LAPORAN
ONSITE ASSESSMENT
INDEKS KAMI

Instansi/Perusahaan: Pemerintah Provinsi Sumatera Barat	**Narasumber Instansi/Perusahaan:** 1. Zulkifli, SE. 2. Roby Charma, S.Kom. 3. Rizki Nurdin 4. Afdhal Rahman, S.T. 5. Rio Bayu Sentosa 6. Andry Kurniawan, S.Kom.
Unit Kerja: Dinas Komunikasi, Informatika, dan Statistik (Diskominfotik)	
Alamat: Jln. Pramuka Raya No. 11 A Belanti, Padang	**Tel:** (0751) 8971361
Email: diskominfo@sumbarprov.go.id	**Pimpinan Unit Kerja:** Drs. Jasman, M.M. Kepala Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat

A. Ruang Lingkup:

1. Instansi / Unit Kerja:
   Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat
2. Fungsi Kerja:
   Berdasarkan Peraturan Gubernur Nomor 65 Tahun 2020 tentang Uraian Tugas Pokok dan Fungsi Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat mempunyai fungsi:
   a. penyelenggaraan perumusan kebijakan teknis di bidang Komunikasi dan Informatika, bidang Statistik dan bidang Persandian yang menjadi kewenangan daerah;
   b. penyelenggaraan pelaksanaan kebijakan teknis di bidang Komunikasi dan Informatika, bidang Statistik dan bidang Persandian yang menjadi kewenangan daerah;
   c. penyelenggaraan administrasi Dinas Komunikasi, Informatika dan Statistik;
   d. penyelenggaraan evaluasi dan pelaporan di bidang Komunikasi, dan Informatika, bidang Statistik dan bidang Persandian;
   e. penyelenggaraan tugas lain yang diberikan oleh pimpinan sesuai dengan tugas dan fungsinya.
3. Lokasi:

No	Nama Lokasi	Alamat
1	Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat	Jln. Pramuka Raya No. 11 A Belanti, Padang
2	Data Center	Jln. Pramuka Raya No. 11 A Belanti, Padang

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 Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat.

C. Aset TI yang kritikal:

1. Informasi:
   - Data Kepegawaian

2. Aplikasi Utama:
   Diskominfotik memiliki 104 aplikasi yang dikelola, tetapi tidak semua aktif. Berikut ini beberapa aplikasi utama yang dikelola:
   - Sistem Informasi Kepegawaian (SIMPEG)
   - Absensi Online (ABON)
   - Sistem Penerimaan Siswa Baru (PPDB Online)
   - Surat Elektronik (Surek)
   - Sumbar Madani

3. Server Utama:
   - Sumbarprov

D. DATA CENTER (DC):

☒ ADA

☐ TIDAK ADA

E. DISASTER RECOVERY CENTER (DRC):

☐ ADA → ☐ Dikelola Internal ☐ Dikelola Vendor

☒ TIDAK ADA

Status Ketersediaan Dokumen Kerangka Kerja
Sistem Manajemen Keamanan Informasi (SMKI)

Tabel 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: • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan kontrol • Struktur dan metodologi manajemen risiko • Organisasi dan tanggungjawab keamanan informasi	Tidak Ada (draf)

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	Ada
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 intenal 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 (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.	Ada
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.	Tidak Ada
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)	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/k 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.	Tidak Ada
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).	Ada

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	Tidak Ada
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi	Tidak Ada
3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor	Tidak Ada

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	Tidak Ada
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/daya “rahasia” baik softcopy maupun hardcopy, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada Instansi	Tidak Ada
6	Pengelolaan Removable Media & Disposal Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (tape/hard disk/Flashdisk/CD) dan penghapusan informasi ataupun penghancuran media	Tidak Ada
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Berisi proses monitoring penggunaan CPU, storage, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil monitoring	Tidak Ada
8	User Access Management	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)	Tidak Ada
9	Teleworking	Pengendalian dan pengamanan penggunaan hak akses secara remote (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.	Tidak Ada
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	Tidak Ada
11	Pengelolaan Perubahan (Change Management) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/database/versi dari aset TIK yang mengalami perubahan.	Tidak Ada
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.	Tidak Ada

Dokumen yang diperiksa:

1. Peraturan Gubernur Nomor 10 Tahun 2018 tentang Pengelolaan Barang Milik Daerah.
2. Peraturan Gubernur Nomor 14 Tahun 2018 tentang Pelaksanaan Aplikasi Sistem Administrasi Perkantoran Berbasis Elektronik.
3. Peraturan Gubernur Nomor 15 Tahun 2018 tentang Pengembangan Sistem Aplikasi Pemerintah Provinsi Sumatera Barat.
4. Peraturan Gubernur Nomor 20 Tahun 2018 tentang Pengelolaan Sistem Pemerintahan Berbasis Elektronik.
5. Peraturan Gubernur Nomor 23 Tahun 2018 tentang Perubahan Rencana Strategis Perangkat Daerah Provinsi Sumatera Barat Tahun 2016 – 2021.
6. Peraturan Gubernur Nomor 10 Tahun 2019 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi.
7. Peraturan Gubernur Nomor 7 Tahun 2020 tentang Jadwal Retensi Arsip Substantif Pemerintahan Daerah Provinsi Sumatera Barat.

8. Peraturan Gubernur Nomor 15 Tahun 2020 tentang Tata Cara Pengelolaan Informasi Dan Dokumentasi di Lingkungan Pemerintah Daerah Provinsi Sumatera Barat.
9. Peraturan Gubernur Nomor 59 Tahun 2020 tentang Rencana Induk Sistem Pemerintahan Berbasis Elektronik.
10. Peraturan Gubernur Nomor 65 Tahun 2020 tentang Uraian Tugas Pokok dan Fungsi Dinas Komunikasi, Informatika Dan Statistik Provinsi Sumatera Barat.
11. Peraturan Gubernur Nomor 21 Tahun 2021 tentang Sistem Klasifikasi Keamanan Dan Akses Arsip Dinamis di Lingkungan Pemerintah Provinsi Sumatera Barat.
12. Daftar Informasi Publik Pemerintah Provinsi Sumatera Barat Tahun 2020.
13. Keputusan Gubernur Nomor 480-595-2017 tentang Perubahan Atas Keputusan Gubernur Nomor 480-1216-2016 tentang Daftar Informasi Publik Yang Dikecualikan di Lingkungan Pemerintah Provinsi Sumatera Barat.
14. Keputusan Gubernur Nomor 555-997-2019 tentang Pembentukan Tim Koordinasi Tanggap Insiden Keamanan Komputer Provinsi Sumatera Barat (Computer Security Incident Response Team).
15. Petunjuk Teknis Pengelolaan Insiden Keamanan Informasi SumbarProv-CSIRT Nomor 555/38/B-2/Diskominfo/VIII/2019.
16. Perjanjian Kerja Sama tentang Pemanfaatan Sertifikat Elektronik dalam Sistem Pemerintahan Berbasis Elektronik (E-government) di Lingkungan Pemerintah Provinsi Sumatera Barat.
17. Rancangan Peraturan Gubernur tentang Penerapan Sertifikat Elektronik di Lingkungan Pemerintah Provinsi Sumatera Barat.
18. Roadmap Penyelenggaraan Urusan Persandian di Lingkungan Pemerintah Provinsi Sumatera Barat Tahun 2017 dari Tim Optimalisasi Lemsaneg.
19. KAK Keg Penyediaan Layanan Keamanan Informasi Pemerintah Daerah Provinsi.
20. KAK Keg Pelaksanaan Keamanan Informasi Pemerintah Daerah Provinsi Berbasis Elektronik dan Non Elektronik.
21. KAK Keg Pelaksanaan Anlisis Kebutuhan dan Pengelolaan Sumber Daya Keamanan Informasi Pemerintah Daerah Provinsi.
22. SOP Back Up Data Eksternal dan Internal.
23. SOP Pengacak Sinyal (Jammer).
24. SOP Penerimaan dan Penerimaan Surat Dinas Biasa melalui Faximile.
25. SOP Penerimaan dan Penerimaan Surat Dinas Biasa Melalui Email Sanapati.
26. SOP Penerimaan dan Penerimaan Surat Dinas yang dikecualikan.
27. Petunjuk Operasional Pengguna untuk Pendaftaran SE.
28. SOP Pembaruan Sertifikat Elektronik dengan Penggantian Pasangan Kunci.
29. SOP Pembuatan Email Instansi.
30. SOP Pencabutan Sertifikat Individu.
31. SOP Pendaftaran dan Pembuatan Akun AMS.
32. SOP Penerbitan Sertifikat Individu.
33. Dokumen Perjanjian Penggunaan Layanan PT. Indonesia Comnets Plus dengan Diskominfo Provinsi Sumbar.
34. Draf SOP Pengelolaan Website OPD.
35. Draf SOP Pelayanan Internet Satu Pintu.
36. Draf SOP Surat Elektronik.
37. Draf SOP Fasilitasi Video Conference.
38. Draf SOP Silahar (sistem laporan harian) Sumatera Barat.
39. Draf SOP E-SPJ Sumatera Barat.
40. Draf SOP Pengelolaan Website OPD.
41. Draf SOP Pelayanan Aplikasi Satu Pintu.
42. Draf SOP Surat Elektronik (Surek).

Dokumen tambahan yang diminta untuk diperiksa:

1. DPA/RKA/Surat terkait adanya refocusing
2. Draft Rancangan SMKI
3. Dokumen Persyaratan Perekrutan Tim IT
4. Anjab/ABK
5. Sertifikat mengikuti pelatihan CEH, ECIH
6. Dokumentasi kegiatan Sosialisasi/Bimtek/Workshop/Bimtek/ Cyber Drill Exercise
7. SPK Tenaga Kontrak
8. Laporan Audit Persandian
9. Laporan ke Kadis yang dilaksanakan setiap minggu
10. Laporan Mitigasi Risiko (Laporan Penanganan Insiden)
11. Laporan ITSA
12. SOP Pengembangan Aplikasi di Bidang Aptika Seksi Tata Kelola
13. Perda SPBE Nomor 20 Tahun 2018

Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber Diskominfo Provinsi Sumatera Barat disimpulkan sbb:

I. KONDISI UMUM:

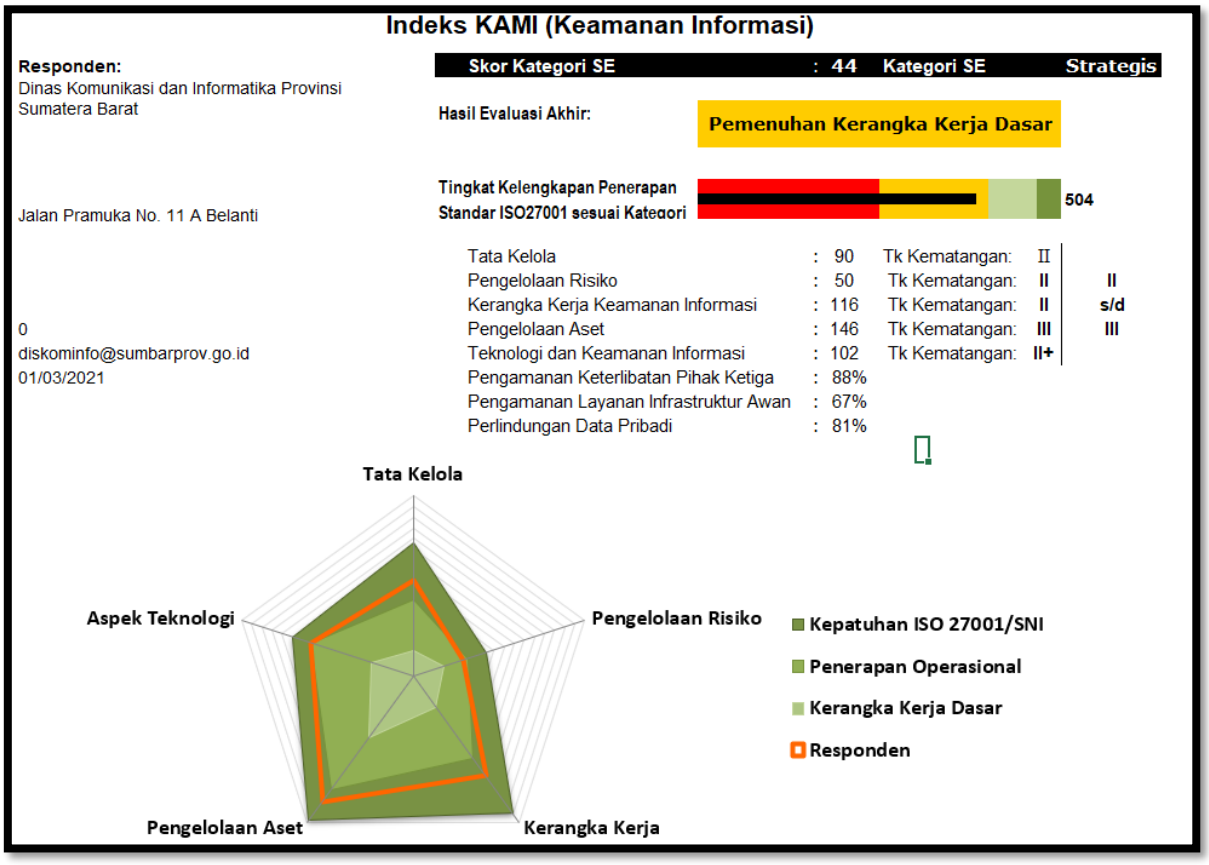
1. Struktur organisasi satuan kerja dalam ruang lingkup berada di bawah Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat yang terdiri atas:
   a. Bidang Informasi dan Komunikasi Publik;
   b. Bidang Aplikasi Informatika;
   c. Bidang Statistik Sektoral; dan
   d. Bidang Siber dan Sandi.

2. SDM pengelola terdiri dari:
   Jumlah pegawai di Diskominfotik Provinsi Sumatera Barat adalah 55 personil PNS dan 28 personil Tenaga IT.

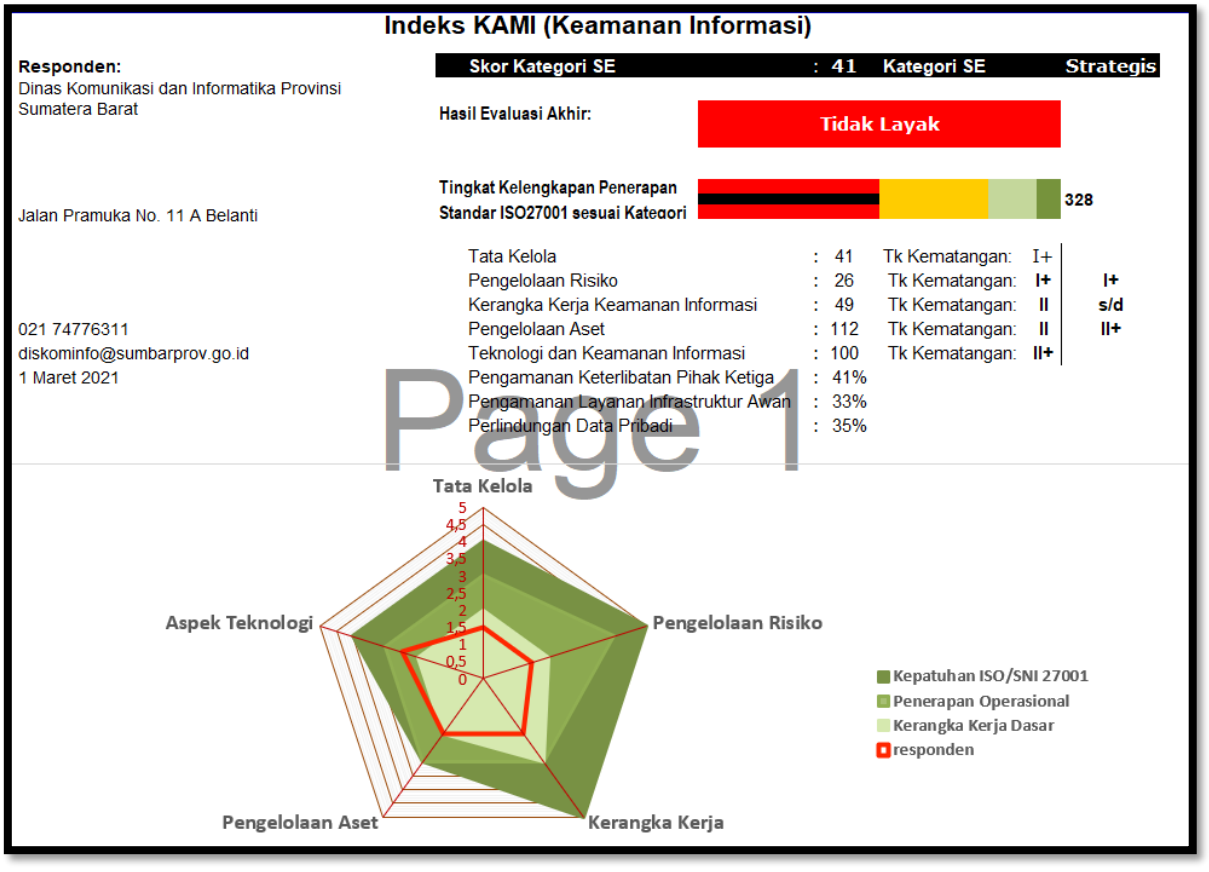
3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

   Dinas Komunikasi, Informatika, dan Statistik Provinsi Sumatera Barat mengelola Sistem Elektronik dalam kategori Strategis dengan hasil evaluasi akhir pada level Tidak Layak dengan tingkat kelengkapan penerapan standar ISO 27001 sesuai kategori pada skor nilai 328.

Total Score Sebelum Verifikasi: 504 (ref. file Indeks KAMI pra Verifikasi)



Total Score Setelah Verifikasi: 328 (ref. file Indeks KAMI pasca Verifikasi)



II. ASPEK TATA KELOLA:

a. Kekuatan/Kematangan
   1. Pimpinan dari Diskominfotik Provinsi Sumatera Barat sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah ada penetapan kebijakan keamanan informasi melalui Renstra dan Peraturan Gubernur.
   2. Sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi kepada semua pihak yang terkait.

b. Kelemahan/Kekurangan
   1. Peran pelaksana pengamanan informasi yang mencakup semua keperluan belum dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan.
   2. Diskominfotik belum melakukan integrasi keperluan/persyaratan keamanan informasi dalam proses kerja yang ada.
   3. Belum adanya tanggungjawab pengelolaan keamanan informasi terkait koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan.
   4. Belum adanya tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans).
   5. Kondisi dan permasalahan keamanan informasi belum menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di Diskominfotik Provinsi Sumatera Barat, dan tidak tertuang atau terdefinisi di dalam dokumen.
   6. Pendokumentasian kebijakan/pedoman/prosedur terkait SMKI masih sangat kurang walaupun telah terdapat beberapa implementasi dalam pelaksanaan kegiatan di Diskominfotik.

III. ASPEK RISIKO:

a. Kekuatan/Kematangan
   1. Diskominfotik Provinsi Sumatera Barat telah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut di dalam dokumen berita acara dan daftar inventaris aset.

b. Kelemahan/Kekurangan
   1. Diskominfotik Provinsi Sumatera Barat belum memiliki kebijakan pengelolaan risiko khususnya di bidang TI sebagai dokumen acuan penerapan manajemen risiko SMKI.
   2. Belum mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian bagi instansi, serta penetapan ambang batas tingkat risiko.
   3. Belum mempunyai program kerja, penanggung jawab, beserta eskalasi pelaporan status pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
   4. Belum ditetapkannya dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama, analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada, serta belum adanya penyelesaian langkah mitigasi dan evaluasnya.
   5. Belum adanya dokumen risk register.

IV. ASPEK KERANGKA KERJA:

a. Kekuatan/Kematangan
   1. Kebijakan keamanan informasi telah dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
   2. Sudah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
   3. Telah memiliki dokumen untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi, yaitu berupa petunjuk teknis pengelolaan insiden keamanan informasi.

b. Kelemahan/Kekurangan
   1. Diskominfotik Provinsi Sumatera Barat belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada.
   2. Keseluruhan kebijakan dan prosedur keamanan informasi yang ada belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu, karena belum adanya dokumen kebijakan manajemen risiko yang didalamnya terdapat risk register.
   3. Belum adanya konsekwensi dari pelanggaran kebijakan keamanan informasi yang didefinisikan, dikomunikasikan dan ditegakkan.
   4. Diskominfotik belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
   5. Penerapan proses pengembangan sistem yang aman (Secure SDLC) dalam tahap perencanaan untuk dilakukan.
   6. Proses untuk menanggulangi akibat timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada (termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya) masih dalam tahap perencanaan.
   7. Belum tersedianya kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.

V. ASPEK PENGELOLAAN ASET:

a. Kekuatan/Kematangan
   1. Diskominfotik Provinsi Sumatera Barat telah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara.
   2. Telah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku serta definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi.
   3. Terdapat proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
   4. Terdapat proses pengecekan latar belakang SDM.
   5. Terdapat prosedur penghancuran data/aset yang sudah tidak diperlukan.
   6. Sudah memiliki proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik, serta infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan gangguan pasokan listrik atau dampak dari petir.
   7. Telah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.

b. Kelemahan/Kekurangan
   1. Belum adanya tata tertib pengamanan dan penggunaan aset di Diskominfotik terkait HAKI.
   2. Diskominfotik Provinsi Sumatera Barat belum memiliki peraturan terkait instalasi piranti lunak di aset TI.
   3. Belum adanya prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku.
   4. Belum tersedianya prosedur penggunaan perangkat pengolah informasi milik pihak ketiga yang memastikan aspek HAKI dan pengamanan akses yang digunakan.
   5. Belum tersedianya proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan.
   6. Belum tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
   7. Belum tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya.

VI. ASPEK TEKNOLOGI:

a. Kekuatan/Kematangan
   1. Pengamanan pada layanan TIK yang menggunakan internet sudah dilakukan lebih dari satu lapis. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll).
   2. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor dan setiap perubahan dalam sistem informasi serta upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log.
   3. Telah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada dan menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya.
   4. Akses yang digunakan untuk mengelola sistem (administrasi sistem) telah menggunakan bentuk pengamanan khusus yang berlapis yaitu dengan VPN dan password.
   5. Telah menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi serta pengamanan khusus untuk melindungi akses dari luar instansi.
   6. Keseluruhan jaringan, sistem dan aplikasi yang ada di Diskominfotik Provinsi Sumatera Barat sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.

b. Kelemahan/Kekurangan
   1. Diskominfotik Provinsi Sumatera Barat belum mempunyai standar dalam menggunakan enkripsi.
   2. Belum secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada.

VIII. REKOMENDASI

1. Sebagai pedoman dalam penerapan SMKI di Diskominfotik Provinsi Sumatera Barat perlu segera untuk dibuatkan kebijakan SMKI yang memuat konsekwensi dari pelanggaran kebijakan keamanan informasi yang didefinisikan, dikomunikasikan dan ditegakkan.
2. Dalam rangka untuk memastikan berjalannya pengelolaan SMKI secara berkesinambungan, perlu dibuat tim pengelola/pelaksana pengamanan informasi yang di dalamnya mendefinisikan peran pelaksana pengamanan informasi yang mencakup semua keperluan yang dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan.

3. Perlunya melakukan integrasi keperluan/persyaratan keamanan informasi dalam proses kerja yang ada.
4. Perlu dicantumkan tanggungjawab pengelolaan keamanan informasi terkait koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan.
5. Perlu membuat dokumen BCP dan DRP yang di dalamnya terdapat tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans).
6. Perlu pencantuman program kerja, penanggung jawab, beserta eskalasi pelaporan status pengelolaan risiko keamanan informasi yang terdokumentasi di dalam suatu dokumen kebijakan SMKI.
7. Menyusun dokumen kebijakan manajemen risiko yang memuat kerangka kerja pengelolaan risiko keamanan informasi yang mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian bagi instansi, serta penetapan ambang batas tingkat risiko.
8. Menyusun dokumen risk register yang di dalamnya berisi dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama, dan analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada, serta penyelesaian langkah mitigasi dan evaluasinya.
9. Menyusun dokumen pedoman manajemen risiko yang di dalamnya terdapat risk register yang dapat merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu.
10. Perlu menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul. Proses tersebut dapat dilakukan jika memiliki dokumen risk register terlebih dahulu.
11. Menyusun prosedur untuk menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi.
12. Perlu menerapkan proses untuk menanggulangi akibat timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada (termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya). Hal ini dapat dicantumkan di dokumen pedoman manajemen risiko.
13. Menyusun kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya yang dapat tertuang di dokumen BCP.
14. Membuat program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada.
15. Menyusun tata tertib pengamanan dan penggunaan aset di Diskominfotik terkait HAKI dan peraturan terkait instalasi piranti lunak di aset TI.
16. Menyusun prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku.
17. Menyusun prosedur penggunaan perangkat pengolah informasi milik pihak ketiga yang memastikan aspek HAKI dan pengamanan akses yang digunakan.
18. Perlu menerapkan proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan.
19. Perlu menerapkan proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
20. Menyusun 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.
21. Perlu dilakukan analisa kepatuhan penerapan konfigurasi standar yang ada secara rutin dan terdokumentasi.
22. Menyusun kebijakan/peraturan yang di dalamnya mencakup standar dalam menggunakan enkripsi. Hal ini bisa dicantumkan dalam dokumen SMKI.

Padang, 15 Desember 2021 Narasumber Instansi: Diskominfotik Provinsi Sumbar	**Assessor Indeks KAMI:**
1. Zulkifli, SE.	1. Guruh P.P., S.ST.,M.Si (Han)
2. Roby Charma, S.Kom.	2. Irma Nurfitri Handayani, S.ST.
3. Rizki Nurdin	3. Ikrima Galuh Nasucha, S.Tr.TP.
4. Afdhal Rahman, S.T.	4. Carissa Mega Y., S.Tr.TP.
5. Rio Bayu Sentosa	5. Ni Putu Ayu Lhaksmi W., S.Tr.TP.
6. Andry Kurniawan, S.Kom.	