



BERITA ACARA PEMERIKSAAN DOKUMEN

Pada hari ini *Jumattanggal dua puluh delapanbulan Desembertahun dua ribu delapan belas* bertempat di Diskominfotik Provinsi DKI Jakarta, Kami selanjutnya disebut sebagai PIHAK II :

1. Kautsarina
2. Pancat Setyantana

Telah melakukan pemeriksaan dokumen dalam rangka Onsite Assessment Pemeringkatan Indeks Keamanan Informasi untuk kepentingan Dinas Komunikasi, Informatika dan Statistik Provinsi DKI Jakarta

Pemeriksaan Dokumen dilakukan terhadap dokumen-dokumen berikut:

1. Peraturan Gubernur Provinsi DKI Jakarta Nomor 16 Tahun 2008 tentang Rencana Induk Teknologi Informasi dan Komunikasi
2. Peraturan Gubernur Provinsi DKI Jakarta Nomor 39 Tahun 2012 tentang Sistem Informasi Manajemen Daerah
3. Peraturan Gubernur Provinsi DKI Jakarta Nomor 142 Tahun 2013 tentang Sistem dan Prosedur Pengelolaan Keuangan Daerah
4. Instruksi Gubernur Provinsi DKI Jakarta Nomor 1 Tahun 2013 tentang Penggunaan Perangkat Lunak dan Perangkat Keras Berlisensi
5. Peraturan Gubernur Provinsi DKI Jakarta Nomor 175 Tahun 2016 tentang Layanan Informasi Publik
6. Peraturan Gubernur Provinsi DKI Jakarta Nomor 57 Tahun 2018 tentang Perubahan Ketiga atas Peraturan Gubernur Nomor 409 Tahun 2016 tentang Tunjangan Kinerja Daerah
7. Peraturan Gubernur Provinsi DKI Jakarta Nomor 11 Tahun 2018 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi
8. Peraturan Gubernur Provinsi DKI Jakarta Nomor 69 Tahun 2018 tentang Penggunaan Sertifikat Elektronik
9. Peraturan Gubernur Provinsi DKI Jakarta Nomor 75 Tahun 2018 tentang Perubahan atas Peraturan Gubernur Nomor 265 tahun 2016 tentang Organisasi dan Tata Kerja Dinas Komunikasi, Informatika dan Statistik
10. Surat Edaran Nomor 44/SE/2018 tentang Dokumen Kelengkapan Sertifikat Elektronik
11. Surat Edaran Nomor 50/SE/2018 tentang Kebijakan Penggunaan Intranet dan Internet dalam Informasi dan Transaksi Elektronik di Lingkungan Pemerintah Provinsi Daerah Khusus Ibukota Jakarta
12. Keputusan Sekretaris Daerah Prov DKI Jakarta Nomor 61 Tahun 2017 tentang Klasifikasi Informasi yang Dilakukan
13. Surat Edaran Nomor 42/SE/2015 tentang Pelaksanaan Permohonan Rekomendasi Bidang Teknologi, Informasi dan Komunikasi di Lingkungan Pemerintah Provinsi DKI Jakarta
14. Surat Edaran Nomor 7/SE/2014 tentang Penggunaan Subdomain www.Jakarta.go.id dan Email @jakarta.go.id
15. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Tata Kelola Teknologi Informasi dan Komunikasi
16. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Siklus Hidup Pembangunan Sistem Informasi

17. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Evaluasi Pasca Implementasi Sistem Informasi
18. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Manajemen Jaminan Mutu Pembangunan Sistem Informasi
19. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Manajemen Tingkat Layanan
20. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Pertukaran Data Elektronik
21. Keputusan Kepala Diskominfotik Provinsi DKI Jakarta Nomor 71 Tahun 2017 tentang Standar Operasional Prosedur Seksi Persandian dan Sistem Keamanan Data Bidang Jaringan dan Komunikasi Data
22. SOP Permohonan Keamanan Aplikasi Berbasis Web
23. SOP Permohonan Pembuatan Domain/Sub Domain
24. SOP Permohonan Instalasi Antivirus
25. SOP Permohonan Investigasi Forensik Keamanan Aplikasi Berbasis Web
26. SOP Permohonan Akses Virtual Private Network
27. SOP Keamanan Kata Sandi
28. Draf SOP Analisis Sistem Informasi
29. Draf SOP Perancangan Sistem Informasi
30. Draf SOP Implementasi Sistem Informasi
31. Draf SOP Pembangunan Sistem Informasi
32. Draf SOP Pengembangan Sistem Informasi
33. Draf SOP Pengkodean Sistem Informasi
34. Draf SOP Pengujian Sistem Informasi
35. Draf SOP Backup Database
36. Draf SOP Restore Database

Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Dashboard monitoring Data Center One Stop Service (DCOSS)
2. Dashboard Gitlab
3. Sertifikat keikutsertaan pelatihan Certified Information Security Manager (CISM) tahun 2018 a.n. Tony Yudianto Pribadi
4. Sertifikat keikutsertaan pelatihan CISA Exam Preparation tahun 2018 a.n. Tony Yudianto Pribadi
5. Daftar User Active
6. Daftar Alamat Email
7. Laporan pemeliharaan Genset Maret – Juni 2018
8. Laporan IT Security Assessment Juni 2018 pada Web Portal BPBD (Badan Penanggulangan Bencana Daerah) dan Sistem APBD
9. Perjanjian Kerahasiaan antara Bidang Jaringan dan Komunikasi Data dengan Tenaga Ahli SKPD/UKPD Permohonan Akses VPN ke Dinas Komunikasi, Informatika dan Statistik Pemprov DKI Jakarta No. 1307/2018/JKD/PSKD/2018
10. Surat Perjanjian untuk melaksanakan Paket Pekerjaan Jasa Lainnya: Sewa Backup Link Jaringan Komuniaksi WAN Nomor: 01.05/1.16.01.004.2/JKD/02/2018
11. Kaspersky Secure Mail Gateway Report Mail Analyzer per 27 Desember 2018
12. Manual Book Aplikasi E-Kinerja Pemerintahan Provinsi DKI Jakarta Versi 1.0
13. Undangan Security Awareness Nomor 4757/-089.51 tanggal 29 November 2018, materi: Sosialisasi Membangun Kesadaran Budaya Keamanan Informasi di Era Siber, Sosialisasi Penggunaan Sertifikat Elektronik di Lingkungan Pemerintah Provinsi DKI Jakarta

14. Foto Dokumentasi Sosialisasi Security Awareness di Lingkungan Pemerintah Provinsi DKI Jakarta, hari Selasa 4 Desember 2018 di Ruang Seribu Wajah Balaikota Provinsi DKI Jakarta Blok G Lantai 22
15. Undangan Pelatihan Bimbingan Teknis Infrastruktur dan Implementasi Sertifikat Elektronik untuk Tandatangan Digital serta Pengamanan Dokumen Nomor 2516-084.6 tanggal 28 Juni 2018
16. Foto Dokumentasi Pelatihan Bimbingan Teknis Infrastruktur dan Implementasi Sertifikat Elektronik untuk Tandatangan Digital serta Pengamanan Dokumen , tanggal 4 Juli 2018 di Ruang Kelas Gedung Balaikota Blok G Lt. 3
17. Daftar Hadir Peserta Pelatihan Bimbingan Teknis Infrastruktur dan Implementasi Sertifikat Elektronik untuk Tandatangan Digital serta Pengamanan Dokumen 4-5 Juli 2018

Dokumen-dokumen tersebut diserahkan oleh Diskominfo Provinsi DKI Jakarta Untuk kepentingan Onsite Assessment PemeringkatanIndeks Keamanan Informasi, sudah dilakukan diskusi tatap muka dan kunjungan dengan selanjutnya disebut PIHAK I :

1. ANDRIE YUSWANTO
2. RYCAN FAHMI
3. TONY YUDIANTO
4. YUNIARTO
5. YULI WAHYUDIANTO
6. DWIANA KUSUMASARI

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

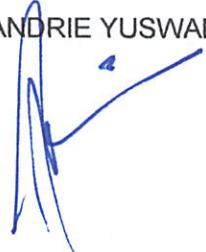
- 1) memperlakukan informasi dan/atau dokumen milik PIHAK I dengan hati-hati dan bijaksana agar terjamin keutuhan dokumen, terhindar dari kerusakan atau kehilangan, dan tidak memberikannya kepada PIHAK lain, mempublikasikan, atau menyebarluaskannya, sama seperti memperlakukan informasi dan/atau dokumen 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 Onsite Assessment PemeringkatanIndeks KAMI selesai.

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

Jakarta, 28Desember 2018

Narasumber DISKOMINFOTIK
PROVINSI DKI JAKARTA

1.. ANDRIE YUSWANTO



2. RYCAN FAHMI



3. TONY YUDIANTO



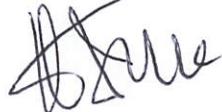
4. YUNIARTO



5. YULI WAHYUDIANTO



6. DWIANA KUSUMASARI

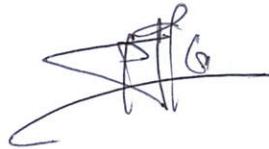


Assessor Indeks KAMI:

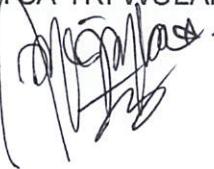
1. Assessor Utama:
KAUTSARINA



2. Assessor Pendamping:
PANCAT SETYANTANA



3. Administrator :
JULXSA TRI WULANDARI



4. Administrator:

SITI MASMUAH



	LAPORAN VERIFIKASI INDEKS KAMI	INDEKS KEAMANAN INFORMASI
Instansi/Perusahaan: PEMERINTAH PROVINSI DKI JAKARTA	Narasumber Instansi/Perusahaan: 1. ANDRIE YUSWANTO 2. RYCAN FAHMI 3. TONY YUDIANTO 4. YUNIARTO 5. YULI WAHYUDIANTO 6. DWIANA KUSUMASARI	
Unit Kerja: DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI DKI JAKARTA		
Alamat: Jl. Medan Merdeka Selatan No. 8 Jakarta, Blok G	Tel: 021 - 3823253 Fax: 021 - 3823253	
Email: diskominfotik@jakarta.go.id	Pimpinan Unit Kerja: ATIKA NUR RAHMANIA, S.I.P., M.Si.	
<p>A. <u>Ruang Lingkup:</u></p> <p>1. Instansi / Unit Kerja: DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI DKI JAKARTA</p> <p>2. Fungsi Kerja:</p> <ol style="list-style-type: none"> 1. Penyusunan rencana strategis dan rencana kerja dan anggaran Dinas Kominfo dan Statistik 2. Pelaksanaan rencana strategis dan dokumen pelaksanaan anggaran 3. Pelaksanaan penyiapan perumusan dan pelaksanaan kebijakan di bidang komunikasi dan informatika, statistic dan persandian 4. Penyusunan norma, standar, prosedur dan kriteria di bidang komunikasi dan informatika, statistic dan persandian 5. Pemberian bimbingan teknis dan supervise, serta pemantauan, evaluasi dan pelaporan di bidang komunikasi dan informatika, statistic dan persandian 6. Pengelolaan opini dan aspirasi public 7. Pengelolaan dan pelayanan informasi public 8. Fasilitasi dan pemberian pelayanan teknis 9. Penyediaan konten lintas sectoral dan pengelolaan media komunikasi public 10. Pelaksanaan layanan hubungan media 11. Penguatan kapasitas sumber daya komunikasi public dan penyediaan akses informasi 12. Penyelenggaraan layanan infrastruktur data center, Disaster Recovery Center dan Teknologi Informasi dan Komunikasi Pemerintah Daerah 13. Penyelenggaraan layanan pengembangan jaringan internet dan penggunaan akses internet 14. Pelaksanaan layanan keamanan informasi e-Government 15. Pelaksanaan layanan system komunikasi intra Pemerintah Daerah 16. Penyelenggaraan layanan pengembangan dan pengelolaan aplikasi generic, spesifik dan suplemen yang terintegrasi 		

17. Penyelenggaraan ekosistem Teknologi Informasi dan Komunikasi dan Smart Province
18. Pelaksanaan layanan nama domain dan sub domain bagi Lembaga
19. Pelayanan public dan kegiatan, penyelenggaraan Government Chief Information Officer (GCIO) Pemerintah Daerah
20. Pengembangan sumber daya TIK Pemerintah Daerah dan masyarakat
21. Pengoordinasian kegiatan statistic
22. Penyediaan, penatausahaan, penggunaan, pemeliharaan dan perawatan prasarana dan sarana kerja di bidang komunikasi, informatika, statistik

3. Lokasi:

No	Nama Lokasi	
1	Kantor Diskominfo TIK Prov DKI Jakarta	Jl. Medan Merdeka Selatan No. 8
2	Data Center	Jl. Medan Merdeka Selatan No. 8
3.	DRC	Bandung

B. Nama /Jenis Layanan Publik:

1. 700 domain Website di Lingkungan Provinsi DKI Jakarta
2. 385 Aplikasi di Lingkungan Provinsi DKI Jakarta

C. Aset TI yang kritikal:

1. Informasi:
- seluruh informasi dalam aplikasi dan infrastruktur
2. Aplikasi:
-385 Aplikasi

3. Server:
-764 Server

4. Infrastruktur Jaringan/Network:
- Telkom
- Moratelindo

Link:

- Telkom
- Lintasarta

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)	✓		D Pergub Prov DKI Tentang Tata Kelola Teknologi Informasi dan Komunikasi
2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	✓		R Surat Edaran Nomor 50/SE/2018 tentang Kebijakan Penggunaan Intranet dan Internet dalam Informasi dan Transaksi Elektronik di Lingkungan Pemerintah Provinsi Daerah Khusus Ibukota Jakarta
3	Sasaran TI / Keamanan Informasi	✓		D Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Tata Kelola Teknologi Informasi dan Komunikasi
4	Organisasi TI / Keamanan Informasi (IT Steering Committee, Fungsi Keamanan TI)	✓		R Peraturan Gubernur Provinsi DKI Jakarta Nomor 75 Tahun 2018 tentang Perubahan atas Peraturan Gubernur Nomor 265 tahun 2016 tentang Organisasi dan Tata Kerja Dinas Komunikasi, Informatika dan Statistik

5	Metodologi Manajemen Risiko TI		✓	
6	Business Continuity Plan		✓	
7	Klasifikasi Informasi			R Peraturan Gubernur Provinsi DKI Jakarta Nomor 175 Tahun 2016 tentang Layanan Informasi Publik R Keputusan Sekretaris Daerah Prov DKI Jakarta Nomor 61 Tahun 2017 tentang Klasifikasi Informasi yang Dilakukan Ref. UU no 14 /2008 - Keterbukaan Informasi Publik. Klasifikasi informasi ada 2: Informasi PUBLIK dan "YANG DIKECUALIKAN"
8	Standar software dekstop		✓	
9	Metode Pengukuran Efektivitas Kontrol		✓	
10	Non Disclosure Agreement (NDA)		✓	D Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Manajemen Tingkat Layanan
	Prosedur- Prosedur:			
1	Pengendalian Dokumen		✓	
2	Pengendalian Rekaman/Catatan		✓	
3	Tindakan Perbaikan & Pencegahan		✓	R Keputusan Kepala Diskominfo Provinsi DKI Jakarta Nomor 71 Tahun 2017 tentang Standar Operasional Prosedur Seksi Persandian dan Sistem Keamanan Data Bidang Jaringan dan Komunikasi Data
4	Audit Internal		✓	

5	Penanganan (Handling) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran		✓	
6	Pengelolaan Media Removable & Disposal		✓	
7	Pengelolaan Perubahan Sistem TI (Change Control Sistem TI)		✓	
8	Pengelolaan Hak Akses (User Access Management)		✓	
9	Teleworking (Akses Remote)		✓	
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	✓	R Keputusan Kepala Diskominfo Provinsi DKI Jakarta Nomor 71 Tahun 2017 tentang Standar Operasional Prosedur Seksi Persandian dan Sistem Keamanan Data Bidang Jaringan dan Komunikasi Data	
11	Pemantauan (Monitoring) Sumber Daya TI: a. Monitoring Kapasitas b. Log Penggunaan User		✓	
12	Instalasi & Pengendalian Software	✓	R Instruksi Gubernur Provinsi DKI Jakarta Nomor 1 Tahun 2013 tentang Penggunaan Perangkat Lunak dan Perangkat Keras Berlisensi	
13	Back-up & restore (prosedur/jadwal)	✓	D Draf SOP Backup Database Draf SOP Restore Database	

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Peraturan Gubernur Provinsi DKI Jakarta Nomor 16 Tahun 2008 tentang Rencana Induk Teknologi Informasi dan Komunikasi
2. Peraturan Gubernur Provinsi DKI Jakarta Nomor 39 Tahun 2012 tentang Sistem Informasi Manajemen Daerah
3. Peraturan Gubernur Provinsi DKI Jakarta Nomor 142 Tahun 2013 tentang Sistem dan Prosedur Pengelolaan Keuangan Daerah
4. Instruksi Gubernur Provinsi DKI Jakarta Nomor 1 Tahun 2013 tentang Penggunaan Perangkat Lunak dan Perangkat Keras Berlisensi

5. Peraturan Gubernur Provinsi DKI Jakarta Nomor 175 Tahun 2016 tentang Layanan Informasi Publik
6. Peraturan Gubernur Provinsi DKI Jakarta Nomor 57 Tahun 2018 tentang Perubahan Ketiga atas Peraturan Gubernur Nomor 409 Tahun 2016 tentang Tunjangan Kinerja Daerah
7. Peraturan Gubernur Provinsi DKI Jakarta Nomor 11 Tahun 2018 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi
8. Peraturan Gubernur Provinsi DKI Jakarta Nomor 69 Tahun 2018 tentang Penggunaan Sertifikat Elektronik
9. Peraturan Gubernur Provinsi DKI Jakarta Nomor 75 Tahun 2018 tentang Perubahan atas Peraturan Gubernur Nomor 265 tahun 2016 tentang Organisasi dan Tata Kerja Dinas Komunikasi, Informatika dan Statistik
10. Surat Edaran Nomor 44/SE/2018 tentang Dokumen Kelengkapan Sertifikat Elektronik
11. Surat Edaran Nomor 50/SE/2018 tentang Kebijakan Penggunaan Intranet dan Internet dalam Informasi dan Transaksi Elektronik di Lingkungan Pemerintah Provinsi Daerah Khusus Ibukota Jakarta
12. Keputusan Sekretaris Daerah Prov DKI Jakarta Nomor 61 Tahun 2017 tentang Klasifikasi Informasi yang Dilkecualikan
13. Surat Edaran Nomor 42/SE/2015 tentang Pelaksanaan Permohonan Rekomendasi Bidang Teknologi, Informasi dan Komunikasi di Lingkungan Pemerintah Provinsi DKI Jakarta
14. Surat Edaran Nomor 7/SE/2014 tentang Penggunaan Subdomain www.Jakarta.go.id dan Email @jakarta.go.id
15. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Tata Kelola Teknologi Informasi dan Komunikasi
16. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Siklus Hidup Pembangunan Sistem Informasi
17. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Evaluasi Pasca Implementasi Sistem Informasi
18. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Manajemen Jaminan Mutu Pembangunan Sistem Informasi
19. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Manajemen Tingkat Layanan
20. Draf Peraturan Gubernur Provinsi DKI Jakarta tentang Pertukaran Data Elektronik
21. Keputusan Kepala Diskominfotik Provinsi DKI Jakarta Nomor 71 Tahun 2017 tentang Standar Operasional Prosedur Seksi Persandian dan Sistem Keamanan Data Bidang Jaringan dan Komunikasi Data
22. SOP Permohonan Keamanan Aplikasi Berbasis Web
23. SOP Permohonan Pembuatan Domain/Sub Domain
24. SOP Permohonan Instalasi Antivirus
25. SOP Permohonan Investigasi Forensik Keamanan Aplikasi Berbasis Web
26. SOP Permohonan Akses Virtual Private Network
27. SOP Keamanan Kata Sandi
28. Draf SOP Analisis Sistem Informasi
29. Draf SOP Perancangan Sistem Informasi
30. Draf SOP Implementasi Sistem Informasi
31. Draf SOP Pembangunan Sistem Informasi
32. Draf SOP Pengembangan Sistem Informasi
33. Draf SOP Pengkodean Sistem Informasi
34. Draf SOP Pengujian Sistem Informasi
35. Draf SOP Backup Database
36. Draf SOP Restore Database

Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Dashboard monitoring Data Center One Stop Service (DCOSS)

2. Dashboard Gitlab
3. Sertifikat keikutsertaan pelatihan Certified Information Security Manager (CISM) tahun 2018 a.n. Tony Yudianto Pribadi
4. Sertifikat keikutsertaan pelatihan CISA Exam Preparation tahun 2018 a.n. Tony Yudianto Pribadi
5. Daftar User Active
6. Daftar Alamat Email
7. Laporan pemeliharaan Genset Maret – Juni 2018
8. Laporan IT Security Assessment Juni 2018 pada Web Portal BPBD (Badan Penanggulangan Bencana Daerah) dan Sistem APBD
9. Perjanjian Kerahasiaan antara Bidang Jaringan dan Komunikasi Data dengan Tenaga Ahli SKPD/UKPD Permohonan Akses VPN ke Dinas Komunikasi, Informatika dan Statistik Pemprov DKI Jakarta No. 1307/2018/JKD/PSKD/2018
10. Surat Perjanjian untuk melaksanakan Paket Pekerjaan Jasa Lainnya: Sewa Backup Link Jaringan Komunikasi WAN Nomor: 01.05/1.16.01.004.2/JKD/02/2018
11. Kaspersky Secure Mail Gateway Report Mail Analyzer per 27 Desember 2018
12. Manual Book Aplikasi E-Kinerja Pemerintahan Provinsi DKI Jakarta Versi 1.0
13. Undangan Security Awareness Nomor 4757/-089.51 tanggal 29 November 2018, materi: Sosialisasi Membangun Kesadaran Budaya Keamanan Informasi di Era Siber, Sosialisasi Penggunaan Sertifikat Elektronik di Lingkungan Pemerintah Provinsi DKI Jakarta
14. Foto Dokumentasi Sosialisasi Security Awareness di Lingkungan Pemerintah Provinsi DKI Jakarta, hari Selasa 4 Desember 2018 di Ruang Seribu Wajah Balaikota Provinsi DKI Jakarta Blok G Lantai 22
15. Undangan Pelatihan Bimbingan Teknis Infrastruktur dan Implementasi Sertifikat Elektronik untuk Tandatangan Digital serta Pengamanan Dokumen Nomor 2516/-084.6 tanggal 28 Juni 2018
16. Foto Dokumentasi Pelatihan Bimbingan Teknis Infrastruktur dan Implementasi Sertifikat Elektronik untuk Tandatangan Digital serta Pengamanan Dokumen , tanggal 4 Juli 2018 di Ruang Kelas Gedung Balaikota Blok G Lt. 3
17. Daftar Hadir Peserta Pelatihan Bimbingan Teknis Infrastruktur dan Implementasi Sertifikat Elektronik untuk Tandatangan Digital serta Pengamanan Dokumen 4-5 Juli 2018

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

I. KONDISI UMUM:

1. Struktur organisasi satuan kerja Dinas Kominfo dan Statistik Provinsi DKI Jakarta dalam ruang lingkup:



2. SDM pengelola terdiri dari:
235 orang PNS/pegawai tetap
274 orang non PNS/honorer
 3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Total Score Sebelum Verifikasi: 302 (ref. file Indeks KAMI sebelum Verifikasi)

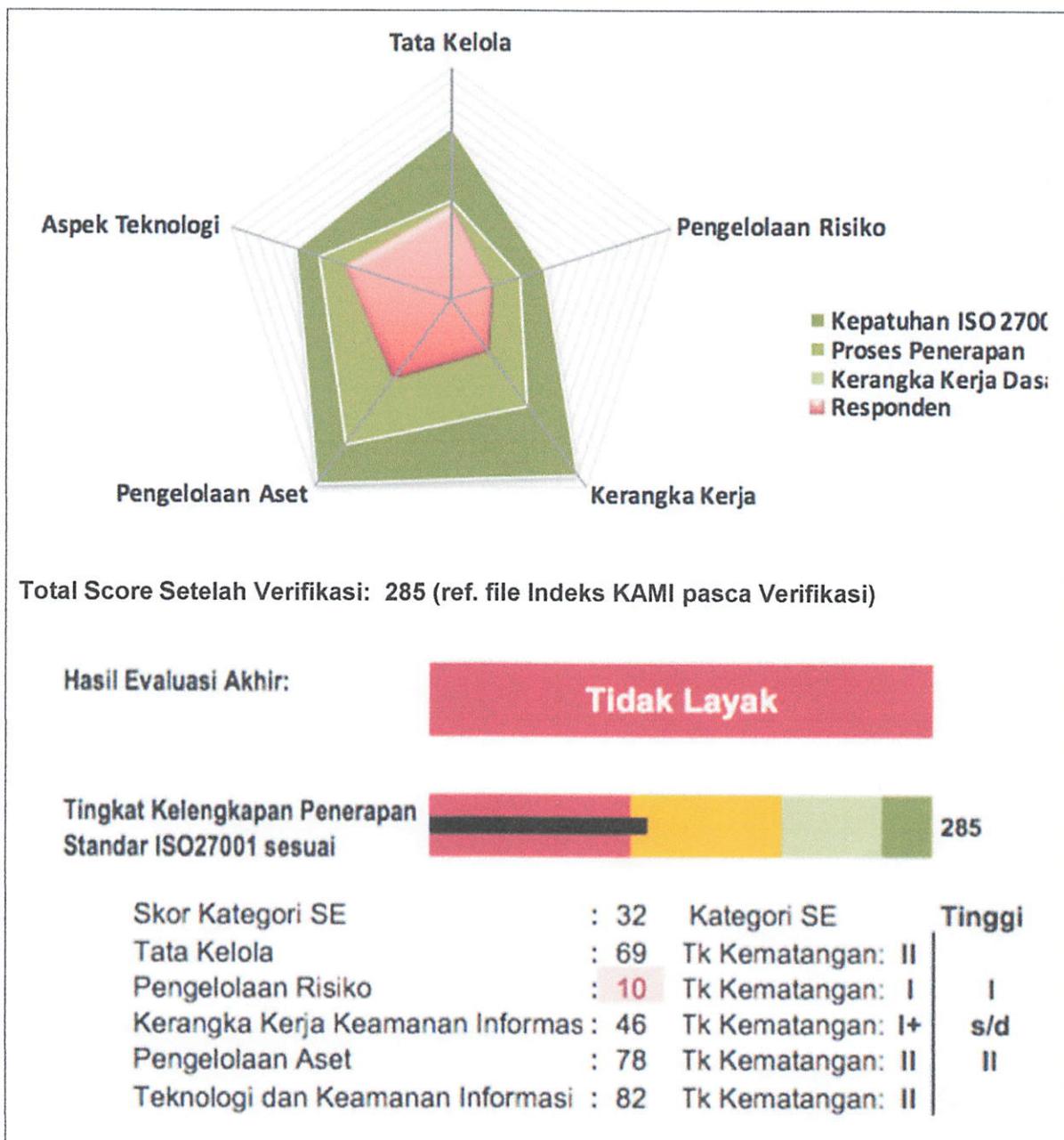
Hasil Evaluasi Akhir:

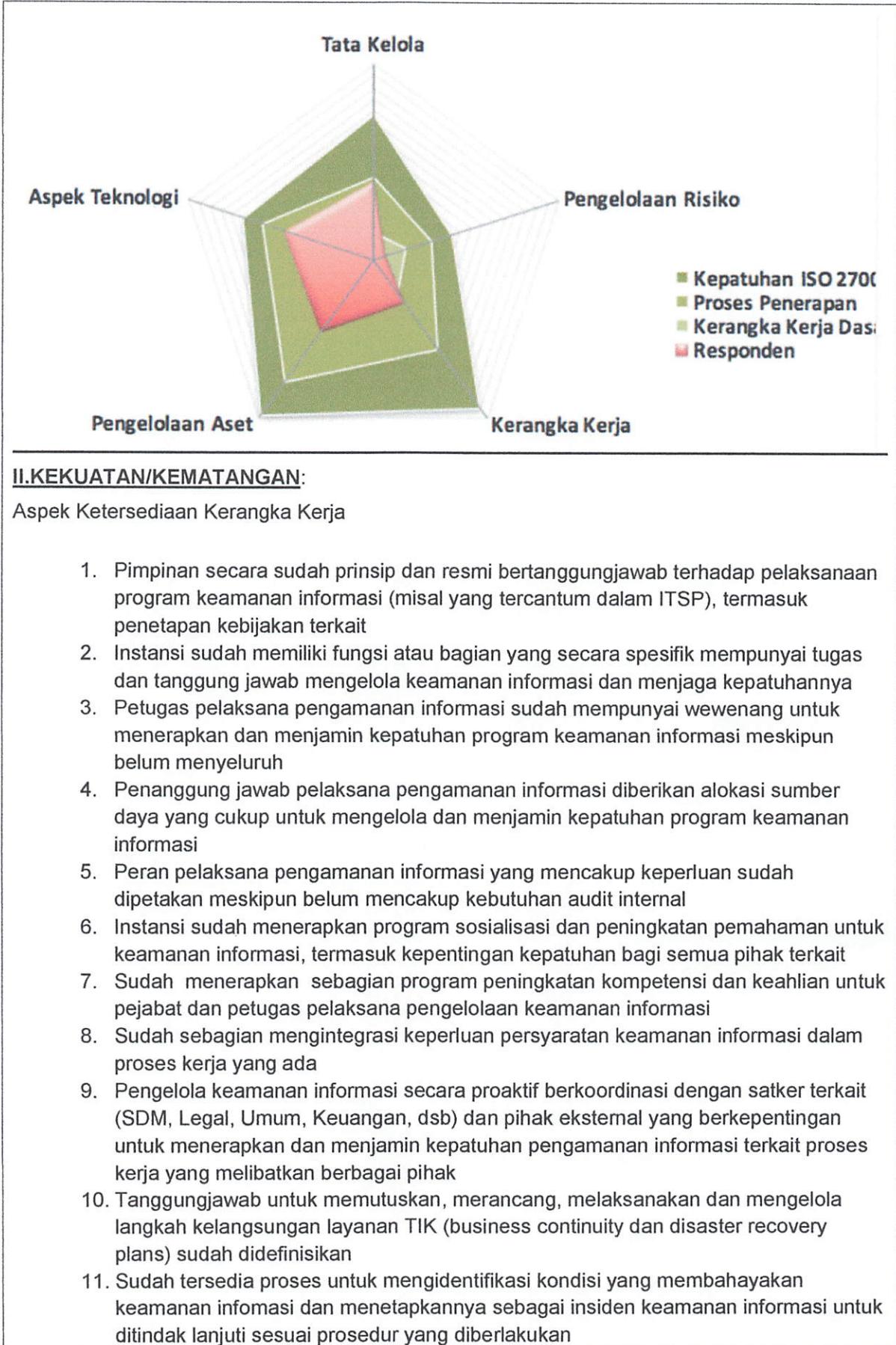
Perlu Perbaikan

Tingkat Kelengkapan Penerapan
Standar ISO27001 sesuai



Skor Kategori SE	:	32	Kategori SE	Tinggi
Tata Kelola	:	69	Tk Kematangan:	II
Pengelolaan Risiko	:	32	Tk Kematangan:	I+
Kerangka Kerja Keamanan Informasi	:	47	Tk Kematangan:	I+ s/d
Pengelolaan Aset	:	72	Tk Kematangan:	I+ II
Teknologi dan Keamanan Informasi	:	82	Tk Kematangan:	II





12. Sudah ada sebagian daftar inventaris asset informasi dan asset yang berhubungan dengan proses teknologi informasi secara lengkap (termasuk kepemilikan asset)
13. Sudah ada definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda
14. Sudah ada kebijakan yang disahkan dalam penggunaan asset instansi terkait HAKI, khususnya perangkat lunak berlisensi
15. Sudah ada sebagian persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan asset informasi
16. Sudah ada sebagian ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya

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
4. 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
5. Sudah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan asset informasi penting
6. Sudah tersedia mekanisme pengamanan dalam pengiriman asset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga
7. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan
8. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)
9. Sebagian infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan
10. Sebagian infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada
11. Sudah menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi
12. Sudah menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi
13. Sebagian jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada

III. KELEMAHAN/KEKURANGAN:

Aspek Kerangka Kerja

1. Pejabat pelaksana pengamanan informasi yang mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi belum ditetapkan
2. Peran pelaksana pengamanan informasi belum mencakup semua keperluan sudah dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan
3. Kebijakan dan Prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi belum disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya
4. Instansi belum mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan
5. Instansi belum menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan
6. Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan asset maupun layanan TIK belum tercantum dalam kontrak dengan pihak ketiga
7. Belum tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait
8. Belum mendefinisikan metrik parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme waktu pengukuran dan pelaksananya
9. Aspek keamanan informasi sebagian belum mencakup pelaporan insiden, menjaga kerahasiaan HAKI dan tata tertib penggunaan dan pengamanan asset
10. Konsekuensi dari sebagian pelanggaran kebijakan keamanan informasi belum seluruhnya didefinisikan, dikomunikasikan dan ditegakkan
11. Belum ada prosedur kajian penggunaan akses dan hak aksesnya berikut langkah pemberahan apabila terjadi ketidaksesuaian terhadap kebijakan yang berlaku
12. Belum tersedia proses pengelolaan perubahan terhadap sebagian system, proses bisnis dan proses teknologi informasi
13. Belum tersedia proses untuk merilis suatu bagian asset baru ke dalam lingkungan operasional dan memutakhirkan inventaris asset informasi, meskipun secara praktik sudah dilakukan
14. Belum ada tata tertib penggunaan komputer secara umum

Aspek Penerapan

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 menindaklanjuti konsekuensi dari kondisi ini
3. Belum tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya
4. Belum tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya
5. Instansi baru merencanakan program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan

6. 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
7. 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
8. Instansi belum membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup
9. Instansi belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul
10. Instansi belum menerapkan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan
11. Belum ada proses penerapan pengamanan baru dan jadwal penyelesaiannya apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada
12. Belum tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya
13. Belum ada perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk
14. Belum ada uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal
15. Belum ada hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pemberian yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada
16. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala
17. 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
18. 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 pemberian yang diperlukan, telah diterapkan secara efektif
19. Instansi belum mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten
20. Belum mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya
21. 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

22. Instansi belum mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya
23. Belum mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi
24. Belum menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaian secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi
25. Belum menetapkan ambang batas tingkat risiko yang dapat diterima
26. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi
27. Dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama belum ditetapkan
28. Belum 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)
29. Langkah mitigasi risiko belum 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
30. Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya
31. Belum disusun Profil risiko dan bentuk mitigasinya untuk secara berkala dikaji ulang penyelesaian langkah mitigasinya
32. Belum membahas aspek keamanan informasi dalam manajemen proyek yang terkait
33. Belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul
34. Perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) belum mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk
35. Uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) belum dilakukan terjadwal
36. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala
37. Pelaksanaan audit internal belum mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi
38. Hasil audit internal belum dikaji/dievaluasi untuk mengidentifikasi langkah pemberian dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi
39. Hasil audit internal dilaporkan kepada pimpinan organisasi tetapi belum untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi
40. Belum secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi

IV. REKOMENDASI:

1. Menyelesaikan dan menetapkan kebijakan tata kelola teknologi informasi dan keamanan informasi sebagai acuan kerja Diskominfotik Provinsi DKI Jakarta
2. Menyesuaikan kebutuhan fungsi kerja dalam Diskominfotik agar lebih memadai, sebaiknya struktur eksisting dilengkapi dengan bagian Compliance untuk dapat memenuhi aktivitas SMKI dalam menyusun kebijakan, prosedur dan memeriksa kesesuaiannya dengan standar yang berlaku dan persiapannya dalam kebutuhan sertifikasi ISO 27001
3. Melengkapi standar dan prosedur , serta bukti implementasi Kebijakan SMKI yang belum disusun
4. Mengajukan Onsite Assesment kembali untuk menilai implementasi SMKI secara menyeluruh apabila sudah ada peningkatan aktivitas dalam dokumen dan implementasi
5. Memenuhi aktivitas yang belum atau baru dilaksanakan sebagian di Aspek Kerangka Kerja, antara lain:
 - a. Semua dokumen SMKI harus ada bukti pengesahan (ditandatangani) fisik atau digital
 - b. Berkoordinasi kembali dengan pihak terkait untuk penomoran SOP yang konsisten
 - c. Mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi
 - d. Menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya
 - e. 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
 - f. Menyusun kerangka kerja pengelolaan risiko ini yang mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugiannya
 - g. Menetapkan ambang batas tingkat risiko yang dapat diterima
 - h. Mengidentifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi
 - i. Menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama
 - j. 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)
 - k. Menyusun langkah mitigasi risiko 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
 - l. Memantau status penyelesaian langkah mitigasi risiko secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya
 - m. Menyusun profil risiko dan bentuk mitigasinya untuk secara berkala dikaji ulang penyelesaian langkah mitigasinya
 - n. Membahas aspek keamanan informasi dalam manajemen proyek yang terkait

- o. Menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul
 - p. Menyusun perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) yang mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk
 - q. Menjadwalkan uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan)
 - r. Melakukan evaluasi secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi
 - s. Melakukan evaluasi pelaksanaan audit internal terhadap tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi
 - t. Melakukan evaluasi hasil audit internal untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi
 - u. Melaporkan hasil audit internal untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi
 - v. Menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi secara periodik
6. Melakukan aktivitas yang belum dilaksanakan atau baru dilaksanakan sebagian di Aspek Penerapan, antara lain:
- a. Menyediakan konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan
 - b. Melakukan analisis kepatuhan penerapan konfigurasi standar yang ada secara rutin
 - c. Memindai jaringan, sistem dan aplikasi yang digunakan untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi secara rutin
 - d. Melakukan analisis log secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)
 - e. Memutakhirkan rekaman dan hasil analisa (jejak audit - audit trail) secara rutin dan sistematis
 - f. Menindaklanjuti laporan penyerangan virus/malware yang gagal/sukses

Jakarta, 28 Desember 2018

Narasumber Instansi:
DISKOMINFOTIK PROV DKI JAKARTA

1. ANDRIE YUSWANTO

2. RYCAN FAHMI

3. TONY YUDIANTO

4. YUNIARTO

5. YULI WAHYUDIANTO

6. DWIANA KUSUMASARI

Assessor Indeks KAMI:

1. Assessor Utama:
KAUTSARINA

2. Assessor Pendamping:
PANCAT SETYANTANA

3. Administrator:
JULYSA TRI WULANDARI

4. Administrator:
SITI MASMUAH