SMKI) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan meninjau ulang (*Check*) serta memelihara dan meningkatkan atau mengembangkan (*Act*) terhadap keamanan informasi perusahaan.

Tujuan penerapan Sistem Manajemen Keamanan Informasi (SMKI) adalah untuk menjaga:

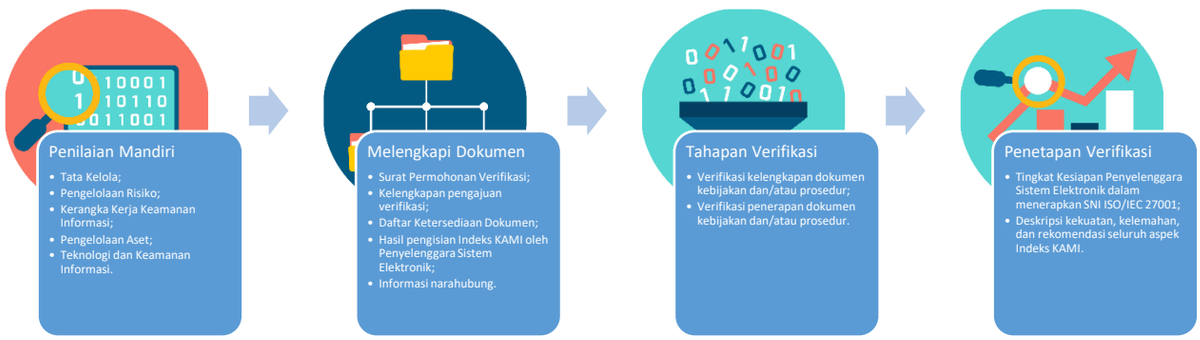
1. Kerahasiaan (*Confidentiality*), menjamin bahwa hanya mereka yang memiliki hak yang dapat mengakses informasi tertentu;
2. Integritas (*Integrity*), menjamin kelengkapan informasi dan menjaga kerusakan atau ancaman yang mengakibatkan berubah informasi dari aslinya;

3. Ketersediaan (*Availibity*), memastikan bahwa pengguna yang berwenang memiliki akses ke informasi tanpa adanya gangguan/ hambatan.

Dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI), Badan Siber dan Sandi Negara (BSSN) menyediakan alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi dalam instansi, yaitu Indeks KAMI. Indeks KAMI memberikan gambaran kondisi kesiapan kerangka kerja pengamanan informasi kepada pimpinan instansi terhadap penerapan SNI/ISO IEC 27001. Indeks KAMI juga sebagai sarana untuk meningkatkan kesadaran Keamanan Informasi dan peningkatan kesiapan Sistem Manajemen Keamanan Informasi (SMKI). Indeks KAMI hendaknya digunakan secara rutin dan berkala sebagai alat dalam melakukan tinjauan ulang kesiapaan Keamanan Informasi sekaligus mengukur keberhasilan inisiatif yang diterapkan.

Di lingkungan Pemerintah Kabupaten Bantul, penilaian mandiri menggunakan alat evaluasi Indeks KAMI telah dilakukan pada Februari 2021 dan Februari 2022 dengan menggunakan Indeks KAMI versi 4.1 yang dirilis pada November 2019 oleh Badan Siber dan Sandi Negara (BSSN).

Peraturan Badan BSSN No 8 dan 9 Tahun 2021 menjelaskan tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 menggunakan Indeks KAMI sebagai berikut :



Gambar 1. Tahapan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001:2013 menggunakan Indeks KAMI

Untuk saat ini, Dinas Komunikasi dan Informatika Kabupaten Bantul masih dalam tahapan Penilaian Mandiri yang telah dilakukan selama 2 (dua) periode, yaitu pada tahun 2021 dan 2022 di bulan Februari.

METODOLOGI PENILAIAN MANDIRI

Penilaian Mandiri yang dilaksanakan oleh Dinas Komunikasi dan Informatika Kabupaten Bantul menggunakan Alat Evaluasi yaitu Indeks KAMI versi 4.1 yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) pada bulan November tahun 2019. Penilaian Mandiri dilakukan

secara berkala pada Bulan Februari dan telah dilaksanakan selama 2 (dua) periode, yaitu tahun 2021 dan 2022.

Ruang Lingkup penilaian mandiri Indeks KAMI pada Dinas Komunikasi dan Informatika Kabupaten Bantul meliputi Pengelolaan Data Center dan layanan pendukungnya.

Penilaian Mandiri dilaksanakan oleh tim auditor internal sebagai berikut :

Tabel 1. Tim Auditor Internal

No	Jabatan Dalam Instansi	Jabatan dalam Tim
1.	Kepala Diskominfo Kab. Bantul	Ketua Tim Audit Internal
2.	Kepala Bidang Teknologi Informasi Keamanan Informasi dan Persandian Diskominfo Kab. Bantul	Sekretaris Tim Audit Internal
3.	Subkoordinator Kelompok Substansi Keamanan Informasi dan Persandian Diskominfo Kab. Bantul	Anggota Tim Audit Internal
4.	Staf Kelompok Substansi Keamanan Informasi dan Persandian Diskominfo Kab. Bantul	Anggota Tim Audit Internal

Adapun beberapa responden yang menjadi sumber dari pengukuran tata kelola Teknologi Informasi adalah :

Tabel 2. Responden Audit Indeks KAMI

No	Jabatan Dalam Instansi
1.	Kepala Diskominfo Kab. Bantul
2.	Sekretariat Diskominfo Kab. Bantul beserta staf
3.	Kepala Bidang Teknologi Informasi Keamanan Informasi dan Persandian Diskominfo Kab. Bantul beserta staf
4.	Kepala Bidang Bidang Tata Kelola E-Goverment, Aplikasi Informatika dan Statistik Diskominfo Kab. Bantul beserta staf

HASIL DAN PEMBAHASAN

Pada Indeks KAMI, bagian pertama dilakukan identifikasi kategori atas sistem elektronik yang hendak dinilai. Pengkategorian ini nantinya terkorelasi dengan Status Kesiapan/Kematangan penerapan Sistem Manajemen Keamanan Informasi (SMKI). Hasil identifikasi kategori Sistem Elektronik Dinas Komunikasi dan Informatika Kabupaten Bantul mendapatkan nilai **29 (Dua Puluh Sembilan)** sehingga masuk dalam Kategori Sistem Elektronik **Tinggi**, dengan rincian sebagai berikut :

Tabel 2 - Bagian I : Kategori Sistem Elektronik

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**
#	**Karakteristik Instansi/Perusahaan**	
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	C
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	B
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	A
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	B

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**
#	**Karakteristik Instansi/Perusahaan**	
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	A
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	C
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	A
	Skor penetapan Kategori Sistem Elektronik	**29**

Tingkat Ketergantungan **Tinggi**

Kemudian pada Bagian II : Tata Kelola Keamanan Informasi diperoleh skor **120 (Seratus Dua Puluh),** dengan rincian sebagai berikut :

Tabel 3 - Bagian II : Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Fungsi/Organisasi Keamanan Informasi**		
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Diterapkan Secara Menyeluruh	3
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Diterapkan Secara Menyeluruh	3
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Diterapkan Secara Menyeluruh	3
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh	3
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Diterapkan Secara Menyeluruh	6

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Fungsi/Organisasi Keamanan Informasi**		
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Diterapkan Secara Menyeluruh	6
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Diterapkan Secara Menyeluruh	6
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Diterapkan Secara Menyeluruh	6
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Diterapkan Secara Menyeluruh	6
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Diterapkan Secara Menyeluruh	6
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Diterapkan Secara Menyeluruh	6
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Diterapkan Secara Menyeluruh	9
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Diterapkan Secara Menyeluruh	9
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Diterapkan Secara Menyeluruh	9
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Diterapkan Secara Menyeluruh	9
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Dalam Perencanaan	3
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Diterapkan Secara Menyeluruh	9
			Total Nilai Evaluasi Tata Kelola	**120**	

Jumlah pertanyaan Tahap 1	8
Jumlah pertanyaan Tahap 2	8
Jumlah pertanyaan Tahap 3	6
Batas Skor Min untuk Skor Tahap Penerapan 3	48
Total Skor Tahap Penerapan 1 & 2	72
Status Peniliaian Tahap Penerapan 3	Valid
Skor Tingkat Kematangan II	54
Skor Minimum Tingkat Kematangan II	*12*
Skor Pencapaian Tingkat Kematangan II	*36*
Status	II
Skor Tingkat Kematangan III	18
Validitas Tingkat Kematangan III	Yes
Skor Minimum Tingkat Kematangan III	8
Skor Pencapaian Tingkat Kematangan III	14
Status	III
Skor Tingkat Kematangan IV	48
Validitas Tingkat Kematangan IV	Yes
Skor Minimum Tingkat Kematangan IV	24
Skor Pencapaian Tingkat Kematangan IV	54
Status	III+

Pada Bagian III : Pengelolaan Risiko Keamanan Informasi diperoleh skor **63 (Enam Puluh Tiga**), dengan rincian sebagai berikut :

Tabel 4 - Bagian III : Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Kajian Risiko Keamanan Informasi**		
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Diterapkan Secara Menyeluruh	3
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian	2
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Penerapan / Diterapkan Sebagian	2
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian	2
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Penerapan / Diterapkan Sebagian	2
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Penerapan / Diterapkan Sebagian	4
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Diterapkan Secara Menyeluruh	6
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Diterapkan Secara Menyeluruh	6
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Diterapkan Secara Menyeluruh	6
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Diterapkan Secara Menyeluruh	9
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Diterapkan Secara Menyeluruh	9
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**63**	

Jumlah pertanyaan Tahap 1	10
Jumlah pertanyaan Tahap 2	4
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	36
Total Skor Tahap Penerapan 1 & 2	45
Status Peniliaian Tahap Penerapan 3	Valid
Skor Tingkat Kematangan II	23
Skor Minimum Tingkat Kematangan II	14
Skor Pencapaian Tingkat Kematangan II	20
Status	II
Skor Tingkat Kematangan III	10
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	4
Skor Pencapaian Tingkat Kematangan III	8
Status	No
Skor Tingkat Kematangan IV	12
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	8
Skor Pencapaian Tingkat Kematangan IV	12
Status	No
Skor Tingkat Kematangan V	18
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18
Status	No

Pada Bagian IV : Kerangka Kerja Pengelolaan Keamanan Informasi diperoleh skor **140 (Seratus Empat Puluh),** dengan rincian sebagai berikut :

Tabel 5 - Bagian IV : Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**		
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Diterapkan Secara Menyeluruh	3
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Diterapkan Secara Menyeluruh	3
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Diterapkan Secara Menyeluruh	3
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Diterapkan Secara Menyeluruh	3
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	Diterapkan Secara Menyeluruh	3
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh	3
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Diterapkan Secara Menyeluruh	6
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	Dalam Penerapan / Diterapkan Sebagian	4
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Diterapkan Secara Menyeluruh	6
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Diterapkan Secara Menyeluruh	6
4.12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Diterapkan Secara Menyeluruh	6
4.13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Diterapkan Secara Menyeluruh	6
4.14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Diterapkan Secara Menyeluruh	6
4.15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Diterapkan Secara Menyeluruh	6
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Diterapkan Secara Menyeluruh	9
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Penerapan / Diterapkan Sebagian	6
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Penerapan / Diterapkan Sebagian	6
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan / Diterapkan Sebagian	6
#			**Pengelolaan Strategi dan Program Keamanan Informasi**		
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Diterapkan Secara Menyeluruh	3
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian	2
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh	3
4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Diterapkan Secara Menyeluruh	3
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Diterapkan Secara Menyeluruh	3
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Diterapkan Secara Menyeluruh	6
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Diterapkan Secara Menyeluruh	6
4.27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian	6

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**		
4.28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Dalam Penerapan / Diterapkan Sebagian	6
4.29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Diterapkan Secara Menyeluruh	9
			Total Nilai Evaluasi Kerangka Kerja	**140**	

Jumlah pertanyaan Tahap 1	12
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	7
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	92

Pada Bagian V : Pengelolaan Aset Informasi diperoleh skor **117 (Seratus Tujuh Belas)**, dengan rincian sebagai berikut :

Tabel 6 - Bagian V : Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	3
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Diterapkan Secara Menyeluruh	3
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Diterapkan Secara Menyeluruh	3
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Dalam Penerapan / Diterapkan Sebagian	2
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	2
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
5.8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dalam Penerapan / Diterapkan Sebagian	2
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Diterapkan Secara Menyeluruh	3
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Dalam Perencanaan	1
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Dalam Penerapan / Diterapkan Sebagian	2
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Dalam Penerapan / Diterapkan Sebagian	2
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Penerapan / Diterapkan Sebagian	2
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian	2
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan / Diterapkan Sebagian	2
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian	2
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Diterapkan Secara Menyeluruh	3
5.18	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	Dalam Penerapan / Diterapkan Sebagian	2
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian	4
5.20	III	2	Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian	4
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Dalam Penerapan / Diterapkan Sebagian	4
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Penerapan / Diterapkan Sebagian	4

Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

#			**[Penilaian]** Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Penerapan / Diterapkan Sebagian	4
5.23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Dalam Perencanaan	2
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Perencanaan	2
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*- nya?	Dalam Penerapan / Diterapkan Sebagian	6
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Dalam Penerapan / Diterapkan Sebagian	6
5.27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Dalam Penerapan / Diterapkan Sebagian	6
#			**Pengamanan Fisik**		
5.28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Dalam Penerapan / Diterapkan Sebagian	2
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Dalam Penerapan / Diterapkan Sebagian	2
5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Perencanaan	1
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Dalam Penerapan / Diterapkan Sebagian	2
5.34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Dalam Penerapan / Diterapkan Sebagian	4
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian	4
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Diterapkan Secara Menyeluruh	6
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Dalam Penerapan / Diterapkan Sebagian	4
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Pengelolaan Aset	**117**	

Jumlah pertanyaan Tahap 1	24
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	4
Batas Skor Min untuk Skor Tahap Penerapan 3	88
Total Skor Tahap Penerapan 1 & 2	91
Status Peniliaian Tahap Penerapan 3	Valid
Skor Tingkat Kematangan II	77
Skor Minimum Tingkat Kematangan II	25
Skor Pencapaian Tingkat Kematangan II	62
Status	II
Skor Tingkat Kematangan III	40
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	35
Skor Pencapaian Tingkat Kematangan III	50
Status	No

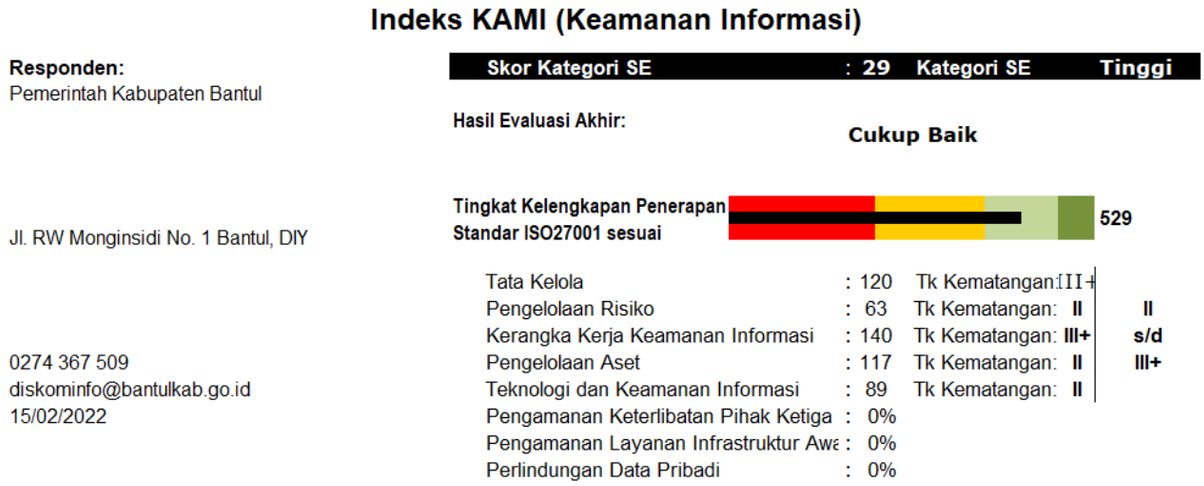
Pada Bagian VI : Teknologi dan Keamanan Informasi diperoleh skor **89 (Delapan Puluh Sembilan),** dengan rincian sebagai berikut :

Tabel 7 - Bagian VI : Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Teknologi**		
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dalam Penerapan / Diterapkan Sebagian	2
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan	1
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Dalam Penerapan / Diterapkan Sebagian	4
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Penerapan / Diterapkan Sebagian	4
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password* , mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Penerapan / Diterapkan Sebagian	4
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Dalam Penerapan / Diterapkan Sebagian	4
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts* , *lockout* setelah kegagalan *login* ,dan penarikan akses?	Dalam Penerapan / Diterapkan Sebagian	4
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Penerapan / Diterapkan Sebagian	4
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Diterapkan Secara Menyeluruh	3
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Penerapan / Diterapkan Sebagian	2
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Dalam Penerapan / Diterapkan Sebagian	4
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Diterapkan Secara Menyeluruh	6
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Dalam Penerapan / Diterapkan Sebagian	4
6.25	III	3	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Dalam Penerapan / Diterapkan Sebagian	6
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**89**	

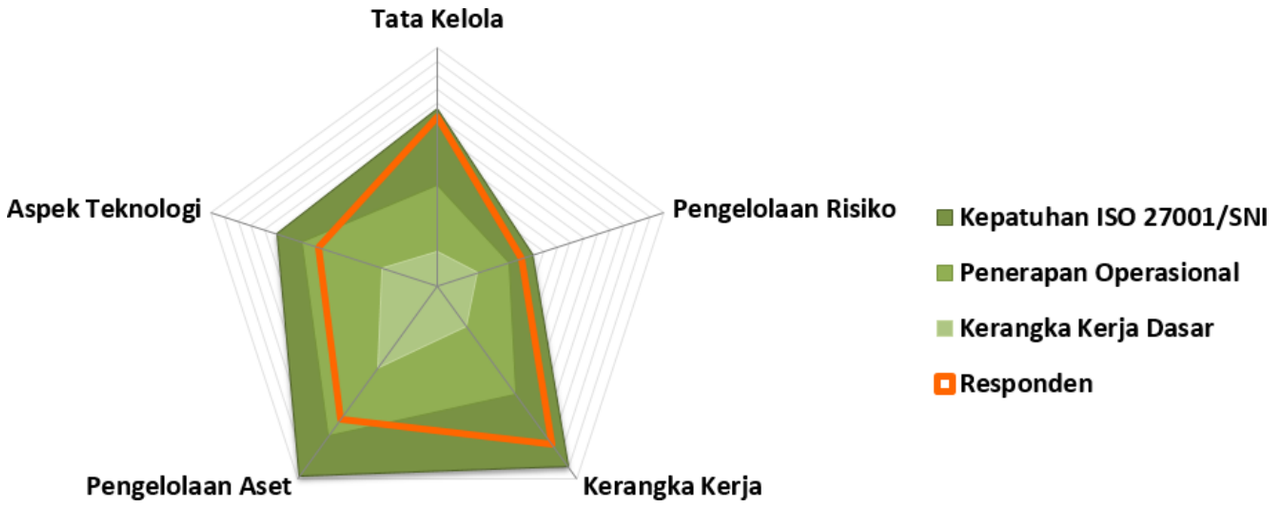
Jumlah pertanyaan Tahap 1	14
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	68
Total Skor Tahap Penerapan 1 & 2	77
Status Peniliaian Tahap Penerapan 3	Valid
Skor Tingkat Kematangan II	33
Skor Minimum Tingkat Kematangan II	18
Skor Pencapaian Tingkat Kematangan II	28
Status	II
Skor Tingkat Kematangan III	50
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	40
Skor Pencapaian Tingkat Kematangan III	62
Status	No
Skor Tingkat Kematangan IV	6
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	6
Skor Pencapaian Tingkat Kematangan IV	9
Status	No

Pada Dashboard Indeks KAMI didapatkan Skor Akhir **529 (Lima Ratus Dua Puluh Sembilan)** dengan predikat **Cukup Baik**.



Gambar 2. Skor pada Dashboard Indeks KAMI

Masih dalam halaman dashboard, terdapat diagram radar korelasi antara implementasi yang telah dilakukan responden dengan kepatuhan terhadap SNI ISO/IEC 27001, Penerapan Operasional, dan Kerangka Kerja Dasar.



Gambar 3. Diagram Radar korelasi dengan SNI ISO/IEC 27001

Terlihat bahwa pada Area Tata Kelola, Pengelolaan Risiko, dan Kerangka Kerja, penerapan Sistem Manajemen Keamanan Informasi di Dinas Komunikasi dan Informatika Kabupaten Bantul sudah mendekati kepatuhan terhadap SNI ISO/IEC 27001, namun pada aspek teknologi dan pengelolaan aset masih sangat kurang.

Kemudian, korelasinya dengan Laporan Penyelenggaraan Pemerintahan Daerah (LPPD) untuk mendapatkan nilai pada area kemananan informasi dilakukan prosentasi nilai yang didapatkan, sebagai berikut :

Tabel 8 - Rekap Penilaian Mandiri Indeks KAMI untuk pengisian LPPD

Pelaksanaan Penilaian : Februari 2022				
No	**Area Evaluasi**	**Skor**	**Maks Skor**	**Nilai**
1	Tata Kelola Keamanan Informasi	120	126	0.95
2	Pengelolaan Risiko Keamanan Informasi	63	72	0.88
3	Kerangka Kerja Pengelolaan Keamanan Informasi	140	159	0.88
4	Pengeloalaan Aset Informasi	117	168	0.70
5	Teknologi dan Keamanan Informasi	89	120	0.74
				4.15

Beberapa poin temuan yang kemudian menjadi masukan untuk perbaikan implementasi Sistem Manajemen Keamanan Informasi di Dinas Komunikasi dan Informatika Kabupaten Bantul antara lain :

1. Membentuk tim pelaksana Sistem Manajemen Keamanan Informasi dan disahkan dengan SK Kepala Dinas Komunikasi dan Informatika Kabupaten Bantul;
2. Menyusun semacam dokumen Induk/ Road Map/ Kerangka Kerja yang memuat gambaran umum Sistem Manajemen Keamanan Informasi di Dinas Komunikasi dan Informatika Kabupaten Bantul;
3. Menyusun Daftar Aset dan Manajemen Risiko yang komprehensif dan ter-*update*;
4. Menyusun dan melengkapi SOP, khususnya terkait pengelolaan Data Center;
5. Melengkapi dokumentasi pelaksanaan kegiatan, misalnya mitigasi insiden, laporan monitoring, laporan gangguan, dan lain-lain;
6. Melaksanakan evaluasi kepatuhan terhadap peraturan perundang-undangan yang berlaku terkait Sistem Manajemen Keamanan Informasi.

Bantul, 11 April 2022

Ditandatangani secara elektronik oleh:
MUJAHID AMRUDIN, S.IP
Pembina Tingkat I, IV/b
NIP. 197005111998031002