



# LAPORAN ONSITE ASSESSMENT INDEKS KAMI



INDEKS  
KEAMANAN  
INFORMASI

<b>Instansi/Perusahaan:</b> PEMERINTAH PROVINSI KALIMANTAN TENGAH	<b>Pimpinan Unit Kerja :</b> Agus Siswadi, S.Pd., M.Pd 19680204 199903 1 007
<b>Unit Kerja:</b> DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK	<b>Narasumber Instansi :</b> 1. Billy Bareto, S.T, 19761123 200604 1 006 2. Marlin Pakondo, SE, M.Si, 19720313 199803 2 008 3. Nursinta Uli Situmorang, S.H., 19671116 199403 2 007 4. Ari Gunadi Palilu, S.Kom, MT, 19870219 201001 1 002 5. Restiasih Pratiwi, ST, 1991062 201903 2 017 6. Ashadi Noor, 19831026 201402 1 002 7. Ivan Oktobrian, S.kom, 19901005 201101 1 001
<b>Alamat:</b> Jl. Tjilik Riwut Km. 3.5 Palangka Raya, Kalimantan Tengah	
<b>Email:</b> diskomin@kalteng.go.id	<b>Asesor :</b> 1. Nurchaerani, S.E. 19650708 198710 2 003 2. Irma Nurfitri Handayani, S.ST. 19850303 200501 2 002 3. Ikrima Galuh Nasucha, S. Tr. TP. 19930329 201412 2 002 4. Ni Putu Ayu Lhaksmi Wulandari, S.Tr.TP 19960622 201812 2 001
<b>Tel/ Fax:</b> -	

## A. Ruang Lingkup:

### 1. Instansi / Unit Kerja:

Dinas Komunikasi, Informatika, Persandian dan Statistik Pemerintah Provinsi Kalimantan Tengah.

### 2. Fungsi Kerja:

Sebagaimana Peraturan Gubernur Kalimantan Tengah Nomor 43 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Komunikasi,

Informatika, Persandian dan Statistik Provinsi Kalimantan Tengah mempunyai tugas pokok membantu Gubernur dalam melaksanakan kewenangan desentralisasi dan dekonsentrasi di bidang Komunikasi, Informatika, Persandian dan Statistik sesuai dengan kebijaksanaan yang ditetapkan berdasarkan ketentuan peraturan perundang-undangan. Untuk melaksanakan tugas sebagaimana dimaksud dalam Pasal 3, Dinas Komunikasi, Informatika, Persandian dan Statistik menyelenggarakan fungsi :

- Perumusan dan pelaksanaan kebijakan teknis bidang Komunikasi, Informatika, Persandian dan Statistik sesuai dengan rencana strategis yang ditetapkan pemerintah daerah;
- Evaluasi, pengendalian dan pelaporan kebijakan teknis bidang komunikasi, Informatika, Persandian dan Statistik sesuai dengan rencana strategis yang ditetapkan Pemerintah Daerah;
- Bimbingan teknis bidang Komunikasi, Informatika, Persandian dan Statistik sesuai dengan rencana strategis yang ditetapkan Pemerintah Daerah;
- Penyelenggaraan urusan kesekretariatan;
- Pembinaan jabatan fungsional, dan
- Pelaksanaan tugas lain yang diberikan oleh atasan sesuai dengan bidang tugasnya.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Tjilik Riwut Km. 3.5 Palangka Raya, Kalimantan Tengah
2	<i>Data Center</i>	Jl. Tjilik Riwut Km. 3.5 Palangka Raya, Kalimantan Tengah
3	<i>Disaster Recovery Center (DRC)</i>	-

B. Nama /Jenis Layanan Publik:

Layanan infrastruktur data center dan aplikasi sistem informasi yang dikelola oleh Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Kalimantan Tengah.

C. Aset TI yang kritikal:

1. Informasi:
  - a. NIP;
  - b. NIK;
  - c. NPWP
  - d. Data Pribadi keluarga

- e. Berkas-berkas bersifat terbatas, rahasia, dan rahasia yang dimasukkan ke dalam sistem.
2. Aplikasi:  
aplikasi SITAGUH (<https://sitaguh.bkd.kalteng.go.id>)
3. Server :  
server di data center dan pendukungnya.
4. Infrastruktur Jaringan/Network:  
Fiber optic Icon +, Telkom, Lintas Data Prima Internet dan Intranet

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

- ADA, dalam ruangan khusus (Ruang server dikelola internal)
- ADA, jadi satu dengan ruang kerja
- TIDAK ADA

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

- ADA       Dikelola Internal       Dikelola Vendor :
- TIDAK ADA

**Status Ketersediaan Dokumen Kerangka Kerja**

**Sistem Manajemen Keamanan Informasi (SMKI)**

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	<b>Kebijakan, Sasaran, Rencana, Standar</b>			
1	Kebijakan Keamanan Informasi	Ya		Pergub Garsan No 11 Tahun 2018
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		Pergub No 43 Tahun 2016
3	Panduan Klasifikasi Informasi	Ya		Pergub Garsan No 11 Tahun 2018, Perda No 5 tahun 2013

4	Kebijakan Manajemen Risiko TIK	YA		Kebijakan Manajemen Risiko TI	
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)	YA		D	
6	Kebijakan Penggunaan Sumberdaya TIK		Tdk		
	<b>Prosedur/ Pedoman:</b>				
1	Pengendalian Dokumen	Ya			
2	Pengendalian Rekaman/Catatan	Ya			
3	Audit Internal SMKI		Tdk		
4	Tindakan Perbaikan & Pencegahan		Tdk		
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Ya		Pergub Garsan No 11 Tahun 2018	
6	Pengelolaan Removable Media & Disposal Media		Tdk		
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Ya		SOP Hak Akses Ruang Data Center	
8	User Access Management		Tdk		
9	Teleworking	Ya		SOP Permohonan hak Akses Aplikasi (Remote)	
10	Pengendalian instalasi software & HAKI		Tdk		
11	Pengelolaan Perubahan (Change Management) TIK	Ya		SOP Pengelolaan Perubahan	
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi		Tdk		

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

**Dokumen yang diperiksa:**

1. Peraturan Gubernur Kalimantan Tengah Nomor 43 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Kalimantan Tengah.
2. Peraturan Gubernur Kalimantan Tengah Nomor 11 Tahun 2018 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Kalimantan Tengah.
3. Peraturan Gubernur Kalimantan Tengah Nomor 45 Tahun 2018 tentang Rencana Induk Teknologi Informasi dan Komunikasi di Lingkungan Provinsi Kalimantan Tengah.
4. Peraturan Gubernur Nomor 38 Tahun 2020 tentang Pengelolaan Arsip Vital di Lingkungan Pemerintah Provinsi Kalimantan Tengah
5. Peraturan Gubernur Nomor 39 Tahun 2020 tentang Jadwal Retensi Arsip Substantif di Lingkungan Pemerintah Provinsi Kalimantan Tengah.
6. Peraturan Daerah No 5 Tahun 2013 tentang Pelayanan Informasi Publik Provinsi Kalimantan Tengah.a
7. Dokumen Pelaksanaan Anggaran Satuan Kerja Perangkat Daerah (DPA SKPD) Tahun Anggaran 2022 Dinas Komunikasi, Informatika, Persandian dan Statistik.
8. Daftar Aset Tetap Peralatan dan Mesin Tahun Anggaran 2021 Dinas Komunikasi, Informatika, Persandian dan Statistik.
9. Dokumen Renja Dinas Komunikasi, Informatika, Persandian dan Statistik tahun 2022.
10. Kebijakan Manajemen Risiko TI.
11. Panduan Teknis Pengelolaan data Center (Standar konfigurasi).
12. Dokumen Standar Tata Kelola Pusat Data Dinas Komunikasi, Informatika, Persandian dan Statistik
13. Standar Kebijakan Layanan;
14. Standar Organisasi Layanan;
15. SOP Pengelolaan Aset;
16. Standar Pengelolaan Perubahan
17. Standar Pengelolaan Kapasitas
18. SOP Akses Ruang Server
19. SOP Penggunaan fasilitas
20. SOP Pemberian Remote Akses
21. SOP Backup
22. SOP Pengelolaan Log
23. SOP Kelangsungan Layanan
24. SOP Pengelolaan Pemasok

25. SOP Penilaian Internal
26. Laporan Penyelenggaraan Persandian Tahun 2020.
27. Laporan Pentest 2021.
28. SK Tim CSIRT.

**Bukti-bukti (rekaman/arsip) penerapan SMKI:**

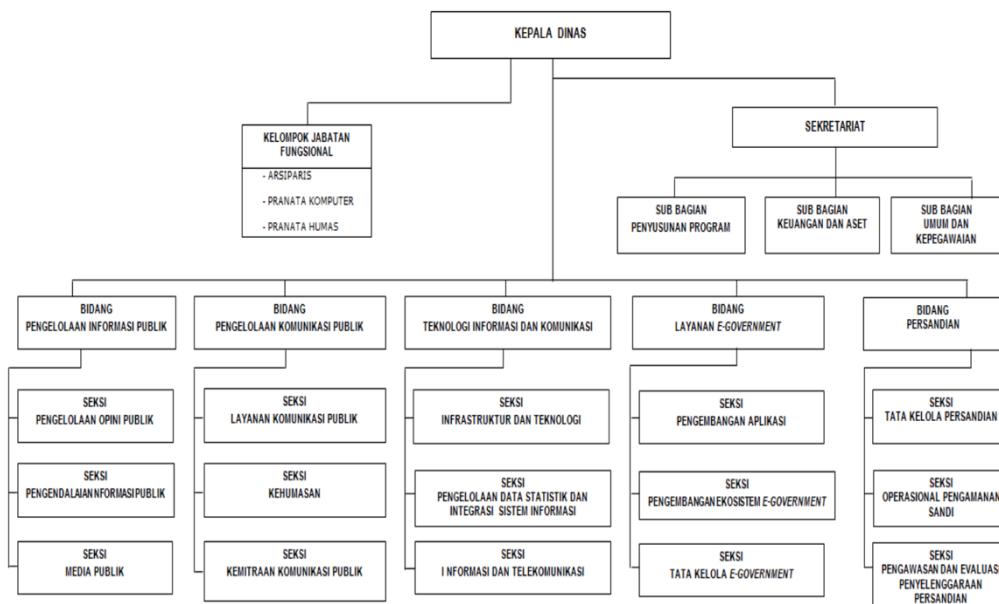
1. Matriks Kompetensi Personil Diskominfosantik Provinsi Kalimantan Tengah Tahun 2021.
2. Tangkapan Layar Aplikasi Stiaguh.
3. Kontrak Bandwidth Internet dan CCTV dan Icon +.

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

**I. KONDISI UMUM:**

1. Diskominfosantik Provinsi Kalimantan Tengah dibentuk berdasarkan Peraturan Gubernur Kalimantan Tengah Nomor 43 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Kalimantan Tengah. Adapun struktur Diskominfosantik Provinsi kalimantan Tengah adalah sebagai berikut:

BAGAN SUSUNAN ORGANISASI DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK PROVINSI KALIMANTAN TENGAH



Gambar 1. Struktur Organisasi Diskominfosantik Pemprov Kalimantan Tengah

2. SDM ASN Diskominfo dan Persandian Statistik Pemerintah Provinsi Kalimantan Tengah berjumlah 40 orang dan 26 orang tenaga kontrak.

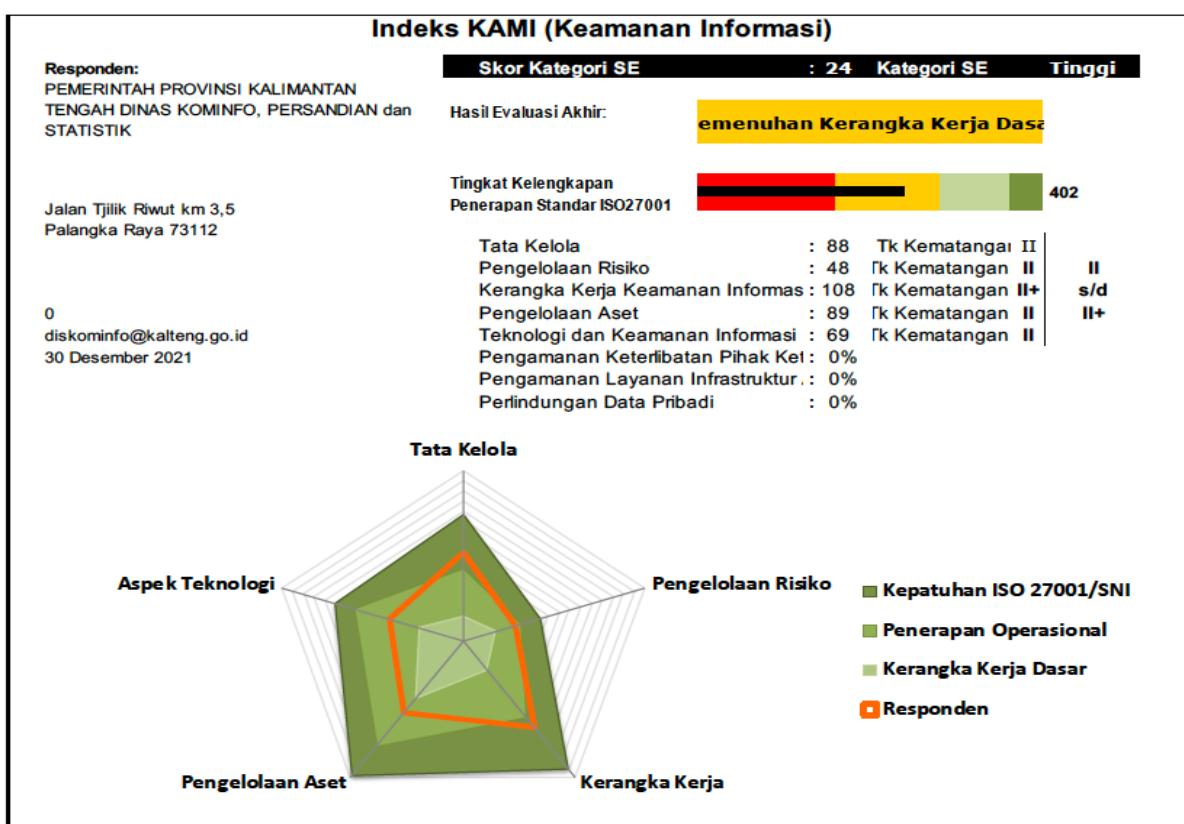
Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 dengan ruang lingkup Diskominfosantik Provinsi Kalimantan Tengah, dilakukan verifikasi oleh Tim BSSN dengan kategori Sistem Elektronik **Tinggi** dan hasil evaluasi akhir **PEMENUHAN KERANGKA KERJA DASAR** dengan total nilai **431**.

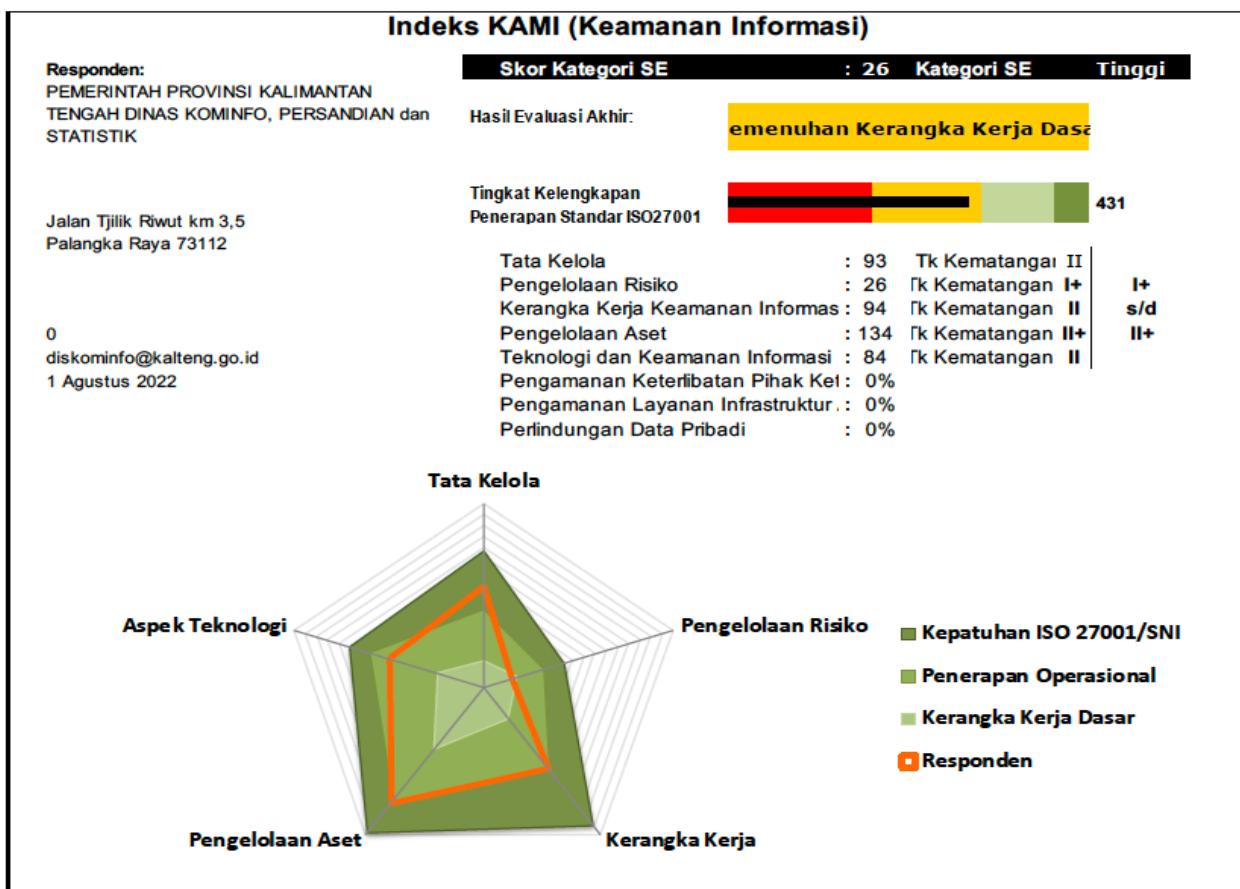
Verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI setelah melakukan pengecekan keseluruhan kelengkapan kebijakan dan/atau prosedur dan penerapan dokumen kebijakan dan/atau prosedur pada area Kategori, Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi.

Tim penilaian tahun 2022 berfokus kepada satu Sistem Elektronik yang dikelola oleh Diskominfosantik Provinsi Kalimantan Tengah dengan kategori Tinggi yaitu: Sistem Elektronik **SITAGUH**.

### **Total Score Self Assessment Penilaian Indeks KAMI Tahun 2022 Sebelum Verifikasi: 402**



## Total Score Verifikasi Penilaian Indeks KAMI Tahun 2022 Setelah Verifikasi: 431



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

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

1. Pimpinan dari Diskominfosantik Provinsi Kalimantan Tengah sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah ada penetapan kebijakan-kebijakan terkait SMKI.
2. Diskominfosantik Provinsi Kalimantan Tengah sudah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memasukan kepatuhannya.
3. Diskominfosantik Provinsi Kalimantan Tengah dan fungsi pengelola keamanan informasi sudah merencanakan dan menerapkan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi dan dievaluasi hasil penerapannya untuk memastikan kepatuhannya bagi semua pihak yang terkait.
4. Diskominfosantik Provinsi Kalimantan Tengah sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi dengan merencanakan secara berkala minimal setiap tahun dalam rangka memastikan kebutuhan penerapan kontrol keamanan informasi telah terpenuhi.
5. Koordinasi antara fungsi pengelola keamanan informasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang

berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak masih belum konsisten dan terlaksana secara memadai.

6. Tanggung jawab terhadap pengelolaan langkah kelangsungan layanan TIK (business continuity and disaster recovery plans) sebagian dirancang dalam dokumentasi yang ada. Hal ini termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat yang telah ditetapkan oleh manajemen.
7. Diskominfosantik Provinsi Kalimantan Tengah sudah menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
8. Diskominfosantik Provinsi Kalimantan Tengah sudah mendefinisikan dan menerapkan program penilaian kinerja terkait penerapan proses keamanan informasi bagi individu (pejabat & petugas) pelaksananya sebagai bagian dari proses evaluasi tingkat pemahaman individu tersebut terhadap pengelolaan keamanan informasi di organisasi.
9. Target dan sasaran pengelolaan keamanan informasi sudah didefinisikan dan diformulasikan, serta dilakukan evaluasi dan mengkaji hasil pencapaiannya secara rutin. Laporan hasil evaluasi terhadap target dan sasaran tersebut telah dilaporkan statusnya kepada pimpinan organisasi.

## B. Kelemahan/Kekurangan

1. Pejabat/petugas pelaksana pengamanan informasi sudah ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang akan dilaksanakan, namun belum menjamin kepatuhan program keamanan informasi.
2. Alokasi sumber daya terkait pelaksanaan program keamanan informasi sudah direncanakan dan disediakan dalam rangka memastikan pengelolaan keamanan informasi namun belum memadai dan belum dipastikan kepatuhannya
3. Peran fungsi pelaksana pengamanan informasi belum dipetakan terkait pengelolaan program keamanan informasi dan belum dilaksanakan secara menyeluruh melibatkan bidang-bidang lain dalam lingkup Diskominfosantik Provinsi Kalimantan Tengah, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
4. Diskominfosantik Provinsi Kalimantan Tengah belum mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
5. Belum Semua pelaksana pengamanan informasi yang terlibat di Diskominfosantik Provinsi Kalimantan tengah sudah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
6. Beberapa persyaratan keamanan informasi yang terdapat dalam standard yang berlaku sudah terintegrasi kedalam proses kerja yang ada namun sebagian lainnya masih bersifat aktivitas kontrol tambahan yang dilakukan.

7. Diskominfosantik Provinsi Kalimantan Tengah belum mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
8. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi belum mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, dan untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada.
9. Fungsi pengelola keamanan informasi sudah melaporkan kepada manajemen mengenai sebagian dari kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi secara rutin, namun laporan belum menyeluruh terkait pelaksanaan keamanan informasi.
10. Belum semua permasalahan keamanan informasi yang terjadi di Diskominfosantik Provinsi Kalimantan Tengah menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektifitas pelaksanaan kontrol keamanan informasi.
11. Metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi belum didefinisikan yang mencakup mekanisme, waktu pengukuran, pelaksananya, dan harus diukur dan dievaluasi pemantauannya secara berkala serta dilakukan eskalasi pelaporan kepada manajemen untuk memastikan efektifitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan.
12. Diskominfosantik Provinsi Kalimantan Tengah belum mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisa tingkat kepatuhannya
13. Diskominfosantik Provinsi Kalimantan Tengah belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

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

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

1. Program kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dan diterapkan secara memadai dalam proses penilaian dan evaluasi risiko.
2. Kerangka kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dalam dokumen metodologi manajemen risiko sehingga dapat digunakan secara resmi.
3. Kerangka kerja pengelolaan risiko sudah mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfosantik Provinsi Kalimantan Tengah.
4. Ambang batas tingkat risiko yang dapat diterima sudah ditetapkan oleh Diskominfosantik Provinsi Kalimantan Tengah dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa.

**B. Kelemahan/Kekurangan**

1. Diskominfosantik Provinsi Kalimantan Tengah belum menentukan penanggung jawab proses manajemen risiko yang berwenang dalam eskalasi terhadap pelaporan hasil analisa risiko keamanan informasi sampai ke tingkat pimpinan organisasi.
2. Dalam proses pengelolaan manajemen risiko, Diskominfosantik Provinsi Kalimantan Tengah belum terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
3. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi.
4. Pada proses analisa risiko belum ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sesuai dengan definisi yang ada.
5. 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 bahan dari program pengelolaan keamanan informasi).
6. Langkah-langkah mitigasi dan penanggulangan risiko yang ada belum disusun sesuai dengan kebutuhan rencana yang jelas.
7. Langkah mitigasi risiko sesuai target penyelesaiannya diprioritaskan serta penanggungjawabnya ditentukan, mekanisme untuk memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK belum diterapkan
8. Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
9. Penyelesaian Langkah mitigasi belum diterpkan dan belum dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya.
10. Profil risiko berikut bentuk mitigasinya belum secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.
11. Kerangka kerja pengelolaan risiko belum secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya.
12. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan.

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

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

1. Kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
2. Sudah adanya proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
3. Kontrak dengan pihak ketiga sudah mencakup aspek-aspek kontrol keamanan informasi seperti proses pelaporan insiden, keharusan menjaga kerahasiaan, penggunaan perangkat lunak yang berlisensi (HAKI), dan tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
4. Diskominfosantik Provinsi Kalimantan Tengah sudah menetapkan dan menerapkan kebijakan dan prosedur operasional terkait implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, hingga pelaporannya.
5. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mencakup persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya sudah disusun dan didokumentasikan.
6. Strategi penerapan keamanan informasi sudah dirumuskan dan ditetapkan sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
7. Strategi penerapan keamanan informasi sudah direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi.
8. Rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) sudah direalisasikan secara konsisten.

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

1. Belum adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan didokumentasikan dengan jelas, termasuk peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
2. Mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya belum diatur dan didokumentasikan secara formal.
3. Kebijakan dan prosedur keamanan informasi yang sudah ditetapkan belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang telah ditetapkan.
4. Belum adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan.

5. Konsekwensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.
6. Belum adanya tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini.
7. Aspek keamanan informasi belum diidentifikasi untuk beberapa aktivitas proyek selama proses manajemen proyek dan sudah tertuang dalam dokumentasi.
8. Evaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul belum dilakukan.
9. Proses pengembangan sistem yang aman (Secure SDLC) belum menerapkan prinsip atau metode sesuai standar platform teknologi yang digunakan.
10. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfosantik Provinsi Kalimantan Tengah belum terdapat proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya.
11. Perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum mencakup mengenai komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk.
12. Uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dilakukan sesuai jadwal.
13. Hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dievaluasi. Langkah perbaikan atau pemberian yang diperlukan (misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal)) belum ditetapkan secara jelas dalam suatu dokumentasi yang resmi.
14. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala.
15. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko belum ditetapkan secara resmi.
16. Diskominfosantik Provinsi Kalimantan Tengah belum menetapkan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku).
17. Audit internal belum mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.

18. Hasil audit internal belum secara rutin dikaji/dievaluasi terkait langkah pemberahan dan pencegahan yang diperlukan, ataupun inisiatif peningkatan kinerja keamanan informasi.
19. Hasil audit internal belum dilaporkan kepada pimpinan organisasi dan sudah ditetapkan langkah-langkah perbaikan atau program peningkatan kinerja keamanan informasi.
20. Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, belum terdapat proses dalam melakukan analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
21. Diskominfosantik Provinsi Kalimantan tengah 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 pemberahan yang diperlukan, telah diterapkan secara efektif.

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

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

1. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi sudah didokumentasikan secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
2. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku sudah didefinisikan.
3. Proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Diskominfosantik Provinsi Kalimantan Tengah dan keperluan pengamanannya sudah didefinisikan dan ditetapkan secara resmi.
4. Definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut sudah didokumentasikan.
5. Sudah adanya proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi).
6. Sudah tersedianya proses pengelolaan konfigurasi yang diterapkan secara konsisten.
7. Sudah ditetapkannya proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
8. Sudah adanya definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Diskominfotik Provinsi DKI Jakarta.
9. Sudah ditetapkannya persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
10. Telah ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
11. Sudah ada prosedur untuk proses *back-up* dan uji coba pengembalian data (*restore*) secara berkala.

12. Sudah adanya ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
13. Telah ada prosedur penghancuran data/aset yang sudah tidak diperlukan.
14. Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya sudah didokumentasikan.
15. Sudah terdokumentasinya daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
16. Pengamanan fasilitas fisik (lokasi kerja) sudah diterapkan sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
17. Infrastruktur komputasi telah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.
18. Infrastruktur komputasi yang terpasang sebagian telah terlindungi dari gangguan pasokan listrik atau dampak dari petir.
19. Sudah ditetapkannya proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
20. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sebagian 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.
21. Sudah adanya proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
22. Sudah didefinisikan dan ditetapkannya peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll).
23. Sudah adanya proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Diskominfotik Provinsi DKI Jakarta.

## B. Kelemahan/Kekurangan

1. Belum adanya tata tertib penggunaan komputer, email, internet dan intranet.
2. Belum ditetapkannya tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI.
3. Belum ada aturan terkait instalasi piranti lunak di aset TI milik Diskominfotik Provinsi DKI Jakarta.
4. Belum diatur mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
5. Sudah ada proses mengenai pengelolaan identitas elektronik dan proses otentikasi (*username & password*) namun belum termasuk kebijakan terhadap pelanggarannya.

6. Belum ada ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
7. Belum tersedianya proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
8. Belum berjalannya proses pengecekan latar belakang SDM.
9. Belum dilakukan mekanisme terkait pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib sudah tertuang dalam dokumentasi.
10. Belum tersedianya prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pemberahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.
11. Belum ada ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
12. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan belum ditetapkan dan didokumentasikan.
13. Belum ada proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik sudah jelas mekanismenya.
14. Belum ditetapkannya peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor).
15. Belum ada mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.

## **VI. ASPEK TEKNOLOGI:**

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

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
2. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll).
3. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi sudah didokumentasikan dan dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
4. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
5. Setiap perubahan dalam sistem informasi sudah direkam pada suatu log pada sistem.
6. Upaya akses oleh yang tidak berhak sudah terekam di dalam log.
7. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, melakukan lockout setelah kegagalan login, dan penarikan akses.
8. Pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi sudah diterapkan.

9. Aplikasi yang ada telah memiliki dokumentasi mengenai spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba.

## B. Kelemahan/Kekurangan

1. Analisa kepatuhan penerapan konfigurasi standar yang ada belum dianalisa secara berkala.
2. Jaringan, sistem dan aplikasi yang digunakan belum secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
3. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sebagian dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
4. Semua log belum dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
5. Diskominfosantik Provinsi Kalimantan Tengah sebagian menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
6. Diskominfosantik Provinsi Kalimantan Tengah belum mempunyai standar dalam menggunakan enkripsi.
7. Pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya belum diterapkan.
8. Sebagian sistem dan aplikasi belum secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menonaktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
9. Akses yang digunakan untuk mengelola sistem (administrasi sistem) belum menggunakan bentuk pengamanan khusus yang berlapis.
10. Belum ada proses untuk menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan.
11. Sistem operasi untuk setiap perangkat desktop dan server belum dimutakhirkan dengan versi terkini.
12. Setiap desktop dan server belum dilindungi dari penyerangan virus (malware).
13. Belum tersimpannya rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
14. Belum adanya proses pelaporan penyerangan virus/malware yang gagal/sukses yang ditindaklanjuti dan diselesaikan.
15. Belum keseluruhan jaringan, sistem dan aplikasi sudah tersinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
16. Lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun belum diterapkan.
17. Diskominfosantik Provinsi Kalimantan Tengah telah melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi namun belum secara rutin.

## VII. REKOMENDASI

1. Pejabat/petugas pelaksana pengamanan informasi sudah ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang akan dilaksanakan, namun belum menjamin kepatuhan program keamanan informasi.
2. Alokasi sumber daya terkait pelaksanaan program keamanan informasi sudah direncanakan dan disediakan dalam rangka memastikan pengelolaan keamanan informasi namun belum memadai dan belum dipastikan kepatuhannya
3. Peran fungsi pelaksana pengamanan informasi belum dipetakan terkait pengelolaan program keamanan informasi dan belum dilaksanakan secara menyeluruh melibatkan bidang-bidang lain dalam lingkup Diskominfosantik Provinsi Kalimantan Tengah, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
4. Diskominfosantik Provinsi Kalimantan Tengah belum mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
5. Belum Semua pelaksana pengamanan informasi yang terlibat di Diskominfosantik Provinsi Kalimantan tengah sudah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
6. Beberapa persyaratan keamanan informasi yang terdapat dalam standard yang berlaku sudah terintegrasi kedalam proses kerja yang ada namun sebagian lainnya masih bersifat aktivitas kontrol tambahan yang dilakukan.
7. Diskominfosantik Provinsi Kalimantan Tengah belum mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundungan yang berlaku.
8. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi belum mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, dan untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada.
9. Fungsi pengelola keamanan informasi sudah melaporkan kepada manajemen mengenai sebagian dari kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi secara rutin, namun laporan belum menyeluruh terkait pelaksanaan keamanan informasi.
10. Belum semua permasalahan keamanan informasi yang terjadi di Diskominfosantik Provinsi Kalimantan Tengah menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektifitas pelaksanaan kontrol keamanan informasi.
11. Metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi belum didefinisikan yang mencakup mekanisme, waktu pengukuran, pelaksananya, dan harus diukur dan dievaluasi pemantauannya secara berkala serta dilakukan eskalasi pelaporan kepada manajemen untuk memastikan

- efektifitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan.
12. Diskominfosantik Provinsi Kalimantan Tengah belum mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisa tingkat kepatuhannya.
  13. Diskominfosantik Provinsi Kalimantan Tengah belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).
  14. Diskominfosantik Provinsi Kalimantan Tengah belum menentukan penanggung jawab proses manajemen risiko yang berwenang dalam eskalasi terhadap pelaporan hasil analisa risiko keamanan informasi sampai ke tingkat pimpinan organisasi.
  15. Dalam proses pengelolaan manajemen risiko, Diskominfosantik Provinsi Kalimantan Tengah belum terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
  16. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi.
  17. Pada proses analisa risiko belum ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sesuai dengan definisi yang ada.
  18. 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 bahian dari program pengelolaan keamanan informasi).
  19. Langkah-langkah mitigasi dan penanggulangan risiko yang ada belum disusun sesuai dengan kebutuhan rencana yang jelas.
  20. Langkah mitigasi risiko sesuai target penyelesaiannya diprioritaskan serta penanggungjawabnya ditentukan, mekanisme untuk memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK belum diterapkan.
  21. Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
  22. Penyelesaian Langkah mitigasi belum diterapkan dan belum dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya.
  23. Profil risiko berikut bentuk mitigasinya belum secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.
  24. Kerangka kerja pengelolaan risiko belum secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya.
  25. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan.
  26. Belum adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan kebijakan dan prosedur maupun dokumen lainnya yang diperlukan

- terkait keamanan informasi sudah disusun dan didokumentasikan dengan jelas, termasuk peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
27. Mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya belum diatur dan didokumentasikan secara formal.
  28. Kebijakan dan prosedur keamanan informasi yang sudah ditetapkan belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang telah ditetapkan.
  29. Belum adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan.
  30. Konsekwensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.
  31. Belum adanya tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini.
  32. Aspek keamanan informasi belum diidentifikasi untuk beberapa aktivitas proyek selama proses manajemen proyek dan sudah tertuang dalam dokumentasi.
  33. Evaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul belum dilakukan.
  34. Proses pengembangan sistem yang aman (Secure SDLC) belum menerapkan prinsip atau metode sesuai standar platform teknologi yang digunakan.
  35. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfosantik Provinsi Kalimantan Tengah belum terdapat proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya.
  36. Perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum mencakup mengenai komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk.
  37. Uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dilakukan sesuai jadwal.
  38. Hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dievaluasi. Langkah perbaikan atau pemberian yang diperlukan (misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal)) belum ditetapkan secara jelas dalam suatu dokumentasi yang resmi.
  39. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala.
  40. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko belum ditetapkan secara resmi.

41. Diskominfosantik Provinsi Kalimantan Tengah belum menetapkan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku).
42. Audit internal belum mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.
43. Hasil audit internal belum secara rutin dikaji/dievaluasi terkait langkah pemberahan dan pencegahan yang diperlukan, ataupun inisiatif peningkatan kinerja keamanan informasi.
44. Hasil audit internal belum dilaporkan kepada pimpinan organisasi dan sudah ditetapkan langkah-langkah perbaikan atau program peningkatan kinerja keamanan informasi.
45. Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, belum terdapat proses dalam melakukan analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
46. Diskominfosantik Provinsi Kalimantan tengah 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 pemberahan yang diperlukan, telah diterapkan secara efektif.
47. Belum adanya tata tertib penggunaan komputer, email, internet dan intranet.
48. Belum ditetapkannya tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI.
49. Belum ada aturan terkait instalasi piranti lunak di aset TI milik Diskominfotik Provinsi DKI Jakarta.
50. Belum diatur mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
51. Sudah ada proses mengenai pengelolaan identitas elektronik dan proses otentifikasi (*username & password*) namun belum termasuk kebijakan terhadap pelanggarannya.
52. Belum ada ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
53. Belum tersedianya proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
54. Belum berjalannya proses pengecekan latar belakang SDM.
55. Belum dilakukan mekanisme terkait pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib sudah tertuang dalam dokumentasi.
56. Belum tersedianya prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pemberahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.
57. Belum ada ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.

58. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan belum ditetapkan dan didokumentasikan.
59. Belum ada proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik sudah jelas mekanismenya.
60. Belum ditetapkannya peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor).
61. Belum ada mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
62. Analisa kepatuhan penerapan konfigurasi standar yang ada belum dianalisa secara berkala.
63. Jaringan, sistem dan aplikasi yang digunakan belum secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
64. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sebagian dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
65. Semua log belum dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
66. Diskominfosantik Provinsi Kalimantan Tengah sebagian menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
67. Diskominfosantik Provinsi Kalimantan Tengah belum mempunyai standar dalam menggunakan enkripsi.
68. Pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya belum diterapkan.
69. Sebagian sistem dan aplikasi belum secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menonaktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
70. Akses yang digunakan untuk mengelola sistem (administrasi sistem) belum menggunakan bentuk pengamanan khusus yang berlapis.
71. Belum ada proses untuk menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan.
72. Sistem operasi untuk setiap perangkat desktop dan server belum dimutakhirkan dengan versi terkini.
73. Setiap desktop dan server belum dilindungi dari penyerangan virus (malware).
74. Belum tersimpannya rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
75. Belum adanya proses pelaporan penyerangan virus/malware yang gagal/sukses yang ditindaklanjuti dan diselesaikan.
76. Belum keseluruhan jaringan, sistem dan aplikasi sudah tersinkronisasi waktu yang akurat, sesuai dengan standar yang ada.

77. Lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun belum diterapkan.
78. Diskominfosantik Provinsi Kalimantan Tengah telah melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi namun belum secara rutin.

## VIII. PENUTUP

Demikian Laporan *Onsite Assessment* Indeks KAMI Diskominfosantik Provinsi Kalimantan Tengah T.A. 2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Diskominfotik Provinsi Kalimantan Tengah.

Laporan *Onsite Assessment* Indeks KAMI Diskominfosantik Provinsi Kalimantan Tengah T.A. 2022 ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Kalimantan Tengah; dan
3. Sekretaris Daerah Provinsi Kalimantan Tengah.

**Jakarta, 4 Agustus 2022**

Kepala Bidang Persandian

Sandiman Madya pada  
Direktorat Keamanan Siber dan Sandi  
Pemerintah Daerah selaku Lead Asesor:

Billy Bareto, S.T.

19761123 200604 1 006

Nurchaerani, S.E

19650708 198710 2 003

Mengetahui,  
Kepala Diskominfo Persandian dan Statistik  
Provinsi Kalimantan Tengah

Agus Siswadi, S.Pd., M.Pd

19680204 199903 1 007