



BERITA ACARA PEMERIKSAAN DOKUMEN



Pada Hari ini Selasa s.d Kamis Tanggal 30 Oktober – 1 November Tahun 2018 bertempat di Dinas Komunikasi dan Informatika Provinsi Jawa Timur, Kami selanjutnya disebut sebagai PIHAK II :

1. DENNY SADIKIN
2. KAUTSARINA
3. M. NUR AFIF
4. SITI MASMU'AH

Telah melakukan pemeriksaan dokumen dalam rangka penerapan Indeks Keamanan Informasi untuk kepentingan Dinas Komunikasi dan Informatika Provinsi Jawa Timur

Pemeriksaan Dokumen dilakukan terhadap dokumen-dokumen berikut :

1. Kerangka Kerja dan Kebijakan SMKI Dinas Komunikasi dan Informatika Pemerintah Provinsi Jawa Timur;
2. Keputusan Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Timur Nomor 188/3467/114.4/2018 Tentang Perubahan Atas Keputusan Kepala Dinas Nomor 188/3360/114.4/2018 Tentang Struktur Organisasi Sistem Manajemen Keamanan Informasi (SMKI) Berbasis ISO 27001:2013;
3. Keputusan Gubernur Jawa Timur Nomor 188/536/KPTS/013/2018 tentang Tim Penanganan Insiden Keamanan Informasi Pemerintah Provinsi Jawa Timur (Government Computer Security Incident Response Team / GOV CSIRT) Tahun 2018;
4. Kebijakan dan Pedoman Klasifikasi dan Penanganan Informasi Versi 1.0 Nomor Dokumen 706/1/114/2018;
5. Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset Versi 1.0, Nomor Dokumen 706/2/114/2018;
6. Kebijakan dan Pedoman Instalasi Perangkat Lunak Versi 1.0 Nomor Dokumen 706/3/114/2018;
7. Kebijakan dan Pedoman Pengendalian Akses Versi 1.0 Nomor Dokumen 706/4/114/2018;
8. Kebijakan dan Pedoman Pengelolaan Insiden Keamanan Informasi Veri 1.0 Nomor 706/5/114/2018;
9. Kebijakan dan Pedoman Kepatuhan Keamanan Informasi Versi 1.0 Nomor Dokumen 706/6/114/2018;
10. Kebijakan dan Pedoman Kelangsungan Bisnis dan Keamanan Informasi Versi 1.0 Nomor Dokumen 706/7/114/2018;
11. Kebijakan dan Pedoman Manaje
12. men Perubahan Fasilitas Data Center Versi 1.0 Nomor Dokumen 706/8/114/2018;
13. Kebijakan dan Pedoman Keamanan Jaringan Versi 1.0 Nomor Dokumen 706/9/114/2018;
14. Kebijakan dan Pedoman Manajemen Kapasitas Versi 1.0 Nomor Dokumen 706/10/114/2018;
15. Kebijakan dan Pedoman Pengelolaan Data Center Versi 1.0 Nomor Dokumen 706/11/114/2018;
16. Kebijakan dan Prosedur Pengamanan Pihak Ketiga Versi 1.0 Nomor Dokumen 706/13/114/2018;
17. Buku Petunjuk Teknis dan Pemeliharaan Pembangunan Data Center Diskominfo Pemerintah Provinsi Jawa Timur Tahun 2015;
18. Peraturan Gubernur Jawa Timur Nomor 98 Tahun 2018 tentang Standar Aplikasi Bagi Perangkat Daerah di Lingkungan Pemerintah Provinsi Jawa Timur (SOP Pengembangan Aplikasi ada di Bab 4);
19. Prosedur Perencanaan Pengembangan Aplikasi Nomor PPSA.01;
20. Prosedur Analisa Kebutuhan Penggunaan Aplikasi Nomor PPSA.02;
21. Prosedur Analisa Kebutuhan Aplikasi Nomor PPSA.03;

22. Prosedur Perancangan Aplikasi Nomor PPSA.04;
23. Prosedur Pemrograman Aplikasi Nomor PPSA.05;
24. Prosedur Pengujian Aplikasi Nomor PPSA.06;
25. Prosedur Implementasi Aplikasi Nomor PPSA.07;
26. Prosedur Evaluasi Pasca Implementasi Aplikasi Nomor PPSA.08;
27. Kebijakan dan Pedoman Manajemen Risiko Sistem Manajemen Keamanan Informasi Versi 1.0.

Dokumen-dokumen tersebut diserahkan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Untuk kepentingan Penerapan Indeks Keamanan Informasi, sudah dilakukan diskusi tatap muka dengan selanjutnya disebut PIHAK I :

1. Dra. Ec. Nirmala Dewi, M.M
2. Ir. Dodong Martiar M, M.Si
3. Aulia Bahar P, S.Kom, M.ISM
4. Achmad Fadlil Chusni, S.Kom, M.MT
5. Agus Budi Sampurno, SE
6. Nofian Adi P, S.Kom, MT
7. Pondra Setiawan
8. Retno Y.W, ST, M.Med.Kom
9. Septian Fajar Arifin, A.Md

Sehubungan dengan hal tersebut, PIHAK II sepakat melakukan penjagaan kerahasiaan informasi dan/atau dokumen yakni dengan:

- 1) memperlakukan informasi dan/atau dokumen milik PIHAK I dengan hati-hati dan bijaksana agar terjamin keutuhan dokumen, terhindar dari kerusakan atau kehilangan, dan tidak memberikannya kepada PIHAK lain, mempublikasikan, atau menyebarluaskannya, sama seperti memperlakukan informasi dan/atau dokumen miliknya sendiri yang tidak ingin diberikan kepada PIHAK lain, dipublikasikan, atau disebarluaskan;
- 2) memanfaatkan informasi dan/atau dokumen milik PIHAK I sesuai tujuan diberikannya informasi dan/atau dokumen tersebut yakni hanya untuk kegiatan Pemeringkatan Indeks KAMI; dan
- 3) mengembalikan seluruh informasi dan/atau dokumen PIHAK I setelah seluruh kegiatan Pemeringkatan Indeks KAMI selesai.

Ketentuan penjagaan kerahasiaan yang dibuktikan dengan membuat surat pernyataan menjaga kerahasiaan yang merupakan lampiran yang tidak terpisahkan dari Berita Acara Pemeriksaan Informasi dan/atau Dokumen ini.

Surabaya, 1 November 2018

Narasumber Dinas Komunikasi dan Informatika Provinsi Jawa Timur

1. Dra. Ec. NIRMALA DEWI, M.M

2. IR. DODONG MARTIAR M, M.SI

3. AULIA BAHAR P, S.KOM, M.ISM

4. ACHMAD FADLIL CHUSNI, S.KOM, M.MT

5. AGUS BUDI SAMPURNO, SE

6. NOFIAN ADI P, S.KOM, MT

7. PONDRA SETIAWAN

8. RETNO Y.W, ST, M.MED.KOM

9. SEPTIAN FAJAR ARIFIN, A.MD

Assessor Indeks KAMI:

1. Assessor Utama:

DENNY SADIKIN

2. Assessor Pendamping:

KAUTSARINA

3. Observer:

M. NUR AFIF

SITI MASMU'AH

	LAPORAN VERIFIKASI INDEKS KAMI	
Instansi/Perusahaan: Dinas Komunikasi dan Informatika Provinsi Jawa Timur	Narasumber Instansi/Perusahaan: 1. Dra. EC. Nirmala Dewi, M.M 2. Ir. Dodong Martiar M, M.Si 3. Aulia Bahar P, S.Kom, MISIM 4. Achmad Fadlil Chusni, S.Kom, M.MT 5. Agus Budi Sampurno, SE 6. Nofian Adi P, S.Kom, MT 7. Pondra Setiawan 8. Retno Y.W, ST, M.Med.Kom 9. Septian Fajar Arifin, A.Md	
Unit Kerja: 1. Bidang Aplikasi Informatika Dinas Komunikasi dan Informatika Provinsi Jawa Timur 2. Bidang Infrastruktur TIK Dinas Komunikasi dan Informatika Provinsi Jawa Timur		
Alamat: Jl. A. Yani No. 242-244 Surabaya Email: kominfo@jatimprov.go.id	Tel: (031) 8294608 Fax: (031) 8294517 Pimpinan Unit Kerja: 1. Dra. Ec. Nirmala Dewi, MM 2. Ir. Dodong Martiar M, M.Si	
<p>A. <u>Ruang Lingkup:</u></p> <p>1. Instansi / Unit Kerja:</p> <ul style="list-style-type: none"> a. Bidang Aplikasi Informatika b. Bidang Infrastruktur TIK <p>2. Fungsi Kerja (berdasarkan:</p> <ul style="list-style-type: none"> a. Fungsi kerja dari Bidang Aplikasi Informatika yaitu : <ul style="list-style-type: none"> 1) Perumusan kebijakan aplikasi informatika; 2) Pengendalian mengendalikan persandian dan keamanan informasi; 3) Fasilitasi integrase pelayanan publik e-government; 4) Pelaksanaan pengembangan perangkat lunak; 5) Pelaksanaan pembinaan dan pengembangnan (Governemnt Chief Information Officer); 6) Pengordinasian kebijakan aplikasi informatika; 7) Pelaksanaan monitoring, evaluasi, dan pelaporan aplikasi informatika; dan 8) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas. 		

- b. Fungsi kerja dari Bidang Infrastruktur TIK yaitu :
- 1) Perumusan kebijakan teknis infrastruktur pemberdayaan TIK;
 - 2) Pelaksanaan kebijakan infrastruktur pemberdayaan TIK;
 - 3) Pelaksanaan pengembangan perangkat keras;
 - 4) Pengoordinasian, sinkronisasi dan fasilitasi bidang infrastruktur pemberdayaan TIK;
 - 5) Pelaksanaan DRC (*Disaster Recovery Center*) dan BCP (*Business Continuity Plan*)
 - 6) Pelaksanaan monitoring, evaluasi, dan pelaporan infrastruktur pemberdayaan TIK;
 - 7) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Dinas.

3. Lokasi:

No	Nama Lokasi	
1	Data Center	Jl. A. Yani No. 242-244, Jawa Timur
2	DRC	Batam

B. Nama /Jenis Layanan Publik:

1. Layanan Jatim Smart Provinces
2. Website Jatimprov.go.id
3. Layanan Buku Tamu Digital

C. Aset TI yang kritis:

1. Informasi:
-
2. Aplikasi:
- Jatim Smart Provinces (Smart Economy, Smart Governance, Smart Environment)
- Guestbook Jatimprov
3. Server:
- HP DL380 Gen9 8SFF CTO Server (3 buah)
4. Infrastruktur Jaringan/Network:
- ASTINET 200 Mbps
- ICON + 100 Mbps

D. DATA CENTER (DC):

(Beri keterangan apakah ruang Data Center terpisah dengan perimeter/pembatas, memiliki pengamanan fisik dan sarana pendukung, dsb)

- ADA, dalam ruangan khusus
 ADA, jadi satu dengan ruang kerja

E. DISASTER RECOVERY CENTER (DRC):

(Jika ada, jelaskan kondisi DRC: colocation di pihak ketiga atau di instansi lain termasuk pengelolaan keamanan DRC)

- ADA → Dikelola Internal Dikelola vendor (outsourced)
 TIDAK ADA

Status Ketersediaan Dokumen Kerangka Kerja Sistem Manajemen Keamanan Informasi (SMKI)				
No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
Kebijakan, Sasaran, Rencana, Standar				
1	Kebijakan Keamanan Informasi (ref. kebijakan yg disyaratkan ISO 27001)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D Terbagi menjadi 13 dokumen
2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
3	Sasaran TI / Keamanan Informasi	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
4	Organisasi TI / Keamanan Informasi (IT Steering Committee, Fungsi Keamanan TI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	T SOTK Nomor 188/3467/114.4/2018
5	Metodologi Manajemen Risiko TI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D Dokumen Kebijakan dan Pedoman Manajemen Risiko Sistem Manajemen Keamanan Informasi
6	Business Continuity Plan	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Kelangsungan Bisnis dan Keamanan Informasi
7	Klasifikasi Informasi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Ref. UU no 14 /2008 - Keterbukaan Informasi Publik. Klasifikasi informasi ada 2: Informasi PUBLIK dan "YANG DIKECUALIKAN" Dokumen Kebijakan dan Pedoman Klasifikasi dan Penanganan Informasi
8	Standar software desktop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Instalasi Perangkat Lunak
9	Metode Pengukuran Efektivitas Kontrol	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK)
10	Non Disclosure Agreement (NDA)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Prosedur Pengamanan Pihak Ketiga Dokumen

	Prosedur- Prosedur:			
1	Pengendalian Dokumen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Manajemen Kapasitas
2	Pengendalian Rekaman/Catatan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-
3	Tindakan Perbaikan & Pencegahan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Hanya Perbaikan, belum ada Pencegahan
4	Audit Internal	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-
5	Penanganan (Handling) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Klasifikasi dan Penanganan Informasi
6	Pengelolaan Media Removable & Disposal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset
7	Pengelolaan Perubahan Sistem TI (Change Control Sistem TI)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-
8	Pengelolaan Hak Akses (User Access Management)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Pengendalian Akses
9	Teleworking (Akses Remote)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Pengelolaan Insiden Keamanan Informasi
11	Pemantauan (Monitoring) Sumber Daya TI: a. Monitoring Kapasitas b. Log Penggunaan User	<input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	D (sudah disahkan oleh Kabid Aplikasi Informatika) Dokumen Kebijakan dan Pedoman Manajemen Kapasitas
12	Instalasi & Pengendalian Software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	D (Sudah disahkan oleh Kabid Infrastruktur TIK) Dokumen Kebijakan dan Pedoman Instalasi Perangkat Lunak
13	Back-up & restore (prosedur/jadwal)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Kerangka Kerja dan Kebijakan SMKI Dinas Komunikasi dan Informatika Pemerintah Provinsi Jawa Timur;
2. Keputusan Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Timur Nomor 188/3467/114.4/2018 Tentang Perubahan Atas Keputusan Kepala Dinas Nomor 188/3360/114.4/2018 Tentang Struktur Organisasi Sistem Manajemen Keamanan Informasi (SMKI) Berbasis ISO 27001:2013;
3. Keputusan Gubernur Jawa Timur Nomor 188/536/KPTS/013/2018 tentang Tim Penanganan Insiden Keamanan Informasi Pemerintah Provinsi Jawa Timur (Government Computer Security Incident Response Team / GOV CSIRT) Tahun 2018;
4. Kebijakan dan Pedoman Klasifikasi dan Penanganan Informasi Versi 1.0 Nomor Dokumen 706/1/114/2018;
5. Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset Versi 1.0, Nomor Dokumen 706/2/114/2018;
6. Kebijakan dan Pedoman Instalasi Perangkat Lunak Versi 1.0 Nomor Dokumen 706/3/114/2018;
7. Kebijakan dan Pedoman Pengendalian Akses Versi 1.0 Nomor Dokumen 706/4/114/2018;
8. Kebijakan dan Pedoman Pengelolaan Insiden Keamanan Informasi Veri 1.0 Nomor 706/5/114/2018;
9. Kebijakan dan Pedoman Kepatuhan Keamanan Informasi Versi 1.0 Nomor Dokumen 706/6/114/2018;
10. Kebijakan dan Pedoman Kelangsungan Bisnis dan Keamanan Informasi Versi 1.0 Nomor Dokumen 706/7/114/2018;
11. Kebijakan dan Pedoman Manajemen Perubahan Fasilitas Data Center Versi 1.0 Nomor Dokumen 706/8/114/2018;
12. Kebijakan dan Pedoman Keamanan Jaringan Versi 1.0 Nomor Dokumen 706/9/114/2018;
13. Kebijakan dan Pedoman Manajemen Kapasitas Versi 1.0 Nomor Dokumen 706/10/114/2018;
14. Kebijakan dan Pedoman Pengelolaan Data Center Versi 1.0 Nomor Dokumen 706/11/114/2018;
15. Kebijakan dan Prosedur Pengamanan Pihak Ketiga Versi 1.0 Nomor Dokumen 706/13/114/2018;
16. Buku Petunjuk Teknis dan Pemeliharaan Pembangunan Data Center Diskominfo Pemerintah Provinsi Jawa Timur Tahun 2015;
17. Peraturan Gubernur Jawa Timur Nomor 98 Tahun 2018 tentang Standar Aplikasi Bagi Perangkat Daerah di Lingkungan Pemerintah Provinsi Jawa Timur;
18. Prosedur Perencanaan Pengembangan Aplikasi Nomor PPSA.01;
19. Prosedur Analisa Kebutuhan Penggunaan Aplikasi Nomor PPSA.02;
20. Prosedur Analisa Kebutuhan Aplikasi Nomor PPSA.03;
21. Prosedur Perancangan Aplikasi Nomor PPSA.04;
22. Prosedur Pemrograman Aplikasi Nomor PPSA.05;
23. Prosedur Pengujian Aplikasi Nomor PPSA.06;
24. Prosedur Implementasi Aplikasi Nomor PPSA.07;
25. Prosedur Evaluasi Pasca Implementasi Aplikasi Nomor PPSA.08;
26. Kebijakan dan Pedoman Manajemen Risiko Sistem Manajemen Keamanan Informasi Versi 1.0.

Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Daftar Instansi Collocation Per September 2018
2. Laporan Keamanan Informasi Bidang Aptika Bulan Februari – Juni 2017

Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber instansi/lembaga disimpulkan sbb:

I. KONDISI UMUM:

1. Struktur organisasi satuan kerja Dinas Komunikasi dan Informatika Provinsi Jawa Timur yang diperiksa dalam ruang lingkup :
 - a. Bidang Aplikasi Informatika
 - b. Bidang Infrastruktur TIK
2. SDM pada Bidang Aplikasi Informatika terdiri dari:
 - 22 orang PNS/pegawai tetap
 - 6 orang non PNS/honorer
 SDM pada Bidang Aplikasi Informatika terdiri dari:
 - 15 orang PNS/pegawai tetap
 - 1 orang non PNS/honorer
3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Total Score Sebelum Verifikasi: N/A (ref. file Indeks KAMI sebelum Verifikasi)

Tidak ada isian Indeks KAMI hasil Self Assessment yang ditunjukkan

Total Score Setelah Verifikasi: 243 (ref. file Indeks KAMI pasca Verifikasi)

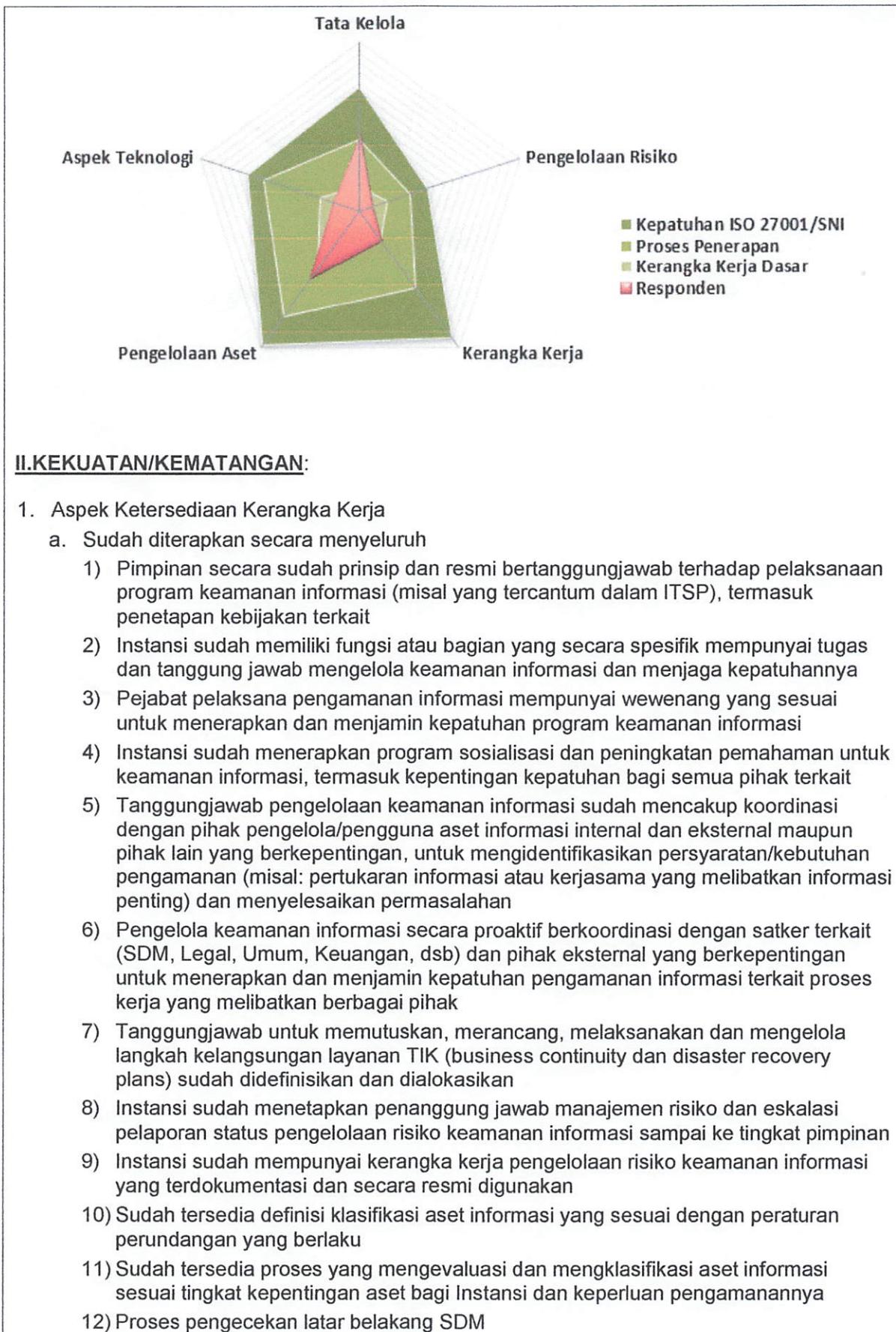
Hasil Evaluasi Akhir:

Tidak Layak

tingkat Kelengkapan Penerapan
Standar ISO27001 sesuai Kategori

243

Skor Kategori SE	:	22	Kategori SE	Tinggi
Tata Kelola	:	77	Tk Kematangan:	II
Pengelolaan Risiko	:	13	Tk Kematangan:	I
Kerangka Kerja Keamanan Informasi	:	38	Tk Kematangan:	I+
Pengelolaan Aset	:	87	Tk Kematangan:	s/d
Teknologi dan Keamanan Informasi	:	28	Tk Kematangan:	II



- 13) Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib
- 14) Prosedur penghancuran data/aset yang sudah tidak diperlukan
- b. Sudah diterapkan sebagian
- 1) Penanggung jawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi
 - 2) Peran pelaksana pengamanan informasi yang mencakup semua keperluan sudah dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan
 - 3) Sebagian pelaksana pengamanan informasi di instansi sudah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku
 - 4) Instansi sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi
 - 5) Instansi sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada
 - 6) Penanggungjawab pengelolaan keamanan informasi sudah melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi
 - 7) Sebagian kondisi dan permasalahan keamanan informasi sudah menjadi konsideran dari proses pengambilan keputusan strategis
 - 8) Pimpinan menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi
 - 9) Instansi sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya
 - 10) Instansi sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)
 - 11) Sudah mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan
 - 12) Kerangka kerja pengelolaan risiko sebagian mencakup definisi dan hubungan tingkat klasifikasi asset informasi, tingkat ancaman, kemungkinan terjadinya ancaman dan dampak kerugian
 - 13) Sudah menetapkan sebagian ambang batas tingkat risiko yang dapat diterima
 - 14) Sudah mendefinisikan sebagian kepemilikan dan pihak pengelola (custodian) asset informasi yang ada
 - 15) Kebijakan dan Prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya
 - 16) Sebagian kebijakan keamanan informasi sudah ditetapkan secara formal dan dipublikasikan kepada semua pegawai termasuk pihak terkait
 - 17) Sudah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan
 - 18) Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK sudah tercantum dalam kontrak dengan pihak ketiga
 - 19) Sudah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya

- 20) Sudah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait
- 21) Sudah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi
- 22) Aspek keamanan informasi sebagian sudah mencakup pelaporan insiden, menjaga kerahasiaan HKI dan tata tertib penggunaan dan pengamanan asset
- 23) Konsekuensi dari sebagian pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan
- 24) Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku sudah ada untuk akses data center
- 25) Sudah ada sebagian daftar inventaris asset informasi dan asset yang berhubungan dengan proses teknologi informasi secara lengkap (termasuk kepemilikan asset)
- 26) Sudah tersedia proses pengelolaan perubahan terhadap sebagian sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang meskipun tidak diterapkan secara konsisten
- 27) Sudah tersedia proses untuk merilis suatu bagian asset baru ke dalam lingkungan operasional dan memutakhirkan inventaris asset informasi
- 28) Sudah ada definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda
- 29) Sudah ada tata tertib penggunaan komputer secara umum
- 30) Sudah ada tata tertib pengamanan dan penggunaan asset instansi terkait HAKI
- 31) Sudah ada peraturan terkait instalansi piranti lunak di asset TI milik instansi
- 32) Sudah ada sebagian persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan asset informasi
- 33) Sudah ada sebagian ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
- 34) Sudah ada proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi meskipun tidak konsisten
- 35) Sudah ada ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi asset yang ada di dalamnya meskipun tidak menyeluruh

2. Aspek Penerapan

- 1) Sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi asset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang meskipun pelaksanaan belum konsisten
- 2) Sudah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik
- 3) Infrastruktur komputasi sudah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya meskipun kasus PAC masih redundan
- 4) Sudah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi
- 5) Sudah tersedia proses untuk memindahkan asset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan
- 6) Konstruksi ruang penyimpanan perangkat pengolah informasi penting sudah 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
- 7) Sudah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting
 - 8) Sudah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga
 - 9) Sudah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga
 - 10) Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan
 - 11) Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)
 - 12) Keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan
 - 13) Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada
 - 14) Sudah menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi
 - 15) Sudah menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi
 - 16) Keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada

III. KELEMAHAN/KEKURANGAN:

1. Aspek Kerangka Kerja

- 1) Belum mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku
- 2) Belum tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini
- 3) Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
- 4) Belum tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya
- 5) Belum tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya
- 6) Instansi baru merencanakan program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan
- 7) Keseluruhan kebijakan dan prosedur keamanan informasi yang ada belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi
- 8) Instansi belum menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya
- 9) Instansi belum membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup
- 10) Instansi belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul

- | |
|--|
| <p>11) Instansi belum menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan</p> <p>12) Belum ada proses penerapan pengamanan baru dan jadwal penyelesaiannya apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada</p> <p>13) Belum tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya</p> <p>14) Belum ada perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk</p> <p>15) Belum ada uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal</p> <p>16) Belum ada 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</p> <p>17) Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala</p> <p>18) Belum 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</p> <p>19) Instansi belum 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</p> <p>20) Instansi belum mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten</p> <p>21) Belum mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya</p> <p>22) Instansi belum 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</p> <p>23) Instansi belum mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya</p> <p>24) Belum mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi</p> <p>25) Belum 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</p> <p>26) Belum menetapkan ambang batas tingkat risiko yang dapat diterima</p> <p>27) Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi</p> <p>28) Dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama belum ditetapkan</p> <p>29) Belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi</p> |
|--|

<p>langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)</p> <p>30) Langkah mitigasi risiko belum disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK</p> <p>31) Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya</p> <p>32) Belum disusun Profil risiko dan bentuk mitigasinya untuk secara berkala dikaji ulang penyelesaian langkah mitigasinya</p> <p>33) Belum membahas aspek keamanan informasi dalam manajemen proyek yang terkait</p> <p>34) Belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul</p> <p>35) Perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) belum mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk</p> <p>36) Uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) belum dilakukan terjadwal</p> <p>37) Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala</p> <p>38) Pelaksanaan audit internal belum mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi</p> <p>39) Hasil audit internal belum dikaji/dievaluasi untuk mengidentifikasi langkah pemberian dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi</p> <p>40) Hasil audit internal dilaporkan kepada pimpinan organisasi tetapi belum untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi</p> <p>41) Belum secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi</p>
2. Aspek Penerapan
<p>1) Belum tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan</p> <p>2) Belum secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada</p> <p>3) Jaringan, sistem dan aplikasi yang digunakan belum secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi</p> <p>4) Setiap perubahan dalam sistem informasi belum secara otomatis terekam di dalam log</p> <p>5) Upaya akses oleh yang tidak berhak belum secara otomatis terekam di dalam log</p> <p>6) Semua log belum dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)</p> <p>7) Belum menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya</p> <p>8) Sistem operasi untuk setiap perangkat desktop dan server belum semua dimutakhirkan dengan versi terkini</p> <p>9) Rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware belum dimutakhirkan secara rutin dan sistematis</p> <p>10) Laporan penyerangan virus/malware yang gagal/sukses belum semua ditindaklanjuti dan diselesaikan</p> <p>11) Belum menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada dan sudah mempunyai standar dalam menggunakan enkripsi</p>

- 12) Semua sistem dan aplikasi belum secara otomatis mendukung dan menerapkan penggantian password, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama
- 13) Akses yang digunakan untuk mengelola sistem (administrasi sistem) sudah menggunakan bentuk pengamanan khusus yang berlapis
- 14) Sistem dan aplikasi yang digunakan belum menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses, meskipun secara peraturan sudah ada
- 15) Belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin
- 16) Belum ada taging number di perangkat server maupun network di Data Center
- 17) Genset untuk DC hanya disediakan 1 buah dan jalur tidak terhubung dengan genset gedung, sehingga jika mengalami kerusakan maka tidak ada backup listrik untuk data center
- 18) Instalasi penangkal petir dan AC Ground sudah terpasang, hanya tidak dilakukan pengecekan secara berkala, karena bak untuk pengecekan sudah tertutup.
- 19) Tidak ada bukti pemeliharaan fire suppression system baik yg FM200 maupun APAR
- 20) Belum ada monitoring untuk switch dan router, sehingga belum ada monitor traffic. Menurut info ini sudah masuk dalam perencanaan
- 21) Set Alarm tidak diaktifkan sehingga pada saat pintu terbuka dalam jangka waktu tertentu tidak ada alert
- 22) Access door lock berdiri sendiri, tidak terhubung dengan system terpusat, sehingga access masuk per orang tidak dapat dimonitor
- 23) log book untuk masuk kedalam ruangan data center sejak akhir oktober menggunakan format baru, hanya saja tidak ada tanda tangan menyetujui dari Kabid Infrastruktur TI
- 24) Berdasarkan observai lapangan clear screen pada desktop yang tidak berjalan sebagaimana kebijakan berlaku
- 25) Pada DC kedua PAC berjalan bersamaan, sehingga tidak terjadi prinsip redudansi

IV. REKOMENDASI:

1. Kebijakan SMKI harus menambahkan beberapa kebijakan dan prosedur yang sesuai dengan ISO 27001 dan juga disesuaikan dengan lingkup yang akan disertifikasi
2. Memenuhi aktivitas yang belum atau baru dilaksanakan sebagian di Aspek Kerangka Kerja, antara lain:
 - a. Mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi
 - b. Menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya
 - c. 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
 - d. Menyusun kerangka kerja pengelolaan risiko ini yang mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugiannya
 - e. Menetapkan ambang batas tingkat risiko yang dapat diterima
 - f. Mengidentifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi

<p>g. Menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama</p> <p>h. 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)</p> <p>i. Menyusun langkah mitigasi risiko sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK</p> <p>j. Memantau status penyelesaian langkah mitigasi risiko secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya</p> <p>k. Menyusun profil risiko dan bentuk mitigasinya untuk secara berkala dikaji ulang penyelesaian langkah mitigasinya</p> <p>l. Membahas aspek keamanan informasi dalam manajemen proyek yang terkait</p> <p>m. Menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul</p> <p>n. Menyusun perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) yang mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk</p> <p>o. Menjadwalkan uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan)</p> <p>p. Melakukan evaluasi secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi</p> <p>q. Melakukan evaluasi pelaksanaan audit internal terhadap tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi</p> <p>r. Melakukan evaluasi hasil audit internal untuk mengidentifikasi langkah pemberian dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi</p> <p>s. Melaporkan hasil audit internal untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi</p> <p>t. Menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi secara periodic</p>
<p>3. Melakukan aktivitas yang belum dilaksanakan atau baru dilaksanakan sebagian di Aspek Penerapan, antara lain:</p> <p>a. Menyediakan konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan</p> <p>b. Melakukan analisis kepatuhan penerapan konfigurasi standar yang ada secara rutin</p> <p>c. Memindai jaringan, sistem dan aplikasi yang digunakan untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi secara rutin</p> <p>d. Melakukan analisis log secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)</p> <p>e. Menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya</p> <p>f. Memutakhirkan Sistem operasi untuk setiap perangkat desktop dan server belum dengan versi terkini</p>

- g. Memutakhirkan rekaman dan hasil analisa (jejak audit - audit trail) secara rutin dan sistematis
- h. Menindaklanjuti laporan penyerangan virus/malware yang gagal/sukses
- i. Perlu didesain control bagi desktop/notebook yang akan masuk dalam jaringan network DISKOMINFO, misal dengan menggunakan Active Directory atau Network access control
- j. Admin untuk Firewall/perangkat network sebaiknya tidak bergantung pada satu orang staff dan dihindari adanya generic user-id
- k. Sistem Access door lock sebaiknya bisa mencatat log keluar-masuk dan server time juga merujuk pada NTP server yang sama dengan CCTV
- l. Semua dokumen SMKI harus ada bukti pengesahan (ditanda tangani)
- m. Perlu untuk dibuat perencanaan agar jika terjadi gangguan pada genset DC, maka bilamana terjadi listrik PLN mati masih ada yang mensuplai listrik
- n. Instalasi grounded dan penangkal petir harus secara berkala dilakukan pengecekan
- o. Semua rack server harus terhubung dengan ground untuk menghindari kerusakan pada perangkat yang terpasang
- p. Perlu dibuat rencana audit berkala minimal 1 tahun sekali, terhadap kesesuaian dengan kebijakan, prosedur dan standard yang ditentukan dalam SMKI
- q. Untuk perangkat jaringan (switch, router,firewall) dan server harus mempunyai standard sesuai keamanan informasi yang ditentukan
- r. Perlu dilakukan vulnerability assessment dan penetration test berkala, juga setiap rencana perbaikan dari hasil tersebut dicatat dan direview secara berkala.
- s. Semua perangkat termasuk utility : fire suppression system, ac, genset perlu untuk dilakukan pemeliharaan secara berkala
- t. PAC harus bisa berjalan dalam posisi redundansi aktif dan stand by
- u. Network traffic juga sebaiknya untuk dimonitor, sehingga kapasitas layanan bisa diukur

Surabaya, 1 November 2018
 Narasumber Dinas Komunikasi dan
 Informatika Provinsi Jawa Timur

1. Dra. Ec. NIRMALA DEWI, M.M

2. IR. DODONG MARTIAR M, M.SI

3. AULIA BAHAR P, S.KOM, M.ISM

4. ACHMAD FADLIL CHUSNI, S.KOM,
 M.MT

5. AGUS BUDI SAMPURNO, SE

6. NOFIAN ADI P, S.KOM, MT

7. PONDRA SETIAWAN

8. RETNO Y.W, ST, M.MED.KOM

9. SEPTIAN FAJAR ARIFIN, A.MD

Assessor Indeks KAMI:

1. Assessor Utama:
 DENNY SADIKIN

2. Assessor Pendamping:
 KAUTSARINA

3. Observer:
 M. NUR AFIF

SITI MASMU'AH