
	<h2 style="margin: 0;">LAPORAN ONSITE ASSESMENT INDEKS KAMI</h2>	 INDEKS KEAMANAN INFORMASI
Instansi/Perusahaan: Pemerintah Kota Batam	Narasumber Instansi/Perusahaan: 1. Indra Sufian, M.Eng. 2. Arreza M.P, S.Kom. 3. Irpan Syarif Hasibuan, S.Kom. 4. Irpa Darajat, ST.	
Unit Kerja: Dinas Komunikasi dan Informatika Kota Batam		
Alamat: Jalan Engku Putri No.1, Batam Centre, Kota Batam	Tel: (0778) 461349	
Email: kominfo@batam.go.id	Pimpinan Unit Kerja: Kepala Dinas Komunikasi dan Informatika Kota Batam Azril Apriansyah, ST, MT. 19730408 200212 1 005	
<p>A. <u>Ruang Lingkup:</u></p> <p>Pengelolaan Data Center (Ruang Server) dan Pengembangan Aplikasi E-Government/SPBE pada Dinas Komunikasi dan Informatika Kota Batam</p> <p>B. <u>Informasi Instansi :</u></p> <ol style="list-style-type: none"> 1. Instansi / Unit Kerja: <p style="margin-left: 40px;">Dinas Komunikasi dan Informatika Kota Batam.</p> 2. Fungsi Kerja: <ol style="list-style-type: none"> a. Penyusunan rencana dan program lingkup Pengelolaan Informasi Publik dan Persandian; b. Penyusunan petunjuk teknis operasional lingkup Pengelolaan Informasi Publik dan Persandian; c. Penyelenggaraan pelayanan publik dan administrasi urusan pemerintahan daerah lingkup Pengelolaan Informasi Publik dan Persandian; d. Pembinaan monitoring, evaluasi dan pelaporan pelaksanaan lingkup Pengelolaan Informasi Publik dan Persandian. 		

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor	Jalan Engku Putri No.1, Batam Centre, Kota Batam
2	Data Center (Ruang Server)	Jalan Engku Putri No.1, Batam Centre, Kota Batam
3	Disaster Recovery Center	Belum ada

C. Nama /Jenis Layanan Publik:

Layanan yang masuk ruang lingkup adalah Sistem Layanan Infrastruktur (Data Center/ Ruang Server, Aplikasi, Jaringan, Server) Sistem Informasi dan Sistem Komunikasi yang dikelola oleh Dinas Komunikasi dan Informatika Kota Batam.

D. Aset TI yang kritikal:

1. Informasi:

- Data Pribadi pegawai
- KTP

2. Aplikasi:

- SIMPEG
- Email Batam
- Website Portal Pemerintah Kota Batam
- LPSE

3. Server:

batam.go.id

4. Infrastruktur Jaringan/Network:

Internet (Lintasarta)

E. DATA CENTER (DC):

ADA (Ruang Server), berada pada tempat khusus.

F. DISASTER RECOVERY CENTER (DRC):

Belum memiliki konsep Disaster Recovery Center

Status Ketersediaan Dokumen (Kebijakan/Prosedur)

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

No	Nama Kebijakan	Cakupan Dokumen	Ada/Tidak
1	Kebijakan Keamanan Informasi	<p>Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain:</p> <ul style="list-style-type: none"> • 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
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 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.	Tidak
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
5	Kerangka Kerja Manajemen Kelangsungan Usaha (<i>Business</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	Tidak

	<i>Continuity Management)</i>	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.	
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).	Tidak

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

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)	Tidak
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.	Tidak
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
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.	Tidak
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

Dokumen-dokumen yang diperiksa:

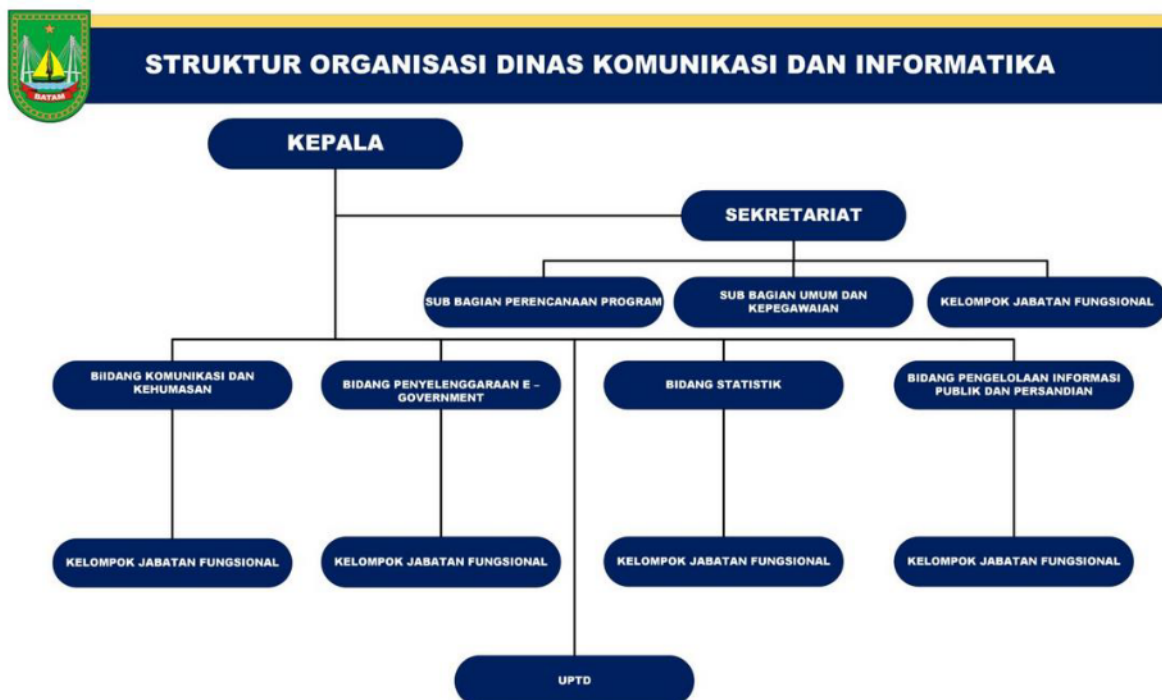
1. Peraturan Wali Kota Batam Nomor 57 Tahun 2019 tentang Perubahan Atas Peraturan Wali Kota Batam Nomor 54 Tahun 2016 tentang Tugas Pokok, Fungsi dan Uraian Tugas Dinas Komunikasi dan Informatika.
2. Peraturan Wali Kota Batam Nomor 55 Tahun 2020 tentang Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis di Lingkungan Pemerintah Kota Batam.
3. Peraturan Wali Kota Batam Nomor 40 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam.
4. Surat Keputusan Walikota Batam Nomor : 40 Tahun 2021 tanggal 7 Juni 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintahan Kota Batam.
5. Surat Keputusan Walikota Batam Nomor : KPTS.315/HK/VII/2020 tanggal 10 Juli 2020 tentang Tim Pengarah dan Tim Evaluator Internal Sistem Pemerintahan Berbasis Elektronik Pemerintah Kota Batam.
6. Surat Keputusan Kepala Diskominfo Kota Batam Nomor KPTS.67/KOMINFO/2/2021 tentang Standardisasi Pengembangan Aplikasi di Lingkungan Pemerintah Kota Batam.
7. Surat Kepala Diskominfo Nomor 495/KOMINFO/6/2021 tanggal 21 Juni 2021 perihal Pelaksanaan Kontra Penginderaan (KP) di Pemko Batam.
8. Surat Edaran Wali Kota Batam Nomor 27/KOMINFO/6/2021 tentang Penggunaan Alamat Email Resmi Pemerintah Kota Batam.
9. Surat Kepala Diskominfo Nomor 66/KI.01.04/II/2022 tanggal 14 Januari 2022 tentang Permohonan IT *Security Assessment* untuk Aplikasi berbasis *Website*.
10. SOP No.01/SOP/Kominfo-PE/6/2021 tentang Pengujian *Unit Testing*.
11. SOP No.02/SOP/Kominfo-PE/6/2021 tentang Pengujian *Usability Testing*.

12. SOP No.03/SOP/Kominfo-PE/6/2021 tentang Pengujian *System Testing*.
13. SOP No.04/SOP/Kominfo-PE/6/2021 tentang Pengujian *User Acceptance Test*.
14. Rencana Pembangunan Jangka Menengah Daerah (RPJMD) Kota Batam Tahun 2021-2026.
15. Dokumen Pengukuran Kinerja Triwulan IV Tahun 2021 Eselon III.
16. Dokumen Pengukuran Kinerja Triwulan IV Tahun 2021 Eselon IV.
17. Dokumen Pernyataan Perjanjian Kinerja
18. Laporan Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian Kota Batam T.A. 2021.
19. Dokumen Daftar Sistem Elektronik Pemko Batam Tahun 2021.
20. RKA Tahun Anggaran 2022.
21. Laporan Kinerja Instansi Pemerintah LKJIP Tahun 2021 Diskominfo Kota Batam.
22. Masterplan TIK Kota Batam 2013-2017.

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

I. KONDISI UMUM:

1. Struktur organisasi satuan kerja dalam ruang lingkup

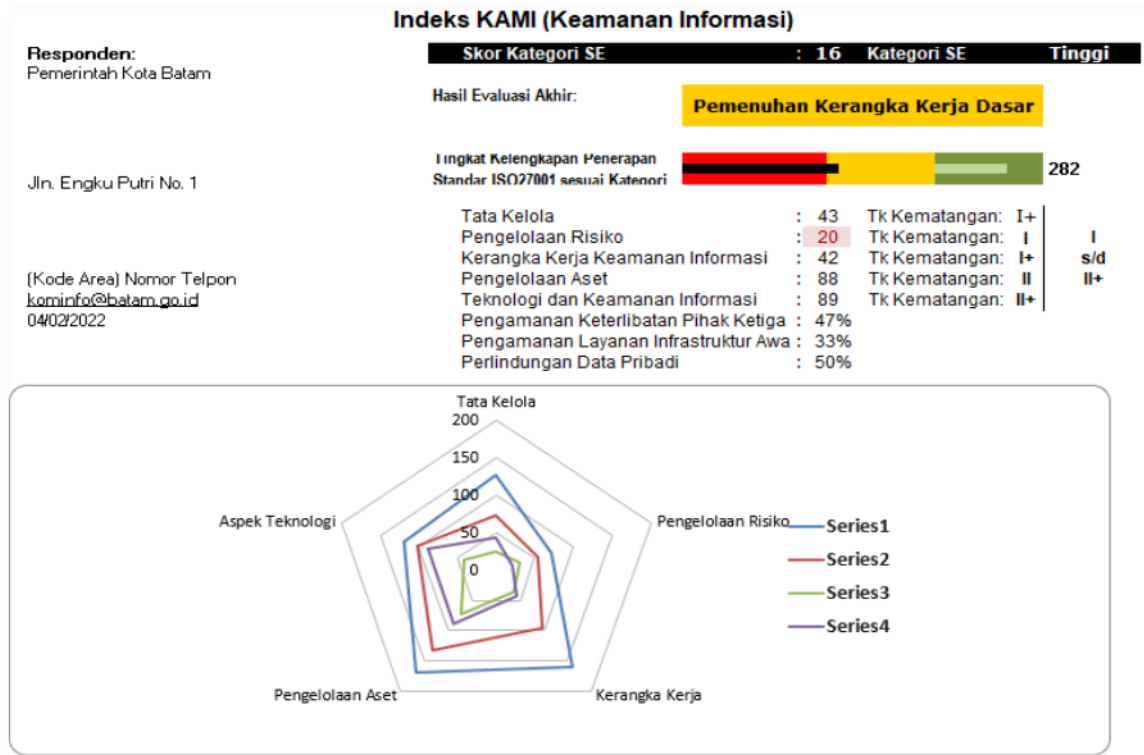


Sumber : <https://kominfo.batam.go.id/struktur-organisasi/>

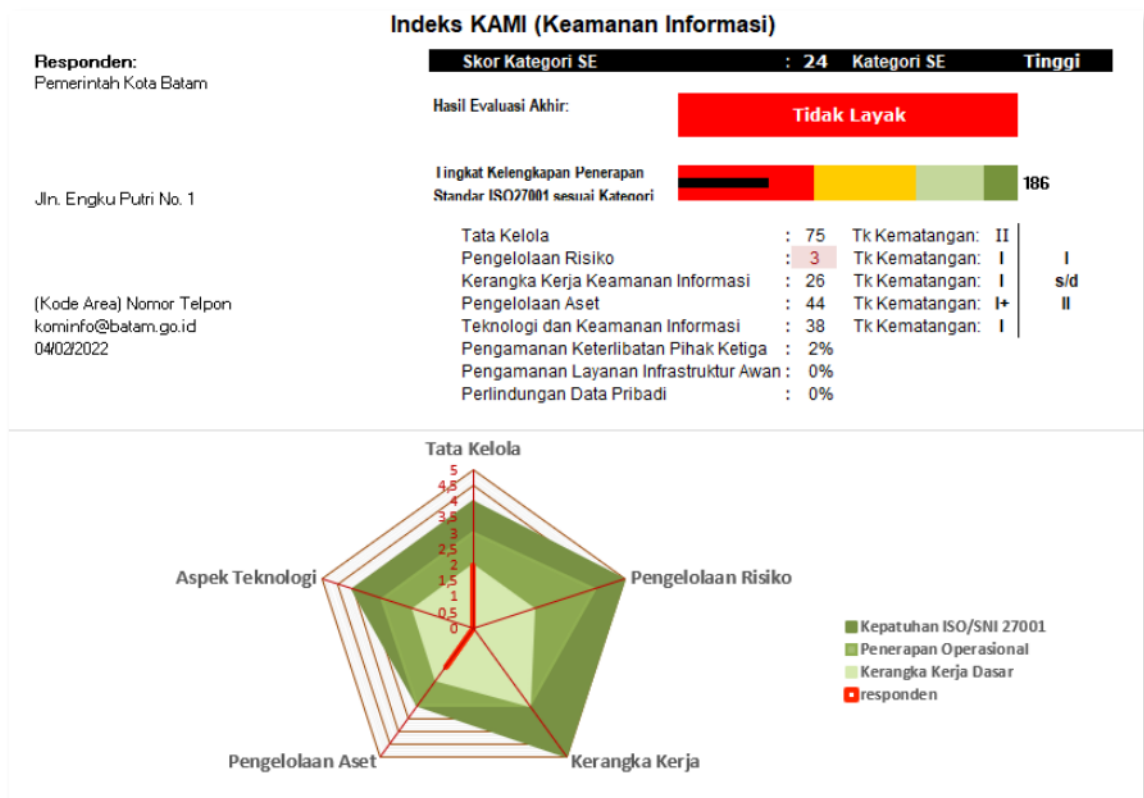
Gambar 1. Struktur Organisasi Diskominfo Kota Batam

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

Total Score Sebelum Verifikasi: 282



Total Score Setelah Verifikasi: 186



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Memiliki kebijakan pengelola keamanan informasi dalam struktur organisasi yang tertuang pada Peraturan Wali Kota Batam Nomor 57 Tahun 2019 tentang Perubahan Atas Peraturan Walikota Batam Nomor 54 Tahun 2016 Tentang Tugas Pokok, Fungsi dan Uraian Tugas Dinas Komunikasi Dan Informatika, sehingga telah terdefinisi penanggung jawab, tugas dan fungsi pengamanan informasi.
2. Telah menyusun draf kebijakan Sistem Manajemen Keamanan Informasi (SMKI) sebagai dasar kebijakan pengelolaan keamanan informasi di lingkungan Pemerintah Kota Batam, namun draf ini perlu segera ditetapkan.
3. Alokasi sumber daya baik anggaran, peralatan dan sumber daya manusia untuk pengelolaan keamanan informasi cukup didukung oleh pimpinan.
4. Telah melakukan identifikasi persyaratan/ standar kompetensi pelaksana pengelola keamanan informasi, namun masih terlalu umum.
5. Telah melakukan program sosialisasi keamanan informasi melalui media sosial.
6. Telah menetapkan penggunaan sertifikat elektronik untuk keamanan informasi yang dimuat dalam Peraturan Wali Kota Batam Nomor 41 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam.
7. Belum mengidentifikasi data pribadi yang dikelola dalam proses kerja dan proses pengamanannya.
8. Telah berkoordinasi dengan pihak eksternal dalam pengelolaan keamanan informasi, namun belum secara proaktif.

B. Kelemahan/Kekurangan

1. Belum disahkannya dokumen SMKI sebagai pedoman pengelolaan keamanan informasi di lingkungan Pemerintah Kota Batam.
2. Belum tersusunnya dokumen masterplan TIK Kota Batam sebagai acuan dan panduan pelaksanaan pengembangan TIK di Kota Batam, termasuk di dalamnya terkait dengan pengelolaan keamanan informasi.
3. Belum mengidentifikasi standar keahlian bagi pelaksana pengelola keamanan informasi, hal ini penting untuk mengetahui kekuatan personil pengelola keamanan informasi, sehingga dapat dipantau dan dilakukan evaluasi secara berkala.
4. Belum memiliki dokumen Dokumen *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP).
5. Belum menyusun pelaporan secara berkala kepada pimpinan terkait pengelolaan keamanan informasi dan kepatuhannya.
6. Belum melakukan standardisasi (matriks, parameter dan proses) pengukuran kinerja pengelolaan keamanan informasi bagi pengelola keamanan informasi.
7. Belum menyusun kebijakan terkait insiden keamanan informasi yang mengarah ke ranah hukum (pidana/ perdana).

III. ASPEK RISIKO:

A. Kekuatan/Kematangan

1. Telah memiliki program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan yaitu program IT *Security Assessment* yang sudah dilakukan secara rutin.
2. Terkait definisi umum manajemen risiko sudah tertuang dalam draf kebijakan Sistem Manajemen Keamanan Informasi (SMKI).

B. Kelemahan/Kekurangan

1. Belum memiliki kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
2. Belum mendefinisikan dan mengidentifikasi ancaman, kelemahan dan dampak kerugian sekaligus langkah mitigasi untuk seluruh aset yang dimiliki.
3. Belum menetapkan ambang batas tingkat risiko yang dapat diterima.

IV. ASPEK KERANGKA KERJA:

A. Kekuatan/Kematangan

1. Telah memiliki standar pengembangan aplikasi yang diperbaharui secara tahunan sebagai pedoman pengembangan dan pembangunan aplikasi di lingkungan Diskominfo Kota Batam, namun belum menerapkan *secure SDLC*.
2. Telah memiliki SOP dalam pengembangan dan pembangunan sistem aplikasi, termasuk di dalamnya uji keamanannya.
3. Telah melakukan kajian risiko terhadap rencana implementasi sistem aplikasi baru.
4. Memiliki strategi penerapan keamanan informasi disandingkan dengan analisa risiko penerapannya yang tertuang dalam dokumen Renstra Diskominfo Kota Batam, selain itu telah diimplementasikan ke dalam program kerja.

B. Kelemahan/Kekurangan

1. Belum memiliki dokumen SMKI yang secara jelas mencantumkan peran dan tanggung jawab pengelola keamanan informasi.
2. Belum melakukan sosialisasi dokumen SMKI kepada seluruh pihak terkait.
3. Belum memiliki proses pengelolaan dokumen kebijakan dan prosedur keamanan informasi.
4. Belum memiliki proses dalam Insiden Keamanan Informasi, mulai dari identifikasi, penetapan status insiden, *recovery* hingga *lesson learnt*.
5. Belum mencantumkan terkait pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset/ layanan TIK dalam dokumen kontrak.
6. Belum tersedia prosedur untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindaklanjuti konsekuensinya.
7. Belum memiliki kebijakan pengelolaan *security patch*.
8. Belum mengimplementasikan *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP).

9. Dokumen masterplan TIK belum diperbaharui dan dievaluasi, dokumen masterplan TIK terakhir tahun 2013-2017.
10. Belum melakukan program audit internal yang dilakukan oleh pihak independen, kemudian melakukan evaluasi dan pelaporan kepada pimpinan.
11. Belum secara periodik melakukan evaluasi tingkat kepatuhan program keamanan informasi untuk memastikan kebijakan yang dimiliki telah mengakomodir pengelolaan keamanan informasi organisasi.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

1. Telah membuat tata tertib penggunaan email yang didistribusikan kepada karyawan dalam bentuk Surat Edaran
2. Sudah menerapkan pengamanan berlapis pada ruang penyimpanan server dan akses masuk ke ruangan Diskominfo
3. Konstruksi ruang penyimpanan perangkat pengolah informasi penting (ruang penyimpanan server) telah dilengkapi fasilitas pendukung (deteksi asap dan pemadam api).

B. Kelemahan/Kekurangan

1. Belum adanya daftar inventaris aset informasi secara keseluruhan/lengkap sesuai *scope* secara akurat dan terpelihara dengan informasi tambahan pemilik aset yang akan bertanggung jawab dalam pemeliharannya, daftar inventaris aset yang ada hanya inventaris aset berupa aplikasi.
2. Belum ada pendefinisian klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku, klasifikasi aset yang didefinisikan dalam draf kebijakan SMKI yang telah dibuat hanya sebatas pembagian klasifikasi aset menjadi 4 kategori namun mekanisme dan detail penjabaran 4 kategori klasifikasi aset tersebut belum tertuang dalam dokumen.
3. Belum terdapat proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya.
4. Belum ada proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten
5. Belum ada proses yang mengatur mengenai perilsan suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
6. Diskominfo Provinsi Kepri belum mendefinisikan tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi.
7. Belum ada tata tertib mengenai penggunaan komputer, email, internet dan intranet serta pengamanan dan penggunaan aset instansi terkait HAKI.
8. Belum ada peraturan terkait instalasi piranti lunak di aset TI milik instansi.
9. Belum ada peraturan mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data.
10. Pengelolaan identitas elektronik dan proses otentikasi termasuk kebijakan terhadap pelanggarannya belum ada.
11. Belum ada ketentuan terkait waktu penyimpanan untuk klasifikasi data yang ada, syarat penghancuran data dan ketentuan terkait pertukaran data dengan pihak eksternal beserta pengamanannya.

12. Belum ada prosedur backup dan uji coba pengembalian data (*restore*)
13. Belum terdapat proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak berwajib.
14. Prosedur penghancuran data/aset yang sudah tidak diperlukan belum ada.
15. Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya berikut langkah pembenahan apabila terjadi ketidaksesuaian terhadap kebijakan yang berlaku belum ada.
16. Prosedur yang mengatur terkait user yang mutasi/keluar atau tenaga kontrak/*outsourcing* yang habis masa kerjanya belum ditetapkan dan belum didokumentasikan.
17. Daftar data/informasi yang harus di backup dan laporan analisa kepatuhan terhadap prosedur *backup*-nya belum ditetapkan dan didokumentasikan
18. 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.
19. Peraturan pengamanan perangkat komputasi milik instansi yang digunakan di luar lokasi kerja resmi (kantor) belum ada.
20. Belum adanya mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
21. Belum 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).

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan

1. Telah memiliki standar pengembangan aplikasi yang diperbaharui secara tahunan sebagai pedoman pengembangan dan pembangunan aplikasi di lingkungan Diskominfo Kota Batam, namun belum terdapat spesifikasi keamanan sistem.
2. Telah melakukan *vulnerability assessment* terhadap aplikasi yang dimiliki untuk memastikan keamanan pada aplikasi yang dikelola.
3. Telah memiliki redundan khusus server untuk memastikan server dapat tetap berjalan dalam kondisi darurat.
4. Telah melakukan pengamanan pada jaringan nirkabel dengan membatasi aksesnya, namun belum pada jaringan nirkabel.
5. Telah mengelola sertifikat elektronik di lingkungan Diskominfo Kota Batam.
6. Telah menerapkan manajemen sesi pada aplikasi yang dimiliki.
7. Baru menerapkan NTP pada jaringan CCTV.
8. Telah secara aktif melibatkan pihak ketiga/ independen (BSSN) untuk melakukan kajian terhadap keandalan keamanan informasi pada aplikasi yang dikelola.

B. Kelemahan/Kekurangan

1. Belum memiliki dokumentasi topologi jaringan termasuk pengamanannya dan segmentasi jaringan sesuai kebutuhan.

2. Belum secara rutin menganalisa kepatuhan penerapan terhadap standar konfigurasi yang dimiliki.
3. Tidak memiliki redundan jaringan atau *backup* jaringan.
4. Belum dapat memastikan ketersediaan kapasitas jaringan, sistem dan aplikasi dengan sistem monitoring yang dimiliki.
5. Belum dapat memastikan setiap jaringan, sistem dan aplikasi yang dikelola merekam log, baik untuk disimpan ataupun dianalisa.
6. Belum memiliki standar dalam penggunaan enkripsi dalam pengamanan informasi.
7. Belum melakukan pengelolaan *password*, baik penerapan penggantian *password* secara berkala, mengatur kompleksitasnya, dan penggunaan kembali *password* lama.
8. Belum dapat memastikan penerapan pengamanan untuk pembatasan akses dari luar organisasi.
9. Belum dapat memastikan versi terkini dari *desktop* dan *server*.
10. Belum seluruh aset yang dimiliki dilindungi oleh antivirus/ *antimalware*.
11. Belum dapat memastikan penerapan lingkungan pengembangan dan uji coba sistem.

VII. SUPLEMEN

A. Kekuatan/Kematangan

Memiliki draf dokumen SMKI yang memuat sebagian rencana pengelolaan layanan pihak ketiga dan pengelolaan data pribadi.

B. Kelemahan/Kekurangan

1. Belum melakukan manajemen risiko dan pengelolaan keamanan pihak ketiga.
2. Belum memastikan terhadap pengelolaan sub-kontraktor/ alih daya pada pihak ketiga, penanganan aset, pengelolaan insiden dan rencana keberlangsungan layanan pihak ketiga.
3. Belum melakukan pengelolaan layanan dan keamanan pihak ketiga.
4. Belum melakukan kajian ketika terdapat perubahan layanan dan kebijakan pihak ketiga.
5. Tidak menggunakan layanan infrastruktur awan (*cloud services*).
6. Belum melakukan penyusunan dokumen terkait pengelolaan perlindungan data pribadi yang dikelola.

VIII. REKOMENDASI

1. Dokumen Sistem Manajemen Keamanan Informasi (SMKI) dapat segera disahkan, disosialisasikan dan dipublikasikan (internal dan eksternal), diimplementasikan dan didokumentasikan, disusun turunan kebijakan (SOP, Juknis, Juklah, Pedoman), serta evaluasi kepatuhannya.
2. Menyusun Dokumen *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP), serta melakukan pengujian secara berkala (1 tahun sekali).
3. Menyusun dan melaksanakan Roadmap / Masterplan TIK termasuk aspek keamanan di dalamnya.
4. Menyusun standar kompetensi dan keahlian pengelola keamanan informasi, melakukan peningkatan kompetensi, dan mendokumentasikannya.
5. Menyusun kebijakan terkait pengelolaan data pribadi (identifikasi data yang diolah, pengamanannya hingga pemusnahannya).

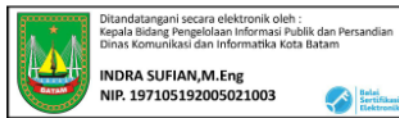
6. Menyusun kerangka kerja pengelolaan risiko keamanan informasi dapat berupa kebijakan manajemen risiko.
7. Menyusun dokumen risk register.
8. Menjabarkan lebih detail dalam draf kebijakan SMKI yang telah disusun terkait definisi klasifikasi aset informasi dan definisi hak akses terhadap masing-masing klasifikasi aset informasi.
9. Menyusun prosedur pengelolaan perubahan dan proses pengelolaan konfigurasi terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) dan menerapkan secara konsisten.
10. Menyusun pelaporan secara berkala kepada pimpinan terkait pengelolaan keamanan informasi.
11. Menyusun kebijakan terkait insiden keamanan informasi yang mengarah ke ranah hukum (pidana/ perdana).
12. Menyusun, mengelola dan mengevaluasi Daftar Induk Dokumen (DID) yang terkait Keamanan Informasi.
13. Menjadikan *risk treatment plan* sebagai dasar adanya kebijakan yang disusun dan diimplementasikan.
14. Menyusun Kebijakan Insiden Keamanan Informasi, mulai dari identifikasi, penetapan status insiden, *recovery* hingga *lesson learnt*.
15. Mencantumkan pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset/ layanan TIK dalam dokumen kontrak.
16. Menyusun kebijakan untuk kondisi tertentu dalam pelaksanaan SMKI.
17. Melaksanakan secara rutin audit internal TIK untuk memastikan kepatuhan dalam pelaksanaan keamanan informasi.
18. Menyusun kebijakan pengelolaan *security patch*.
19. Menyusun topologi jaringan (termasuk pengamanan) dan topologi segmentasi jaringan.
20. Menyusun standar konfigurasi dan mengevaluasi kepatuhannya.
21. Menyusun kebijakan pengelolaan log, mengimplementasikan dan mendokumentasikannya.
22. Menyusun kebijakan manajemen *password* dan mengimplementasikannya.
23. Memastikan antivirus/*antimalware* berjalan di seluruh desktop dan *server*.
24. Secara berkala dapat melaporkan pelaksanaan keamanan informasi (misalkan: *traffic*, anomali, tren ancaman, dsb).
25. Melakukan pengujian keamanan berkala seluruh aset yang dikelola (aplikasi, jaringan, sistem).
26. Menyusun kebijakan penggunaan enkripsi untuk pengamanan aset informasi.
27. Menerapkan lingkungan pengembangan dan uji coba yang diamankan sesuai dengan prosedur.
28. Menerapkan jaringan redundan untuk memastikan berjalannya sistem untuk dapat diakses dalam keadaan darurat.
29. Menyusun prosedur rilis aplikasi yang perlu dituangkan dalam SOP manajemen rilis aplikasi dengan tujuan untuk menyediakan aplikasi yang sesuai dengan spesifikasi tingkat akurasi yang telah ditetapkan dan menjamin *quality assurance* terhadap aplikasi yang akan naik ke *production*.
30. Perlu menyusun tata tertib penggunaan komputer, email, internet dan intranet, tata tertib pengamanan dan penggunaan aset instansi terkait HAKI, peraturan terkait instalasi piranti lunak di aset TI milik instansi, peraturan yang mengatur terkait penggunaan data pribadi dan ketentuan terkait pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.

31. Menyusun prosedur terkait penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi serta pelaporan insiden tersebut kepada pihak eksternal ataupun pihak yang berwajib.
32. Menyusun prosedur penghancuran data/aset yang sudah tidak diperlukan.
33. Menyusun prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
34. Perlu menyusun daftar data/informasi yang harus di back-up dan laporan analisa kepatuhan terhadap prosedur backup.
35. Perlu menyusun dan menetapkan peraturan pengamanan perangkat komputasi milik instansi apabila digunakan diluar lokasi kerja resmi.
36. Melakukan manajemen risiko dan pengelolaan keamanan pihak ketiga dengan menyusun *risk register*, melakukan kajian risiko, memastikan risiko tersampaikan ke pihak ketiga, tertuang dalam dokumen kontrak dan memastikan langkah mitigasi risikonya.
37. Memastikan kepada pihak ketiga dalam pengamanan informasi dalam pengelolaan sub-kontraktor/ ahli daya pada pihak ketiga.
38. Melakukan pengelolaan layanan dan keamanan pihak ketiga, mulai dari penetapan proses pengelolaannya, menentukan penanggungjawab, pengelolaan pelaporan layanan pihak ketiga dan tindak lanjutnya.
39. Melakukan pengelolaan manajemen risiko ketika perubahan layanan dan kebijakan pihak ketiga.
40. Memastikan bahwa pihak ketiga memiliki langkah dalam pengelolaan insiden dan langkah perencanaan keberlangsungan layanannya.
41. Melakukan turunan kebijakan SMKI yang disusun terkait pengelolaan perlindungan data pribadi.

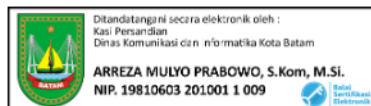
Batam, 6 April 2022

Narasumber Dinas Komunikasi dan Informatika Kota Batam :

1. Indra Sufian, M.Eng.



2. Arreza M.P, S.Kom.



3. Irpan Syarif Hasibuan, S.Kom.



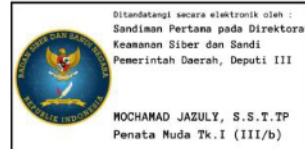
4. Irpa Darajat, ST.



Depok, 6 April 2022

Assessor Indeks KAMI:

1. Assessor : Mochamad Jazuly, S.S.T.TP.



2. Assesor : Ni Putu Ayu Lhaksmi, S.Tr.TP.

