
	<b>LAPORAN ONSITE ASSESMENT INDEKS KAMI</b>	 <b>INDEKS KEAMANAN INFORMASI</b>												
<b>Instansi/Perusahaan:</b> Dinas Komunikasi dan Informatika Pemerintah Kota Tangerang Selatan (Pemkot Tangsel)	<b>Narasumber Instansi/Perusahaan:</b> <ol style="list-style-type: none"> <li>1. Syaiful Bachri, S.Sos</li> <li>2. Eva Suryani, S.SiT, MT</li> <li>3. Ellya Mufidah, S.Ikom</li> <li>4. Jimmy Alberto, ST</li> <li>5. Dimaz Arno, ST, M.Kom</li> <li>6. Irfan Rasyidi, S.Si</li> <li>7. Edi Rasidi, SE</li> <li>8. R. Adhyaksa Raharjo, S.T</li> <li>9. Ibnu Mas'ud, S.Kom</li> <li>10. Talitha U.A, S.IKom</li> </ol>													
<b>Unit Kerja:</b> Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian	<b>Tel:</b> (021) 74646336													
<b>Alamat:</b> Jl. Maruga Raya No. 1 Kelurahan Serua – Kecamatan Ciputat Kota Tangerang Selatan, Banten	<b>Pimpinan Unit Kerja:</b> Kepala Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian													
<b>Email:</b> diskominfo@tangerangselatankota.go.id														
<p>A. <u>Ruang Lingkup:</u></p> <p>Pengelolaan Data Center pada Dinas komunikasi dan Informatika Kota Tangerang Selatan</p> <p><b>1. Instansi / Unit Kerja:</b></p> <p>Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian, Dinas Komunikasi dan Informatika Tangerang Selatan</p> <p><b>2. Fungsi Kerja</b></p> <p>Membantu Kepala Dinas dalam menyelenggarakan aplikasi dan integrasi sistem informasi, infrastruktur dan jaringan komunikasi, serta persandian dan keamanan informasi.</p> <p><b>3. Lokasi:</b></p> <table border="1" data-bbox="316 1765 1374 2022"> <thead> <tr> <th>No</th> <th>Nama Lokasi</th> <th>Alamat</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Kantor</td> <td>Jl. Maruga Raya No.1 Serua-Ciputat</td> </tr> <tr> <td>2</td> <td>Data Center</td> <td>Jl. Maruga Raya No.1 Serua-Ciputat</td> </tr> <tr> <td>3</td> <td>Disaster Recovery Center</td> <td>Colocation Kerjasama dengan BPPT (LPSE)</td> </tr> </tbody> </table>			No	Nama Lokasi	Alamat	1	Kantor	Jl. Maruga Raya No.1 Serua-Ciputat	2	Data Center	Jl. Maruga Raya No.1 Serua-Ciputat	3	Disaster Recovery Center	Colocation Kerjasama dengan BPPT (LPSE)
No	Nama Lokasi	Alamat												
1	Kantor	Jl. Maruga Raya No.1 Serua-Ciputat												
2	Data Center	Jl. Maruga Raya No.1 Serua-Ciputat												
3	Disaster Recovery Center	Colocation Kerjasama dengan BPPT (LPSE)												

**B. Nama /Jenis Layanan Publik:**

Layanan yang masuk ruang lingkup adalah Sistem Layanan Infrastruktur (Data Center, Aplikasi, Jaringan, Server) Sistem Informasi dan Sistem Komunikasi yang dikelola oleh Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian, Dinas Komunikasi dan Informatika Tangerang Selatan.

**C. Aset TI yang kritikal:**

1. Informasi:

- Data Pribadi
- KTP
- Kartu Keluarga
- Data Kepegawaian Pegawai
- Data LPSE (dokumen LPSE)

2. Aplikasi:

- Sisumaker
- Lasik
- Amando
- Simral
- PPDB
- Siaran Tangsel
- Website CSIRT

3. Server:

Nutanix

**D. DATA CENTER (DC):**

ADA, berada pada tempat khusus pada lantai 7 dan pemilihan lokasi didasarkan pada pertimbangan konstruksi gedung. Data Center Diskominfo Pemkot Tangerang Selatan memiliki fasilitas dan peralatan sebagai berikut:

- Ruang Data Center memiliki satu pintu masuk dan tidak memiliki pintu darurat.
- Perimitri untuk akses masuk sudah menggunakan akses *fingerprint* dan RFID.
- Perimitri untuk mengukur suhu, kelembaban, tegangan, dll pada ruangan Data Center sudah terpantau melalui sistem aplikasi **SmartRow**, salah satu produk dari Vertiv yang digunakan dalam pengelolaan infrastruktur Data Center secara terpusat seperti power management, penyediaan rak data center dengan teknologi pendinginan, UPS dan monitoring serta kontrol presisi yang dapat dilakukan secara *realtime*.
- CCTV untuk monitoring perangkat pengelolaan informasi pada Data Center berjalan dengan baik dan recorder CCTV disimpan dalam periode jangka waktu tertentu. Salah satu perangkat CCTV terpasang di luar ruangan Data Center dengan tujuan untuk memberikan informasi aktivitas keluar masuk personil.
- Pengecekan grounding dilaksanakan satu kali saat implementasi **SmartRow**.
- Sarana pendukung untuk kondisi kebakaran di dalam Data Center sudah diakomodasi dengan menggunakan APAR sebanyak 1 (satu) unit.
- Belum adanya panduan/aturan/informasi tertulis yang memberikan penjelasan terkait dengan hal yang diperbolehkan/dilarang dilakukan pada ruangan Data Center (tulisan peringatan).

**E. DISASTER RECOVERY CENTER (DRC):**

Belum memiliki konsep Disaster Recovery Center secara menyeluruh, namun untuk layanan LPSE telah dialokasikan kerjasama dengan BPPT untuk proses *back up* data center layanan tersebut (*Colocation*).

**Status Ketersediaan Dokumen (Kebijakan/Prosedur)**

Table 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

No	Nama Kebijakan	Cakupan Dokumen	Ada/Tidak
1	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain: <ul style="list-style-type: none"><li>• Definisi, sasaran dan ruang lingkup keamanan informasi</li><li>• Persetujuan terhadap kebijakan dan program keamanan informasi</li><li>• Kerangka kerja penetapan sasaran kontrol dan kontrol</li><li>• Struktur dan metodologi manajemen risiko</li><li>• Organisasi dan tanggungjawab keamanan informasi</li></ul>	√
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggungjawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah	√
3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara internal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan ( <i>confidentiality</i> ), keutuhan ( <i>integrity</i> ) dan ketersediaan ( <i>availability</i> ) informasi.	√
4	Kebijakan Manajemen Risiko TIK	Berisi metodologi/ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi	√

		risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.	
5	Kerangka Kerja Manajemen Kelangsungan Usaha ( <i>Business Continuity Management</i> )	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana/darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.	√
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).	√

No	Nama Prosedur/ Pedoman	Cakupan Dokumen	Ada/Tidak
1	Pengendalian Dokumen	Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan jika tidak digunakan, daftar dan pengendalian dokumen eksternal yang menjadi rujukan	√
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi	√
3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor	√
4	Tindakan Perbaikan & Pencegahan	Berisi tatacara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TI	√
5	Pelabelan, Pengamanan, Pertukaran & Disposasi Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/data "rahasia" baik softcopy maupun hardcopy, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada Instansi	√
6	Pengelolaan Removable Media & Disposasi Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (tape/hard disk/Flashdisk/CD) dan penghapusan informasi ataupun penghancuran media	√

7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Berisi proses monitoring penggunaan CPU, storage, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil monitoring	√
8	<i>User Access Management</i>	Berisi proses dan tatacara pendaftaran, penghapusan dan review hak akses user, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, database, internet, email dan internet)	√
9	<i>Teleworking</i>	Pengendalian dan pengamanan penggunaan hak akses secara remote (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.	√
10	Pengendalian instalasi software & Hak Kekayaan Intelektual	Berisi daftar software standar yang diijinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan software yang tidak diijinkan	√
11	Pengelolaan Perubahan ( <i>Change Management</i> ) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/database/versi dari aset TIK yang mengalami perubahan.	√
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan/pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.	√

**Dokumen-dokumen yang diperiksa:**

1. Kebijakan Sistem Manajemen Keamanan Informasi
2. Kebijakan Keamanan Informasi
3. Kebijakan Kepatuhan Sistem Informasi
4. SOP Audit Internal
5. SOP Manajemen Risiko Keamanan Informasi
6. SOP Tindakan Perbaikan
7. SOP *Business Continuity Plan*
8. SOP Manajemen dan Klasifikasi Aset TI
9. SOP Manajemen Insiden
10. SOP Kerjasama Supplier
11. SOP Manajemen Akses User
12. SOP Rencana Kapasitas Infrastruktur
13. SOP Pembangunan Sistem
14. SOP Pendaftaran Nama Domain
15. Standar Keamanan Fisik dan Lingkungan
16. Standar Keamanan Sumber Daya Manusia
17. Standar *Mobile Device dan Teleworking*
18. Standar Keamanan Operasional

19. SOP Kriptografi
20. SOP Rapat Tinjauan Manajemen
21. Formulir NDA Diskominfo
22. Rencana Sistem Manajemen Keamanan Informasi
23. Standar Sistem Manajemen Keamanan Informasi
24. *Business Continuity Planning*
25. Notulen-notulen dan SOP Teknis lainnya pada Kegiatan Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian

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

#### **I. KONDISI UMUM:**

A. Struktur organisasi satuan kerja dalam ruang lingkup berada di bawah Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian, Dinas Komunikasi dan Informatika Kota Tangerang Selatan.

Bidang Pengelolaan Teknologi Informasi Komunikasi dan Persandian terdiri atas:

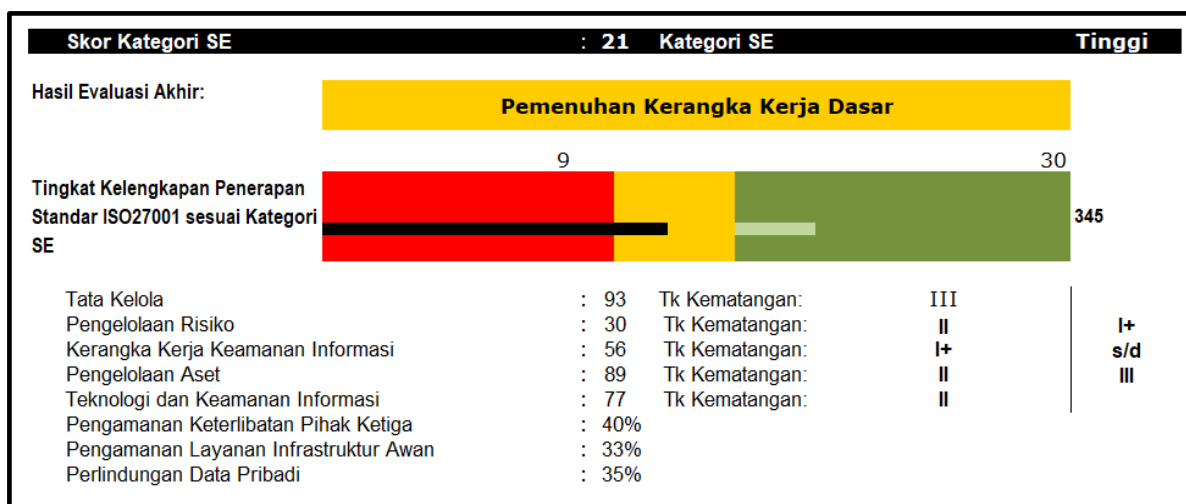
1. Seksi Aplikasi dan Integrasi Sistem Informasi;
2. Seksi Infrastruktur dan Jaringan Komunikasi; dan
3. Seksi Persandian dan Keamanan Informasi.

B. SDM pengelola terdiri dari:

- 58 orang PNS dan pegawai tenaga ahli/kontrak.

C. Berdasarkan verifikasi terhadap hasil *Self Assessment* isian file Indeks KAMI diperoleh hasil sebagai berikut:

**Total Score Sebelum Verifikasi: 345**



## Total Score Setelah Verifikasi: 405

Indeks KAMI (Keamanan Informasi)						
<b>Responden:</b> Dinas Komunikasi dan Informatika Kota Tangerang Selatan  Jl. Maruga Raya No.1, Serua Ciputat, Kota Tangerang Selatan Propinsi Banten, 15414  021 74776311 sandi@tangerangselatankota.go.id 17/02/2021	<b>Skor Kategori SE</b>		<b>: 33</b>	<b>Kategori SE</b>	<b>Tinggi</b>	
	Hasil Evaluasi Akhir:		Pemenuhan Kerangka Kerja Dasar			
	Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai		<div><div></div><div></div><div></div><div></div></div> <div>30405</div>			
	Tata Kelola		: 105	Tk Kematangan:	III	II s/d III
	Pengelolaan Risiko		: 45	Tk Kematangan:	III	
Kerangka Kerja Keamanan Informasi		: 56	Tk Kematangan:	II		
Pengelolaan Aset		: 117	Tk Kematangan:	II		
Teknologi dan Keamanan Informasi		: 82	Tk Kematangan:	II+		
Pengamanan Keterlibatan Pihak Ketiga		: 41%				
Pengamanan Layanan Infrastruktur Aw		: 33%				
Perlindungan Data Pribadi		: 35%				

### Gap Analisis hasil *self assessment* internal dan Verifikasi oleh tim BSSN adalah:

- Penilaian *self assessment* yang dilakukan oleh Tim Pemkot Tangerang Selatan dengan menggunakan instrumen Indeks KAMI versi 4.1 dengan hasil diperoleh adalah:
  - Skor Kategori yang diperoleh adalah sejumlah 21 poin dengan pengelompokan kategori berdasarkan asas risiko yaitu kategori Sistem Elektronik Tinggi.
  - Nilai skor akhir yang diperoleh dari hasil penilaian adalah 345 dengan hasil status kesiapan berada dalam Pemenuhan Kerangka Kerja Dasar dan hasil tingkat kematangan dari 5 area (Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset dan Teknologi Keamanan Informasi) berada pada tingkat I+ sampai dengan III.
  - Penilaian suplemen untuk tiga ruang lingkup yaitu pengamanan dan keterlibatan pihak ketiga, pengamanan layanan infrastruktur awan dan perlindungan data pribadi diperoleh persentase rata-rata sejumlah 36,09%
- Penilaian verifikasi yang dilakukan oleh Tim BSSN dengan menggunakan instrumen Indeks KAMI versi 4.2 dengan hasil diperoleh adalah:
  - Skor Kategori yang diperoleh adalah sejumlah 33 poin dengan pengelompokan kategori berdasarkan asas risiko yaitu kategori Sistem Elektronik Tinggi.
  - Nilai skor akhir yang diperoleh dari hasil penilaian adalah 405 dengan hasil status kesiapan berada dalam Pemenuhan Kerangka Kerja Dasar dan hasil tingkat kematangan dari 5 area (Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset dan Teknologi Keamanan Informasi) berada pada tingkat II sampai dengan III.
  - Penilaian suplemen untuk tiga ruang lingkup yaitu pengamanan dan keterlibatan pihak ketiga, pengamanan layanan infrastruktur awan dan perlindungan data pribadi diperoleh persentase rata-rata sejumlah 36,5%
- Diperoleh hasil gap analisis dari dua hasil penilaian adalah:
  - Pada penetapan kategori terdapat perbedaan skor sejumlah 12 poin lebih besar dari hasil *self assessment*, namun untuk pengelompokan kategori masih berada dalam lingkup yang sama yaitu kategori Sistem Elektronik Tinggi.
  - Hasil skor akhir dari lima area penilaian terdapat perbedaan sejumlah 60 poin lebih besar dari hasil *self assessment*. Untuk tingkat kematangan terdapat perubahan pada batas bawah, yang sebelumnya adalah tingkat I+, sedangkan hasil verifikasi adalah tingkat II. Untuk batas atas tingkat kematangan adalah sama yaitu pada tingkat III.
  - Penilaian suplemen terdapat perbedaan nilai sejumlah 0,41%.

## **II. ASPEK TATA KELOLA:**

### **A. Kekuatan/Kematangan**

1. Diskominfo Pemkot Tangsel telah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen melalui sekumpulan kebijakan dan regulasi yang dijadikan panduan dalam penerapan pelaksanaan kegiatan khususnya dalam mengoptimalkan fungsi persandian untuk penyelenggaraan keamanan informasi sesuai dengan peraturan perundang-undangan yang berlaku.
2. Pimpinan dari Diskominfo Pemkot Tangsel secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, hal ini ditandai dengan adanya norma, standar, prosedur dan kriteria yang telah ditetapkan sebagai dasar teknis pelaksanaan kegiatan penerapan keamanan informasi pada lingkup tugasnya.
3. Diskominfo Pemkot Tangsel memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi
4. Diskominfo Pemkot Tangsel sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi.
5. Pimpinan satuan kerja di Diskominfo Pemkot Tangsel telah menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
6. Diskominfo Pemkot Tangsel sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporannya.
7. Diskominfo Pemkot Tangsel telah menerapkan program kedisiplinan dalam menjalankan keamanan informasi sesuai dengan prosedur dimana penerapan proses tersebut dilakukan secara formal melalui penetapan Indikator Kinerja dan dinilai secara periodik melalui SKP Pimpinan sampai dengan level individu.

### **B. Kelemahan/Kekurangan**

1. Diskominfo Pemkot Tangsel belum mendefinisikan persyaratan/standar kompetensi dan keahlian khusus terkait pelaksana pengelolaan keamanan informasi dalam bentuk kebijakan yang ditetapkan oleh pimpinan/organisasi. Kondisi saat ini memang telah diidentifikasi persyaratan kompetensi untuk menjalankan tugas secara umum namun belum ada mekanisme secara tertulis peningkatan kompetensi yang akan dilakukan dapat memenuhi persyaratan/standar yang diharapkan.
2. Belum menetapkan penanggung jawab untuk memutuskan, merancang, melaksanakan, dan mengelola langkah keberlangsungan layanan TIK dimana perlu ada pembagian pengelola kelangsungan layanan dalam bagian-bagian tertentu secara khusus sehingga dari pembagian tugas yang dilakukan per bagian akan dapat membuat analisis dampak bisnis dari proses mitigasi yang dilakukan akan menjadi prasyarat perencanaan keberlangsungan bisnis dan pemulihan bencana organisasi serta dapat meminimalkan situasi dan kondisi yang merugikan organisasi.
3. Belum mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku. Meskipun telah tercantum bentuk pengamanan informasi pribadi dalam dokumen kebijakan kepatuhan sistem informasi namun masih memerlukan kebijakan secara terpisah yang akan menjelaskan bentuk perlindungan terhadap jenis data pribadi tertentu dan mengkomunikasikannya dengan pihak yang terlibat dalam pengelolaan data pribadi baik secara tertulis maupun secara verbal seperti sosialisasi atau banner/poster pemberitahuan.



### **III. ASPEK RISIKO:**

#### **A. Kekuatan/Kematangan**

1. Diskominfo Pemkot Tangsel telah menetapkan penanggung jawab proses manajemen risiko dan menetapkan bentuk eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan.
2. Kerangka kerja pengelolaan risiko keamanan informasi sudah disusun dan terdokumentasi dengan baik dimana di dalamnya telah mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut hingga dampak kerugiannya serta telah menetapkan ambang batas tingkat risiko yang dapat diterima oleh organisasi.
3. Diskominfo Pemkot Tangsel telah melakukan identifikasi ancaman dan kelemahan yang terkait dengan aset informasi dan menetapkan dampak kerugian akibat hilangnya/terganggunya aset utama yang dimiliki ke dalam form daftar risiko (*risk register*) Data Center.
4. Diskominfo Pemkot Tangsel telah menyusun langkah mitigasi dan penanggulangan risiko sesuai tingkat prioritas dengan target waktu penyelesaiannya dan penanggungjawabnya.

#### **B. Kelemahan/Kekurangan**

1. Diskominfo Pemkot Tangsel belum melakukan monitoring dan evaluasi terhadap status penyelesaian langkah mitigasi risiko yang telah disusun baik secara periodik sesuai dengan jadwal waktu yang telah ditetapkan.
2. Diskominfo Pemkot Tangsel belum melakukan pengkajian ulang sebagai bentuk akurasi dan validasi terhadap kerangka kerja pengelolaan risiko dan profil risiko berikut bentuk mitigasinya yang perlu dilakukan secara berkala.
3. Diskominfo Pemkot Tangsel belum melakukan penilaian risiko sebagai bagian dari implementasi program yang dapat mengintegrasikan seluruh bagian dari bisnis proses organisasi dan menjadi bagian dari kriteria penilaian obyektif kinerja efektivitas pengamanan.

### **IV. ASPEK KERANGKA KERJA:**

#### **A. Kekuatan/Kematangan**

1. Diskominfo Pemkot Tangsel sudah memiliki proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetakannya sebagai insiden keamanan informasi untuk ditindaklanjuti sesuai prosedur yang diberlakukan.
2. Dokumen kontrak dengan pihak ketiga sudah mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
3. Diskominfo Pemkot Tangsel telah menjadikan aspek keamanan informasi menjadi bagian dari ruang lingkup manajemen proyek dan dituangkan dalam bagian dari kebijakan keamanan informasi yang telah dibuat identifikasi dan mitigasi risikonya.

#### **B. Kelemahan/Kekurangan**

1. Belum adanya kebijakan dan prosedur maupun dokumen teknis/operasional lainnya yang diperlukan dalam mendukung program keamanan informasi dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang dalam penerapannya.
2. Belum adanya proses review/evaluasi kebijakan dan prosedur yang telah disusun sebagai bagian dari peningkatan efektivitas dan penyesuaian kondisi saat ini baik melalui

kegiatan publikasi kepada pihak terkait termasuk pihak ketiga yang berkepentingan terhadap bisnis proses organisasi.

3. Belum adanya penerapan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan baik dalam pembahasan secara formal maupun yang dituangkan dalam formulir evaluasi rencana pengadaan/implementasi sistem TI.
4. Belum adanya penerapan mekanisme proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar keamanan platform teknologi.
5. Belum adanya dokumen *Disaster Recovery Plan* yang mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim dan pelaksanaan uji cobanya belum dilakukan secara berkala sesuai dengan jadwal yang telah ditetapkan.
6. Diskominfo Pemkot Tangsel belum mendefinisikan konsekuensi dari adanya pelanggaran kebijakan keamanan informasi yang dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.
7. Diskominfo Pemkot Tangsel belum melakukan uji dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada.
8. Belum adanya mekanisme dan prosedur resmi terhadap pengelolaan suatu pengecualian terhadap penerapan keamanan informasi, termasuk tindak lanjut konsekuensi dari kondisi yang ada.

#### **V. ASPEK PENGELOLAAN ASET:**

##### **A. Kekuatan/Kematangan**

1. Diskominfo Pemkot Tangsel telah memiliki definisi klasifikasi aset informasi yang tertuang dalam kebijakan/prosedur resmi.
2. Diskominfo Pemkot Tangsel telah menerapkan proses pengecekan latar belakang SDM pengelola TIK.
3. Prosedur terkait kontrol terhadap user yang mutasi/keluar atau tenaga ahli/kontrak (*outsourcing*) yang habis masa kerjanya sudah ada dan sudah diterapkan.
4. Pengamanan fasilitas fisik (lokasi kerja) sudah diterapkan secara berlapis sesuai dengan kepentingan/klasifikasi aset informasi.
5. Diskominfo Pemkot Tangsel telah menerapkan perlindungan terhadap infrastruktur komputasi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikaan dan dalam konstruksinya telah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukungnya.

##### **B. Kelemahan/Kekurangan**

1. Belum adanya inventaris aset informasi secara keseluruhan/lengkap sesuai *scope* secara akurat dan terpelihara dengan informasi tambahan pemilik aset yang akan bertanggung jawab dalam pemeliharaannya.
2. Belum adanya proses evaluasi aset informasi sesuai tingkat kepentingan aset bagi Diskominfo Pemkot Tangsel dan keperluan pengamanannya belum didefinisikan.
3. Proses pengelolaan konfigurasi belum diterapkan secara konsisten.
4. Belum diimplementasikannya secara menyeluruh dokumen kebijakan tata tertib penggunaan perangkat TIK dan pengamanannya.
5. Diskominfo Pemkot Tangsel belum menerapkan pengelolaan aset informasi berupa identitas elektronik, pengelolaan/pemberian akses dan proses otentikasi serta otorisasi termasuk kebijakan terhadap pelanggarannya secara menyeluruh.

6. Belum adanya penerapan proses pengamanan lokasi kerja yang diterapkan dari risiko terhadap aset informasi dan dari keberadaan/kehadiran pihak ketiga.

## **VI. ASPEK TEKNOLOGI:**

### **A. Kekuatan/Kematangan**

1. Layanan dan sistem yang dikelola dan akses ke administrasi sistem sudah menerapkan lebih dari 1 (satu) lapis pengamanan.
2. Diskominfo Pemkot Tangsel sudah menerapkan segmentasi jaringan sesuai dengan kepentingannya.
3. Jaringan, sistem dan aplikasi yang digunakan telah dilakukan pemindaian secara rutin dan berkala.
4. Diskominfo Pemkot Tangsel telah menerapkan mekanisme perekaman secara otomatis terhadap perubahan dalam sistem informasi dan terdapat pengaturan/pembatasan terhadap upaya akses oleh yang tidak berhak/berkepentingan.
5. Adanya kebijakan penerapan standar dalam implementasi enkripsi yang digunakan secara menyeluruh.

### **B. Kelemahan/Kekurangan**

1. Sistem dan aplikasi yang dibuat masih belum menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama.
2. Belum adanya analisa kepatuhan penerapan konfigurasi standar.
3. Diskominfo Pemkot Tangsel belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

## **VIII. REKOMENDASI**

1. Dalam rangka menjaga seluruh aset di Diskominfo Pemkot Tangsel khususnya data dan informasi sebagai aset yang perlu dijaga dan dilindungi, maka perlu menerapkan program *capacity building* terhadap pegawai melalui pelatihan dan sertifikasi ISO 27001 Implementator untuk kompetensi auditor keamanan informasi internal, sertifikasi ISO 27001 Lead Auditor, Sertifikasi CISM untuk mengelola, mendesain, mengawasi dan atau menilai keamanan informasi, CRISC untuk mengidentifikasi dan mengelola risiko melalui pengembangan, implementasi dan pemeliharaan sistem informasi, Certified Ethical Hacking untuk meningkatkan kompetensi pelaksanaan kegiatan penetration testing dan lainnya.
2. Diskominfo Pemkot Tangsel perlu untuk melakukan evaluasi terhadap seluruh kebijakan keamanan informasi yang telah dimiliki dan perlu adanya monitoring terhadap implementasinya yang dilakukan secara periodik dalam rangka mengantisipasi adanya kejadian/insiden yang akan merugikan organisasi dan berdampak terhadap reputasi maupun dampak signifikan lainnya.
3. Diskominfo Pemkot Tangsel perlu melakukan pemantauan dan evaluasi terhadap status penyelesaian langkah mitigasi risiko yang telah diidentifikasi secara berkala.
4. Diskominfo Pemkot Tangsel perlu melakukan pengkajian ulang secara berkala terhadap kerangka kerja pengelolaan risiko dan profil risiko berikut bentuk mitigasinya.
5. Kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi perlu disusun dan dituliskan dengan jelas termasuk mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya

6. Perlunya Diskominfo Pemkot Tangsel untuk memperhatikan penerapan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi.
7. Diskominfo Pemkot Tangsel penting untuk menyusun *disaster recovery plan* sebagai bagian dari tahap perencanaan yang akan dilakukan dalam rangka proses *recovery* setelah terjadinya bencana termasuk mendefinisikan peran, wewenang dan tanggung jawab tim yang telah diberikan tugas.
8. Diskominfo Pemkot Tangsel perlu melakukan evaluasi secara berkala terhadap kebijakan dan prosedur keamanan informasi yang sudah dibuat.
9. Diskominfo Pemkot Tangsel perlu melakukan uji dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada.
10. Pentingnya melakukan pengelolaan konfigurasi dilakukan secara konsisten dan perlu keterlibatan pihak independen dalam mengkaji kehandalan keamanan informasi.
11. Diskominfo Pemkot Tangsel perlu menyusun proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga dengan membuat buku catatan bagi tamu/pengunjung, penerapan kartu identitas yang ditukar untuk setiap tamu yang akan masuk pada lokasi kerja terbatas.
12. Diskominfo Pemkot Tangsel perlu memperhatikan sistem dan aplikasi yang dibuat secara otomatis mengatur penggantian password, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
13. Diskominfo Pemkot Tangsel perlu untuk melakukan peningkatan pengelolaan pengamanan keterlibatan pihak ketiga penyedia layanan melalui proses penyusunan kebijakan yang ditetapkan dan dievaluasi secara berkala mulai dari proses identifikasi risiko sampai dengan kelangsungan layanan dengan pihak ketiga.
14. Diskominfo Pemkot Tangsel perlu untuk meningkatkan prosedur pengamanan layanan infrastruktur awan yang dikelola melalui penerapan kebijakan secara tertulis dan kajian risiko serta melakukan evaluasi terhadap implementasinya baik terhadap standar keamanan teknis dan pemenuhan sertifikasi layanan berbasis ISO 27001.
15. Diskominfo Pemkot Tangsel perlu untuk menerapkan kebijakan terkait dengan perlindungan data pribadi dan mendorong kesadaran tentang pentingnya perlindungan data pribadi baik internal maupun pengguna layanan (publik) dengan merujuk pada peraturan perundang-undangan yang telah ada.

<p><b>Tangerang Selatan,</b> Dinas Komunikasi dan Informatika Kota Tangerang Selatan</p> <p>1. Nama: Syaiful Bachri, S.Sos</p> <p>2. Nama: Eva Suryani, S.SiT, MT</p> <p>3. Nama: Jimmy Alberto, ST</p> <p>4. Nama: Ellya Mufidah, S.Ikom</p>	<p><b>Assessor Indeks KAMI:</b> Badan Siber dan Sandi Negara</p> <p>1. Lead Assessor: Nurchaerani, S.E.</p> <p>2. Asesor: Diah Sulistyowati, S.Kom</p> <p>3. Asesor: Ikrima Galuh Nasucha, S.Tr.TP</p> <p>4. Asesor: Ni Putu Ayu Lhaksmi Wulansari, S.Tr.TP</p>
---	---