
	<b>LAPORAN VERIFIKASI INDEKS KAMI</b>	
<b>Instansi/Perusahaan:</b>  PEMERINTAH KOTA BEKASI	<b>Narasumber Instansi/Perusahaan:</b> <ol style="list-style-type: none"> <li>1. Nindya Sari, S.Kom., M.M. 19730214 200701 2 006</li> <li>2. Zaky Ismail, A.Md. 19950511 201902 1 005</li> <li>3. Dina Yohana P. S., A.Md 19921122 201902 2 003</li> </ol>	
<b>Unit Kerja:</b> DINAS KOMUNIKASI INFORMATIKA STATISTIK DAN PERSANDIAN		
<b>Alamat:</b> Jl. Jend. A. Yani No. 2, Komplek GOR Bekasi Selatan, Kota Bekasi Jawa Barat	<b>Tel: (021) 8895 9980</b> <b>Fax:</b>	
<b>Email:</b> opd.diskominfostandi@bekasikota.go.id	<b>Pimpinan Unit Kerja:</b> Drs. Hudi Wijayanto, M.Si 19690121 199007 1 001	
<p><b>A. Ruang Lingkup:</b></p> <p>1. Instansi / Unit Kerja:</p> <p>Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi (termasuk layanan TIK seperti pusat data, NOC, Jaringan dan sistem informasi, pengelolaan informasi publik, pengelolaan statistik, dan pengelolaan persandian).</p> <p>2. Fungsi Kerja:</p> <p>Sesuai dengan Peraturan Walikota Bekasi Peraturan Wali Kota Bekasi Nomor 54 Tahun 2018 Perubahan Kedua Atas Peraturan Wali Kota Bekasi Nomor 79 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas Pokok Dan Fungsi Serta Tata Kerja Pada Dinas Komunikasi, Informatika, Statistik Dan Persandian Kota Bekasi mempunyai fungsi:</p> <ol style="list-style-type: none"> <li>a. perumusan dan penetapan rencana strategis dan rencana kerja Dinas sesuai dengan visi dan misi Daerah;</li> <li>b. penetapan pedoman dan petunjuk teknis penyelenggaraan urusan lingkup bidang komunikasi, informatika, statistik dan persandian;</li> <li>c. pembinaan dan pengendalian pelaksanaan tugas Sekretariat, Bidang-Bidang, dan Kelompok Jabatan Fungsional;</li> <li>d. pembinaan administrasi perkantoran;</li> <li>e. pemberian pelayanan dan pembinaan kepada unsur terkait di bidang komunikasi, informatika, statistik dan persandian serta pelaksanaan hubungan kerja sama dengan Perangkat Daerah, lembaga/instansi terkait dalam rangka penyelenggaraan kegiatan Dinas;</li> <li>f. pembinaan dan pengembangan karir pegawai Dinas;</li> <li>g. pelaksanaan tugas selaku Pengguna Anggaran/Pengguna Barang;</li> <li>h. penyusunan dan penyampaian laporan keuangan Dinas sesuai ketentuan yang berlaku;</li> </ol>		

## 3. Lokasi:

No.	Nama Lokasi	Alamat
1.	Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi	Gedung Diskominfo Jl. Jend. A. Yani No. 2, Komplek GOR Bekasi Selatan, Kota Bekasi Jawa Barat
2.	<i>Data Center, NOC dan Utility</i>	Gedung Setda Jl. Jend. A. Yani No. 1, Kantor Wali Kota Bekasi Jawa Barat

## B. Nama/Jenis Layanan Publik:

- Layanan informasi publik;
- Layanan informasi *website* Pemerintah Kota Bekasi;
- Layanan TIK untuk OPD (penyediaan pusat data terpusat);
- Layanan aduan masyarakat

## C. Aset TI yang kritis:

## 1. Informasi :

- Data Pribadi Masyarakat;
- Data Pegawai;
- Data Penganggaran dan Keuangan;
- Data Jaringan Komunikasi;
- Data Konfigurasi Sistem;
- Data Prosedur/ Proses Bisnis;
- Data Log dan Audit;
- Basis Data dan data file;
- Data Kontrak/ Dokumen legal.

## 2. Aplikasi:

Total aplikasi yang terdaftar dalam Asset Register 009/FRM-018/TIK/DISKOMINFOSTANDI/VII/2017 Rev 00 Agustus 2020 adalah 53 aplikasi, beberapa aplikasi tersebut antara lain:

- bekasikota.go.id;
- siap.bekasikota.go.id;
- sikerja.bekasikota.go.id;
- siencang.bekasikota.go.id;
- corona.bekasikota.go.id;
- bansosocovid19.bekasikota.go.id.

## 3. Server:

- Application Server
- Storage Server

## 4. Infrastruktur Jaringan/Network:

Intranet dan internet. Moratelindo (utama), Moratelindo (redundan dan DRC), dan Telkom (cadangan).

## D. DATA CENTER (DC):

(Beri keterangan apakah ruang Data Center terpisah dengan perimeter/pembatas, memiliki pengamanan fisik dan sarana pendukung, dsb)

X ADA, dalam ruangan khusus

☐ ADA, jadi satu dengan ruang kerja

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

*(Jika ada, jelaskan kondisi DRC: colocation di pihak ketiga atau di instansi lain termasuk pengelolaan keamanan DRC)*

X ADA

☐ Dikelola Internal

X Dikelola vendor : di Batam

☐ 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 (ref. kebijakan yang disyaratkan ISO 27001)	Ya		R
2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	Ya		R
3	Sasaran TI / Keamanan Informasi	Ya		R
4	Organisasi TI / Keamanan Informasi (IT <i>Steering Committee</i> , Fungsi Keamanan TI)	Ya		R
5	Metodologi Manajemen Risiko TI	Ya		R
6	<i>Business Continuity Plan</i>	Ya		R
7	Klasifikasi Informasi	Ya		R
8	Standar <i>software dekstop</i>	Ya		R
9	Metode Pengukuran Efektivitas Kontrol	Ya		R
10	Non Disclosure Agreement (NDA)	Ya		R
	<b>Prosedur- Prosedur:</b>			
1	Pengendalian Dokumen	Ya		R
2	Pengendalian Rekaman/Catatan	Ya		R
3	Tindakan Perbaikan & Pencegahan	Ya		R
4	Audit Internal	Ya		R
5	Penanganan ( <i>Handling</i> ) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran	Ya		R
6	Pengelolaan Media <i>Removable &amp; Disposal</i>	Ya		R
7	Pengelolaan Perubahan Sistem TI ( <i>Change Control</i> Sistem TI)	Ya		R
8	Pengelolaan Hak Akses ( <i>User Access Management</i> )	Ya		R
9	<i>Teleworking</i> (Akses Remote)	Ya		R
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	Ya		R

No.	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R: Rilis, T: Tersosialisasikan)
11	Pemantauan Sumber Daya TI: a. <i>Monitoring</i> Kapasitas b. Log Penggunaan User	Ya		R
12	Instalasi & Pengendalian <i>Software</i>	Ya		R
13	<i>Back-up &amp; restore</i> (prosedur/jadwal)	Ya		R

**Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)**

**Dokumen yang diperiksa:**

1. Peraturan Wali Kota Bekasi Nomor 54 Tahun 2018 Tentang Perubahan Kedua Atas Peraturan Wali Kota Bekasi Nomor 79 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas Pokok Dan Fungsi Serta Tata Kerja Pada Dinas Komunikasi, Informatika, Statistik Dan Persandian Kota Bekasi.
2. Peraturan Daerah Kota Bekasi Nomor 03 Tahun 2020 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kota Bekasi.
3. Keputusan Wali Kota Bekasi Nomor 555/Kep.151-DiskominfoStandi/III/2017 tentang Petunjuk Teknis Tata Kelola Pusat Data, Pemulihan, dan Komputasi Awan di Lingkungan Pemerintah Kota Bekasi.
4. Keputusan Wali Kota Bekasi Nomor 555/Kep.150-DiskominfoStandi/III/2017 tentang Tata Kelola Keamanan Informasi di Lingkungan Pemerintah Kota Bekasi.
5. Rencana Strategis Dinas Komunikasi Informatika Statistik dan Persandian Tahun 2018-2023.
6. Rencana Kerja (Renja) T.A. 2020.
7. Sertifikat ISO 2013:27001 dengan ruang lingkup layanan Data Center dan Jaringan sesuai dengan SOA 001/SOA/TIK/DISKOMINFOSTANDI/VII/ Rev 02 pada 26 Juni 2020.
8. 001/SMKI/TIK/DISKOMINFOSTANDI/VII/2017 Revisi 01 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi.
9. 001/RP/DISKOMINFOSTANDI/VII/2019 tentang *Risk Profile*.
10. 001/RCN/TIK/ DISKOMINFOSTANDI/VII/2019 Revisi 02 tentang Rencana Sasaran dan Struktur Organisasi Sistem Manajemen Keamanan Informasi.
11. 001/SOA/TIK/DISKOMINFOSTANDI/VII/2019 tentang Penetapan Ruang Lingkup SMKI dan *Statement Of Applicability* (SOA).
12. 001/RISK/TIK/DISKOMINFOSTANDI/VII/2017 Revisi 01 tentang Panduan Umum Manajemen Risiko.
13. 001/BCM/TIK/DISKOMINFOSTANDI/X/2019 tentang *Business Continuity Management* (Pengelolaan Keberlangsungan Kegiatan).
14. 001/CPST/TIK/ DISKOMINFOSTANDI/X/2019 tentang Perencanaan Kapasitas.
15. 001/RR/TIK/DISKOMINFOSTANDI/VII/2017 tentang Laporan Penilaian Risiko.
16. 004/STDR/TIK/DISKOMINFOSTANDI/VII/2017 tentang Standar Keamanan Email.
17. 006/STDR/TIK/DISKOMINFOSTANDI/VII/2017 tentang Standar Keamanan Jaringan.
18. 011/STDR/TIK/DISKOMINFOSTANDI/VII/2017 tentang Standar Penggunaan *Password*.
19. 012/STDR/TIK/DISKOMINFOSTANDI/IX/2019 tentang Standar Klasifikasi Informasi.
20. 013/STDR/TIK/DISKOMINFOSTANDI/VII/2020 tentang Standar Penggunaan Aset.
21. 001/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Pengendalian Dokumen.

22. 004/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Pemusnahan, Pembuangan atau Penggunaan Ulang Perangkat.
23. 007/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Penanganan Insiden Keamanan Informasi.
24. 011/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur *Change Manajemen*.
25. 010/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Rapat Tinjauan Manajemen.
26. 015/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Pengelolaan Data Center.
27. 023/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Pengamanan Area.
28. 024/SOP/TIK/ DISKOMINFOSTANDI/VII/2017 tentang Prosedur Pengendalian Akses.
29. 028/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur *Hardening*.
30. 030/SOP/TIK/DISKOMINFOSTANDI/VII/2017 tentang Prosedur Pengelolaan Pemasok.
31. 005/FRM-005/TIK/ DISKOMINFOSTANDI/VII/2017 tentang Formulir Rekapitulasi Hasil Internal Audit.
32. 004/FRM-006/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir *Maintenance* Pemeriksaan Suhu, Kelembaban dan Tegangan.
33. 003/FRM-007/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Analisis Insiden Keamanan Informasi (*Security Incident Analysis*).
34. 002/FRM-011/TIK/DISKOMINFOSTANDI/VII/2017 tentang *Log Change*.
35. 003/FRM-012/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Berita Acara Backup.
36. 001/FRM-016/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Kebutuhan Pelatihan.
37. 003/FRM-016/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Laporan Hasil Pelatihan.
38. 008/FRM-018/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Peminjaman dan Pengembalian Aset TI.
39. 001/FRM-020/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir *Security Screening*.
40. 009/FRM-018/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Daftar Aset.
41. 002/FRM-021/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Perjanjian Kerahasiaan NDA.
42. 002/FRM-023/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Daftar Lokasi atau Area kerja.
43. 001/FRM-024/TIK/DISKOMINFOSTANDI/III/2019 tentang Formulir User Access Matrix.
44. 003/FRM-024/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Permintaan/Penghapusan Akses.
45. 001/FRM-028/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir Permintaan *Hardening*.
46. 002/FRM-028/TIK/DISKOMINFOSTANDI/VII/2017 tentang Formulir *Cheklist Hardening*.
47. 003/FRM-028/TIK/DISKOMINFOSTANDI/VII/2017 tentang Berita Acara *Hardening*.
48. Surat Nomor 611/KOM.03.05.02/SANDIKAMI tanggal 23 Oktober 2020 tentang Hasil Pendampingan Indeks Keamanan Informasi Kota Bekasi.
49. Surat Edaran Nomor 555/240/Diskominfostandi.TIK tanggal 3 September 2020 tentang Ketentuan Kunjungan ke dalam Infrastruktur Pusat Data.

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

50. *Risk Treatment Plan* (RTP).
51. Berita Acara Pengembalian Barang (Laptop).
52. Laporan *Vulnerability Assesment Website* bekasikota.go.id. Periode Juli 2020.

53. Laporan Hasil Pengujian Rencana Keberlangsungan Kegiatan *Business Continuity Plan* (BCP).
54. Laporan *Scanning Website*/Aplikasi Server.
55. *Assessment Report* Dinas Komunikasi, Informatika, Statistik dan Persandian Pemerintah Kota Bekasi Tahun 2020.
56. Surat Perintah Kerja (SPK) Dinas Komunikasi Informatika Statistik dan Persandian.
57. Surat Undangan Pelatihan, Lembar Konfirmasi Kehadiran Pelatihan, dan Sertifikat Pelatihan.
58. *Maintenance Visit Form* dan Berita Acara Pekerjaan *Fire Susspension* dan PAC Denco Happel.
59. Info grafis Kesadaran Keamanan Informasi.
60. Formulir Kartu Inventaris Barang.
61. Tangkapan layar, Log DNS, Log IP Fire, Laporan Log Firewall, WPA PSK2 Access Point, Konfigurasi Auto Update OS, Autentikasi DNS Server, clamAV, aplikasi kepegawaian (Sikerja), aplikasi SIAP, aplikasi perencanaan & keuangan (Siencang).
62. Foto Akses Pintu NOC dan Ruang Utility, Alarm Firepro Data Centre, Vertiv Device Monitoring Suhu, Access Door dan kegiatan pada Dinas Komunikasi Informatika Statistik dan Persandian.
63. DPA Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi.
64. Daftar Induk Dokumen.

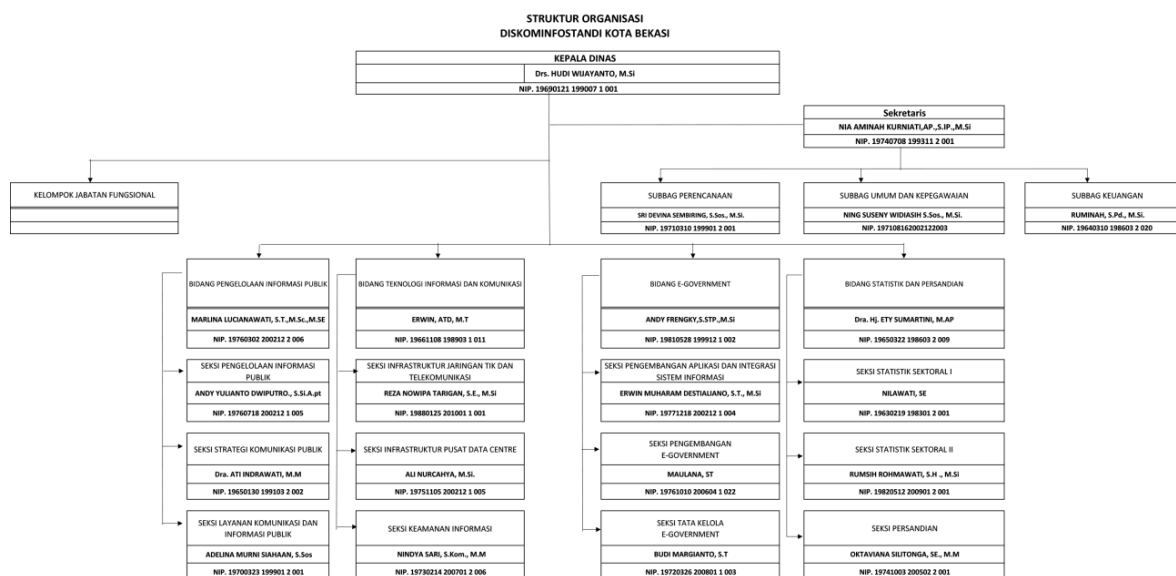
**Pemeriksaan Fisik di Lapangan:**  
Tidak ada.

Berdasarkan verifikasi terhadap dokumen, pemeriksaan desktop dan wawancara terhadap narasumber instansi/perusahaan disimpulkan sebagai berikut:

## I. KONDISI UMUM:

### Struktur Organisasi

Pada tahun 2018, terdapat perubahan struktur Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi. Adapun struktur Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi adalah sebagai berikut:



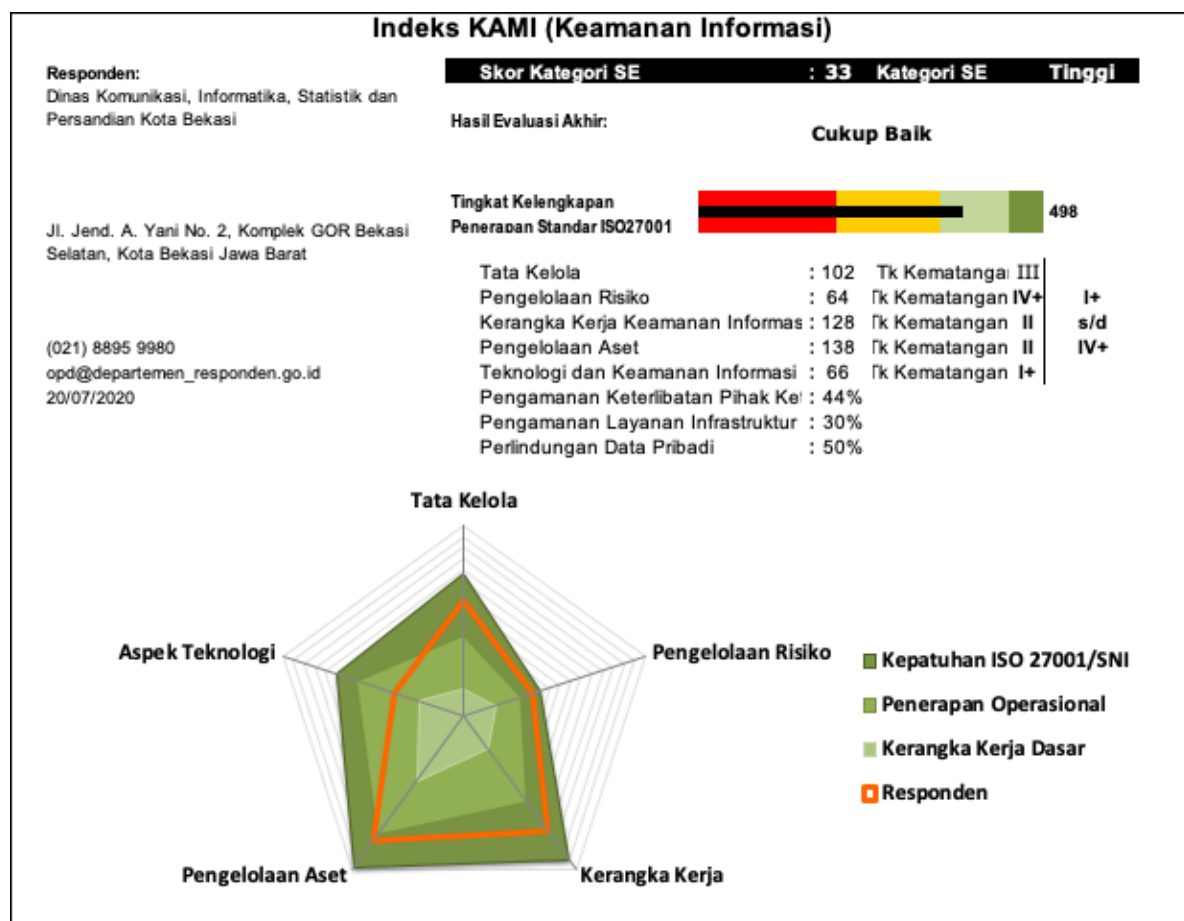


Jumlah pegawai di Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi adalah 51 personil ASN, dan 49 personil Non ASN. Sedangkan jumlah pegawai yang berhubungan dengan pengelolaan SMPI sesuai dengan Asset Register 009/FRM-018/TIK/DISKOMINFOSTANDI/VII/2017 Rev 00 Agustus 2020 berjumlah 22 orang yang berasal dari Bidang TIK dan Bidang E-Gov.

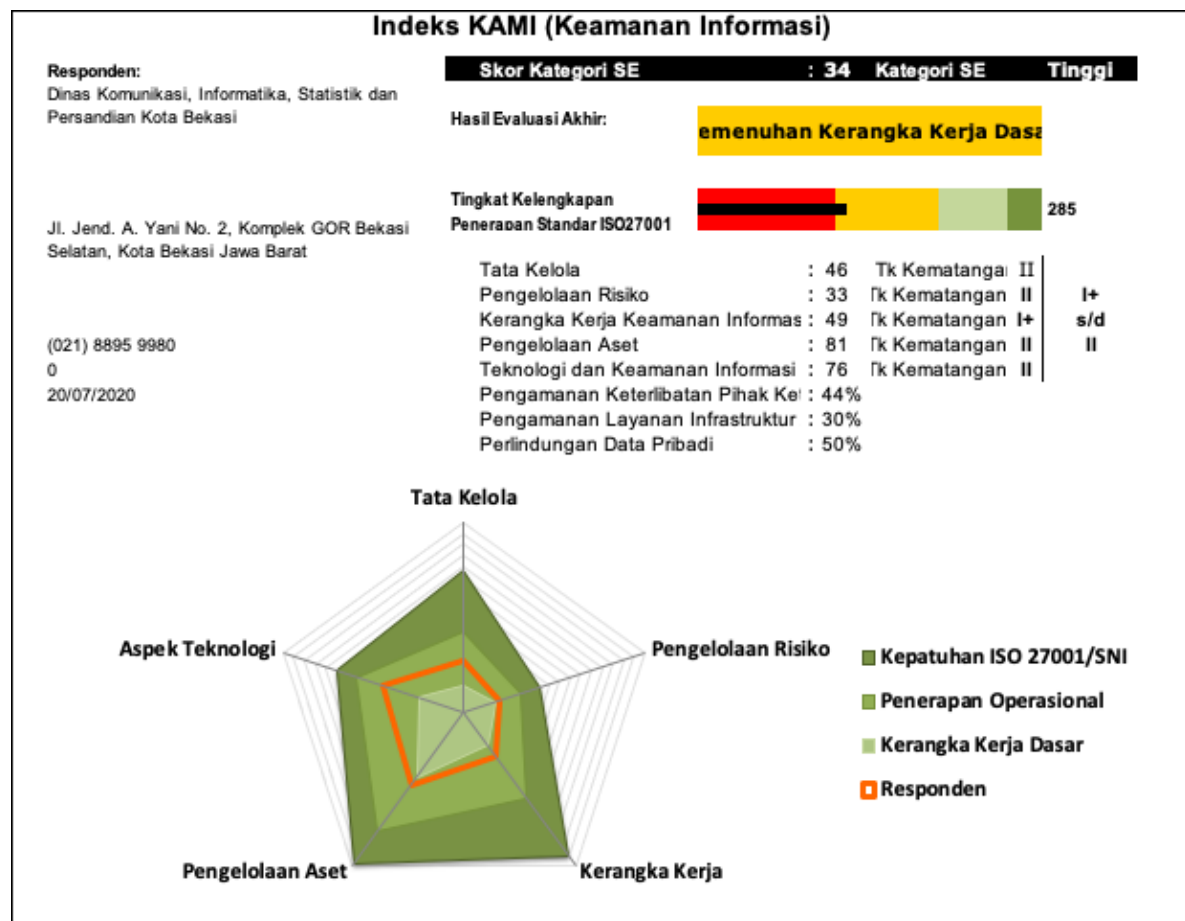
Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi telah mendapatkan Sertifikasi ISO 27001:2013 pada tahun 2020 layanan Data Center dan Jaringan sesuai dengan SOA 001/SOA/TIK/DISKOMINFOSTANDI/VII/ Rev 02 pada 26 Juni 2020. Untuk tahun 2020 ini Penilaian Mandiri indeks KAMI dilakukan dengan peningkatan ruang lingkup yaitu menjadi lingkup Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi (termasuk layanan TIK seperti pusat data, NOC, Jaringan dan sistem informasi, pengelolaan informasi publik, pengelolaan statistik, pengelolaan persandian, dan UPT) dengan kategori **TINGGI** dan hasil evaluasi akhir **CUKUP BAIK** dengan total nilai 498.

Pada tahun 2020, pemeriksaan terhadap Penilaian Mandiri yang memfokuskan pada kriteria-kriteria yang perlu dilakukan evaluasi berkala dan tindak lanjut dari rekomendasi pemeriksaan atas Penilaian Mandiri tahun 2020.

**Total nilai Penilaian Mandiri: 498 (ref. file Indeks KAMI sebelum pemeriksaan)**



**Total nilai hasil pemeriksaan atas Penilaian Mandiri: 285 (ref. file Indeks KAMI pasca pemeriksaan)**



## II. ASPEK TATA KELOLA:

### a. Kekuatan/Kematangan

1. Pimpinan dari Pemerintah Kota Bekasi sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah ada penetapan kebijakan keamanan informasi melalui Peraturan Walikota, Rensta dan Renja Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi.
2. Sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan tetapi belum melakukan pemetaan mana yang menyangkut pelanggaran hukum (pidana dan perdata) atau yang dapat di selesaikan secara internal.
3. Meskipun pihak yang terkait dengan kegiatan SMKl dengan adanya peningkatan ruang lingkup perlu untuk diidentifikasi kembali (dalam dokumen SOA dan Rencana Sasaran dan Struktur Organisasi Sistem Manajemen Keamanan Informasi), namun kegiatan sosialisasi dan peningkatan pemahaman untuk keamanan informasi (termasuk kepatuhannya) bagi semua pihak yang terkait sudah dilaksanakan.
4. Integrasi keperluan/persyaratan keamanan informasi dalam proses kerja yang ada sudah dilakukan dengan baik namun perlu untuk disesuaikan dengan adanya perubahan ruang lingkup.
5. Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku, khususnya terkait identitas pribadi di bidang kepegawaian.



**b. Kelemahan/Kekurangan**

1. Untuk lingkup layanan Data Center dan Jaringan, Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi sudah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memastikan kepatuhannya. Selain itu pejabat/petugas pelaksana pengamanan informasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi sudah ditunjuk. Namun dikarenakan adanya perubahan ruang lingkup maka penetapan tugas dan tanggung jawab serta pejabat pelaksana pengamanan informasi dalam tahap perencanaan untuk dibuat karena perlu disesuaikan dengan melibatkan bidang lain dalam Dinas.
2. Pihak-pihak terkait termasuk dengan pihak eksternal belum disesuaikan dengan lingkup Dinas. Karenanya koordinasi dengan satker terkait dan pihak eksternal yang berkepentingan untuk penerapan dan penjaminan kepatuhan pengamanan informasi dalam tahap perencanaan untuk dilakukan.
3. Laporan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan untuk bidang lain pada Dinas dalam tahap perencanaan untuk dilakukan.
4. Target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan belum dilakukan untuk semua bidang pada Dinas. Karenanya, evaluasi pencapaian, penerapan langkah perbaikan, termasuk pelaporan statusnya dalam tahap perencanaan untuk dilakukan.
5. Analisa tingkat kepatuhan di bidang lain terkait keamanan informasi belum dalam tahap perencanaan untuk dilakukan.
6. Kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata) dalam tahap perencanaan untuk disusun.

**III. ASPEK RISIKO:****a. Kekuatan/Kematangan**

1. Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi sudah mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan. Untuk ruang lingkupnya sendiri sudah menyebutkan Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi.
2. Untuk kertas kerja (*risk register*) secara keseluruhan sudah sangat baik dan rinci namun dikarenakan adanya peningkatan lingkup maka kertas kerja tersebut perlu untuk direview ulang dan di update mencakup keseluruhan risiko yang ada pada Dinas Komunikasi dan Informatika Pemerintah Kota Bekasi.

**b. Kelemahan/Kekurangan**

1. Evaluasi penyelesaian langkah mitigasi yang sudah diterapkan, pengkajian ulang profil risiko dan pengkajian ulang kerangka kerja pengelolaan risiko untuk memastikan/meningkatkan efektivitasnya dalam tahap perencanaan untuk dilakukan karena daftar risiko yang disajikan masih daftar risiko tahun 2017.
2. Pengelolaan risiko dalam tahap perencanaan untuk menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan karena mitigasi untuk risiko yang masuk dalam kategori tinggi belum terlihat efektivitasnya (terkait kemampuan program untuk dapat menurunkan risiko tersebut).

**IV. ASPEK KERANGKA KERJA:****a. Kekuatan/Kematangan**

1. Sudah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
2. Dalam dokumen kebijakan SMKI sudah ada terkait aspek keamanan dalam manajemen proyek sehingga Dinas Komunikasi, Informatika, Statistik dan

Persandian Kota Bekasi sudah membahas aspek keamanan informasi dalam manajemen proyek.

3. Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul, namun perlu dievaluasi sesuai lingkup yang baru.

**b. Kelemahan/Kekurangan**

1. Proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga dalam tahap perencanaan untuk disediakan (khususnya *Training Awareness* terkait SMKI pada Dinas untuk pihak ketiga)
2. Kebijakan dan prosedur keamanan informasi dalam tahap perencanaan untuk dapat merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi. Hal ini terlihat dari daftar risiko dan program mitigasi yang belum mewakili semua bidang dan masih dalam tahap perencanaan untuk dievaluasi).
3. Prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi (termasuk proses untuk menindak lanjuti konsekuensi dari kondisi ini) dalam tahap perencanaan untuk disusun.
4. Penerapan implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru sudah dilakukan namun untuk kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru belum ada (pada standar menyebutkan terdapat *patching* pada *firewall* dan *patching* tersebut harus dilakukan sebelum implementasi).
5. Penerapan proses pengembangan sistem yang aman (Secure SDLC) dalam tahap perencanaan untuk dilakukan.
6. Penanggulangan penerapan suatu sistem yang mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada dalam tahap penerapan.
7. Seluruh kebijakan dan prosedur keamanan informasi dalam tahap perencanaan untuk dievaluasi kelayakannya secara berkala.
8. Pelaksanaan audit internal, pengkajian/evaluasi hasil audit internal tersebut serta pelaporan hasil audit internal dinilai belum dilakukan karena lingkup baru saja ditingkatkan menjadi Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi.
9. Pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada serta rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) untuk ruang lingkup yang baru dinilai belum ada.

**V. ASPEK PENGELOLAAN ASET**

**a. Kekuatan/Kematangan**

1. Pengelolaan aset pada Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi secara umum sudah baik. Pengelolaan tersebut dilakukan melalui Aset Register dan User Access Matrix. Proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi juga sudah tersedia dalam SOP Pengelolaan Perubahan/*Change Manajemen*.
2. Tata tertib penggunaan komputer, email, internet dan intranet sudah tersedia.
3. Mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga sudah ada dalam *Non Disclosure Agreement* (NDA) dan Perjanjian Kerja Sama.
4. Pengelolaan konfigurasi dinilai dalam tahap sebagian diterapkan. Hal ini dapat dilihat dari Log Change dan Proses Konfigurasi.

**b. Kelemahan/Kekurangan**

1. Definisi tanggung jawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan dalam tahap perencanaan untuk disusun, khususnya untuk lingkup yang baru.
2. Peraturan terkait instalasi peranti lunak di aset TI milik instansi/perusahaan dalam perencanaan untuk disusun. Dalam kebijakan SMKI sudah terdapat pengaturan terkait instalasi perangkat lunak, namun perlu direviu apakah masih reliabel atau perlu ditambahkan kontrol baru.
3. Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi dalam tahap perencanaan.
4. Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi dan proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib dalam perencanaan untuk diatur. Hal ini terhubung dengan pengaturan pada Aspek Tata Kelola (2.22).
5. Daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur backup-nya dalam perencanaan untuk dibuat. Untuk Berita Acara Backup-Restore dan Form Backup sudah ada namun tidak memenuhi untuk menjadi bukti dari poin ini.
6. Secara keseluruhan terkait pengamanan fisik dinilai dalam tahap perencanaan. Hal tersebut dikarenakan adanya penambahan ruang lingkup yang mengakibatkan bertambahnya lokasi fisik dan penerapan pengamanan fisiknya. Untuk data center sendiri pengamanan fisiknya dinilai sudah baik.

**VI. ASPEK TEKNOLOGI****a. Kekuatan/Kematangan**

1. Pengamanan sudah dilakukan lebih dari satu lapis. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll). Hal ini dapat dilihat dari topologi jaringan pada Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi.
2. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor dan setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log. Hal ini terlihat dari sistem SOC dan log yang ada.
3. Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi baik dari dalam instansi maupun luar instansi. Pengamanan tersebut dilakukan untuk fisik (kontrol akses berdasar *fingerprint* atau PIN) dan jaringan (terdapat *monitoring wireless* dan *password* untuk keamanan jaringan).
4. Terdapat rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa *antivirus/antimalware* telah dimutakhirkan secara rutin dan sistematis. Untuk update antivirus dilakukan secara otomatis sesuai dengan pengaturan update yang diset.
5. Laporan penyerangan virus/*malware* yang gagal/sukses ditindaklanjuti dan diselesaikan sudah ada dan dilakukan sebagai bagian dari penanganan insiden.
6. Audit eksternal untuk ruang lingkup *data center* dan layanan sudah dilakukan namun untuk lingkup keseluruhan dinas dinilai dalam tahap perencanaan.

**b. Kelemahan/Kekurangan**

1. Log dinilai dalam perencanaan untuk dianalisis secara berkala.
2. Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi dinilai dalam tahap perencanaan terkait dengan penerapan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan.
3. Sistem dan aplikasi secara belum secara otomatis mendukung dan menerapkan penggantian *password*. Prosedur penggantian *password* juga belum diatur secara lengkap pada Standar Penggunaan *Password*.

4. Akses yang digunakan untuk mengelola sistem (administrasi sistem) dalam perencanaan untuk menggunakan bentuk pengamanan khusus yang berlapis.
5. Mekanisme sinkronisasi waktu yang akurat untuk keseluruhan jaringan, sistem dan aplikasi dinilai dalam perencanaan untuk dilakukan. Hal tersebut dikarenakan pemeriksaan NTP Server dan semua komputer yang terhubung dengan jaringan untuk keseluruhan ruang lingkup yang baru.
6. Penerapan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun dinilai belum dilakukan. Hal ini terhubung dengan SDLC yang ada pada Area Kerangka Kerja (4.13).

## VII. REKOMENDASI

1. Secara keseluruhan aspek Tata Kelola Pemerintah Kota Bekasi sudah memiliki dasar fungsi atau organisasi keamanan informasi yang baik untuk lingkup layanan *data center* dan jaringan. Dikarenakan peningkatan ruang lingkup menjadi Dinas, maka beberapa hal perlu disesuaikan khususnya yang berada pada bidang selain TIK dan E-government di Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi. Misalnya Dokumen Rencana SMKI khususnya bagian Sumber Daya yang dibutuhkan, Dokumen Anjab ABK, BCP/DRP, Struktur dan pihak-pihak yang terkait, risiko keamanan informasi dari bidang lain, tinjauan manajemen, kepatuhan, kebijakan/SOP terkait insiden apabila ada eskalasi insiden ke ranah hukum /pelanggaran hukum, dan penjadwalan.
2. Terkait dengan kepatuhan, dikarenakan ruang lingkup dari penerapan SMKI semakin luas (menjadi Dinas) maka kepatuhan terhadap peraturan baik itu kebijakan, standar dan prosedur SMKI perlu dilakukan untuk semua bidang yang ada pada Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi.
3. Untuk kertas kerja (*risk register*) untuk dievaluasi dan diidentifikasi terlebih dahulu sehingga mencakup risiko seluruh bidang di Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi. Risiko dari tahun 2017 juga perlu dilakukan evaluasi untuk melihat apakah mitigasi yang dipilih (dan dimasukkan dalam program) sudah berjalan dengan efektif sehingga dapat mengurangi risiko tersebut.
4. Daftar aset (*Asset Register*) untuk dapat didata kembali dengan memasukkan aset (Informasi, SDM, Fisik, Software/Aplikasi, Layanan, dan Integible) dari bidang lainnya pada Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi. Selain itu beberapa data pada daftar aset saat ini juga perlu direviu dan dilengkapi dengan kondisi saat ini, khususnya untuk daftar aplikasi yang dikelola pada Aset Software.
5. Guna mengetahui aset yang perlu dilakukan *backup*, maka daftar aset perlu untuk ditambahkan kolom terkait *backup* (jika di x maka aset tersebut perlu dilakukan *backup*) dan periode *backup* dari aset tersebut. Aset yang wajib ditambahkan terkait *backup* ini adalah Aset Informasi dan Software.
6. Perlu adanya koordinasi dengan bidang lain pada Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi terkait pelaksanaan dan evaluasi kerangka kerja kebijakan panduan manajemen risiko sebagai bagian dari SMKI Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi.
7. Perlu diperjelas pejabat/personil yang masuk dalam Tim Pengelola Risiko dan sebaiknya melibatkan bidang lain pada Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi.
8. Disarankan untuk mengevaluasi kebijakan panduan manajemen risiko terutama terkait selera risiko (ambang penerimaan risiko) melihat lingkup untuk manajemen risiko saat ini adalah Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi.
9. Daftar Induk Dokumen perlu untuk dilakukan reviu dan pendataan ulang dikarenakan beberapa dokumen yang ditemukan selama pelaksanaan verifikasi tidak terdaftar dalam Daftar Induk Dokumen.

10. Perlu dibuatkan formulir komunikasi kebijakan keamanan informasi ke internal dan eksternal Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Bekasi.
11. SOP *patch manajemen* yang menyangkut operasional layanan yang ada saat ini perlu untuk disusun.
12. Sebaiknya disusun prosedur/*flowchart*/kebijakan apabila ada pembangunan atau pengembangan aplikasi baru termasuk memasukkan tahapan yang perlu dilakukan apabila ada insiden saat menerapkan atau mengembangkan sistem baru.
13. Pelaksanaan audit internal untuk ruang lingkup yang baru perlu dilakukan. Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi juga perlu melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada.
14. Perlu dibuatkan kebijakan terkait penggunaan data pribadi dengan pemberian ijin tertulis dari pemilik data dan sebaiknya dibuatkan templat perijinan tertulis penggunaan data pribadi.
15. Daftar lokasi atau area kerja perlu untuk diperbaharui sesuai dengan ruang lingkup yang baru dan pengamanan khususnya pengamanan fisik perlu ditentukan. Misalnya seperti pembuatan *visitor log* untuk seluruh area fisik yang berada dalam lokasi yang berbeda.
16. Laporan *monitoring* analisa log perlu dibuatkan formulirnya dan dilakukan penyusunannya secara berkala untuk semua log yang ada di lingkup Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi.
17. Perlu dibuatkan mekanisme agar SOC dapat memastikan semua komputer yang terhubung ke jaringan Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi terpantau dan terotomatisasi pembaharuan khususnya pembaharuan anti virus, OS, dan *password*.
18. Pengamanan berlapis untuk akses yang digunakan untuk mengelola sistem (administrasi sistem) perlu diterapkan. Misalnya dengan menggunakan dua metode (*what you know* dan *what you have* atau *what you are*).
19. Secara besaran kegiatan SMKI pastinya akan berhubungan dengan persandian, karenanya pada saat penyusunan dan pelaksanaan untuk dapat berkoordinasi dan mengikutsertakan Seksi Persandian yang ada pada Bidang Statistik dan Persandian. Keikutsertaan antara lain dalam penyusunan aturan (khususnya terkait pembagian area atau metode pengamanan), pengelolaan kunci enkripsi, dan juga audit internal (karena dibutuhkan pihak ketiga independen selain implementor SMKI atau Bidang TIK dan E-Government untuk pelaksanaan audit internal).
20. Audit eksternal secara berkala perlu dilakukan untuk keseluruhan lingkup Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Bekasi.

<p><b>Sawangan, 22 Desember 2020</b></p> <p>Narasumber Instansi/Perusahaan:</p> <ol style="list-style-type: none"> <li>1. Nindya Sari, S.Kom., M.M. 19730214 200701 2 006</li> <li>2. Zaky Ismail, A.Md. 19950511 201902 1 005</li> <li>3. Dina Yohana P. S., A.Md 19921122 201902 2 003</li> </ol>	<p>Asesor Indeks KAMI:</p> <ol style="list-style-type: none"> <li>1. Asesor Utama: Julysa Tri Wulandari, S.ST.</li> <li>2. Asesor Utama: Fajarudin Setio Utomo, S.ST., M.AP.</li> <li>3. Asesor Pendamping: Vira Septiyana Kasma, S.ST.</li> </ol>
---	--