LAPORAN VERIFIKASI INDEKS KAMI

INDEKS KEAMANAN INFORMASI

Instansi/Perusahaan: PEMERINTAH DAERAH PROVINSI JAWA BARAT	**Narasumber Instansi/Perusahaan:** 1. HERMIN WIJAYA, ST, M.Kom 19730916 199803 2 002 2. RIZKI HUSTINIASARI, ST 19840213 201503 2 003 3. IWAN GUNAWAN, SE, Msi 19610523 199203 1 005 4. BAMBANG INDRA RACHMAWAN, A.Md 19690115 199803 1 003
Unit Kerja: DINAS KOMUNIKASI & INFORMATIKA	
Alamat: Jl. Taman Sari no. 55 Bandung	**Tel: 022 2502898** **Fax:**
Email: *bid.pkami@jabarprov.go.id*	**Pimpinan Unit Kerja:** Dr. HENING WIDIATMOKO, MA 19640831 199203 1 008

A. Ruang Lingkup:

1. Instansi / Unit Kerja:

DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH PROVINSI JAWA BARAT

2. Fungsi Kerja:

Merencanakan, mengoperasikan, mengelola, menganalisa, memelihara dan mengimplementasikan sistim informasi di Dinas Komunikasi dan Informatika Provinsi Jawa Barat termasuk di dalamnya aplikasi dan database, jaringan, kebijakan, keamanan,dan risiko Teknologi Informasi serta menjamin kualitas layanan TIK agar sesuai dengan standar nasional dan internasional

3. Lokasi:

No	Nama Lokasi	
1	Diskominfo Provinsi Jawa Barat	Jl. Taman Sari no. 55 Bandung
2	Data Center	Jl. Taman Sari no. 55 Bandung

B. Nama /Jenis Layanan Publik:

a. MCAP (Mobile Community Access Point)
b. Layanan wifi area publik
c. Ruang layanan internet publik
d. Layanan informasi website jabarprov.go.id
e. Layanan aduan masyarakat

C. Aset TI yang kritikal:

1. Informasi :
   - -Data pegawai
   - -Data keuangan
   - -Data Jaringan Komunikasi
   - -Data Konfigurasi Sistem

2. Aplikasi:
   -E-office
   -RKPD Online
   -E-monev
   -Simpeg
   -SIPKD
   -SKP
   -Aplikasi Perijinan
   -Website Jabarprov.go.id
   -Website diskominfo
   -E-SAKIP
   -ATISIBADA
3. Server:
   -server e-Office
   -server RKPD Online
   -server e-Monev
   -server Simpeg
   -server SIPKD
   -server SKP
   -server Perijinan
   -server website jabarprov.go.id
   -server e-SAKIP
4. Infrastruktur Jaringan/Network:
   - Telkom dan Indosat

D. DATA CENTER (DC):

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

☑ 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)

☑ ADA → ☐ Dikelola Internal ☑ Dikelola vendor : ICON+

☐ TIDAK ADA

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

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draft, R:Rilis, T:Tersosialisasikan)
	Kebijakan, Sasaran, Rencana, Standar			
1	Kebijakan Keamanan Informasi (ref. kebijakan yg disyaratkan ISO 27001)	✓		R
2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	✓		R
3	Sasaran TI / Keamanan Informasi	✓		R
4	Organisasi TI / Keamanan Informasi (IT Steering Committee, Fungsi Keamanan TI)	✓		R

5	Metodologi Manajemen Risiko TI	✓		R
6	Business Continuity Plan	✓		R
7	Klasifikasi Informasi	✓		R
8	Standar software dekstop	✓		R
9	Metode Pengukuran Efektivitas Kontrol	✓		R
10	Non Disclosure Agreement (NDA)	✓		R
	Prosedur- Prosedur:			
1	Pengendalian Dokumen	✓		R
2	Pengendalian Rekaman/Catatan	✓		R
3	Tindakan Perbaikan & Pencegahan	✓		R
4	Audit Internal	✓		R
5	Penanganan (Handling) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran	✓		R
6	Pengelolaan Media Removable & Disposal	✓		R
7	Pengelolaan Perubahan Sistem TI (Change Control Sistem TI)	✓		R
8	Pengelolaan Hak Akses (User Access Management)	✓		R
9	Teleworking (Akses Remote)	✓		R
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	✓		R
11	Pemantauan Sumber Daya TI: a. Monitoring Kapasitas b. Log Penggunaan User	✓		R
12	Instalasi & Pengendalian Software	✓		R
13	Back-up & restore (prosedur/jadwal)	✓		R

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Peraturan Menteri KP No. 31/Permen-KP/2018 tentang Masterplan Teknologi Informasi Kementerian Kelautan dan Perikanan Tahun 2018 – 2022
2. K01/SMKI Kebijakan Keamanan Informasi Diskominfo
3. K02/SMKI Kebijakan Manajemen Risiko Teknologi Informasi
4. K03/SMKI Kebijakan Ruang Lingkup Sertifikasi & SOA
5. K04/SMKI Kebijakan Kelangsungan Layanan Data Center
6. K05/SMKI Kebijakan Peran dan Tanggung Jawab Keamanan Informasi
7. PR-01/SMKI Prosedur Pengendalian Dokumen
8. PR-02/SMKI Prosedur Pengendalian Rekaman
9. PR-03/SMKI Prosedur Audit Internal
10. PR-04/SMKI Prosedur Komunikasi Internal dan Eksternal
11. PR-05/SMKI Prosedur Manajemen Review
12. PR-06/SMKI Prosedur Tindakan Perbaikan dan Improvement

13. PR-07/SMKI Prosedur Monitoring dan Evaluasi Vendor
14. PR-08/SMKI Prosedur Pengelolaan dan Penghancuran Removable Media
15. PR-09/SMKI Prosedur Penanganan Pelabelan dan Pertukaran Informasi (termasuk disposal)
16. PR-10/SMKI Prosedur Pengendalian Perubahan TI
17. PR-11/SMKI Prosedur Pengelolaan Insiden Keamanan Informasi
18. PR-12/SMKI Prosedur Instalasi dan Kepatuhan Lisensi Software
19. SOP-01/eGov SOP Backup dan Restore
20. SOP-02/eGov SOP Penempatan (Co-location) Server
21. SOP-03/eGov SOP Pemberian Hak Akses Pengunjung Data Center
22. SOP-04/eGov SOP Hosting Aplikasi dan Web
23. SOP-05/eGov SOP Monitoring & Pemeliharaan Data Center
24. SOP-06/eGov SOP Pengunggahan Konten Release
25. SOP-07/eGov SOP Penerbitan Sub Domain
26. SOP-08/eGov SOP Pemeriksaan Rutin Suhu Ruangan Server
27. SOP-09/eGov SOP Raised Floor Ruang Server, NOC dan Ruang Telco
28. SOP-10/eGov SOP Pemeriksaan Kabel Perangkat Data Center dan Jaringan Komunikasi
29. SOP-11/eGov SOP Penanganan Permasalahan Jaringan Komputer
30. SOP-12/eGov SOP Layanan Video Conference
31. SOP-13/eGov SOP Monitoring dan Pemeliharaan CCTV
32. SOP-14/eGov SOP Pemeriksaan Jaringan VPN
33. SOP-13/eGov SOP Alarm Fire
34. SOP-12/eGov SOP Pengelolaan Insiden Keamanan Informasi Jabarprov-CSIRT

Bukti-bukti (rekaman/arsip) penerapan SMKI:

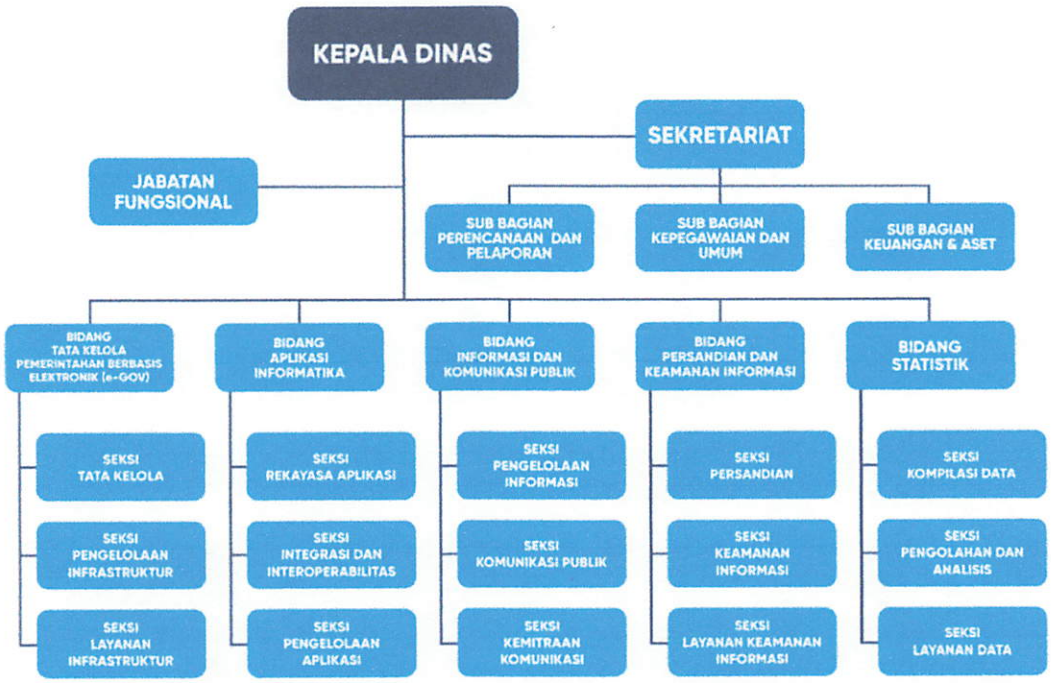
1. Rekaman video Edukasi Pencegahan dan Penaggulangan Kebakaran
2. Rekaman video Latihan Evakuasi Bencana
3. Daftar Induk Dokumen
4. Dokumentasi Jaringan
5. Daftar aset
6. Risk Register
7. Laporan pendampingan Persiapan ISO27001 (Sucofindo)
8. Standard Kompetensi Jabatan
9. Risalah Rapat Tinjauan Manajemen (Management Review)

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

I. KONDISI UMUM:

Struktur Organisasi

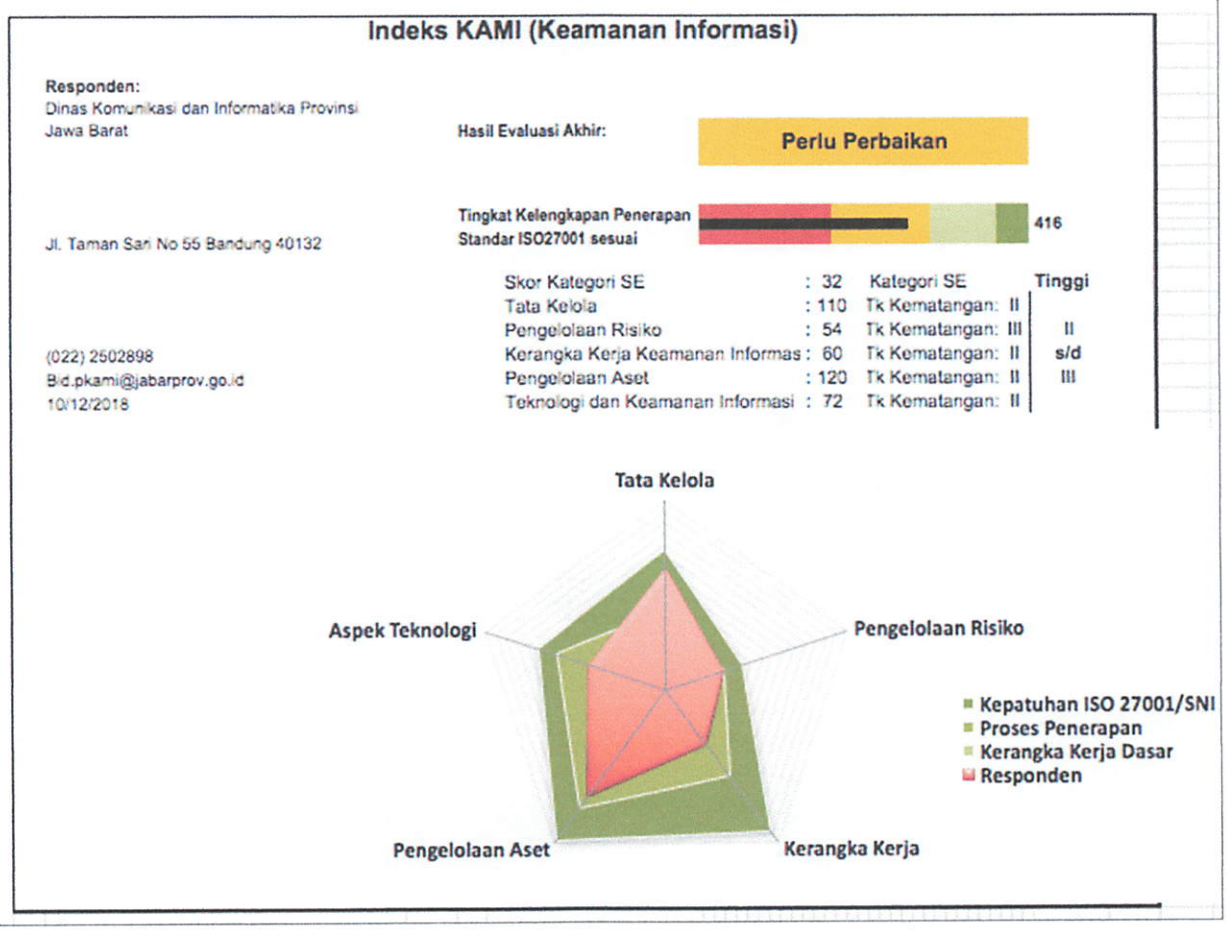
Dinas Kominfo Provinsi Jabar mengalami perubahan struktur organisasi akhir tahun 2016, dengan adanya pemisahan struktur dengan Dinas Perhubungan. Pada tahun 2018 mengalami perubahan struktur organisasi lagi dengan adanya penambahan Bidang Persandian dan Keamanan Informasi. Adapun struktur Dinas Komunikasi dan Informatika yang baru adalah sebagai berikut:



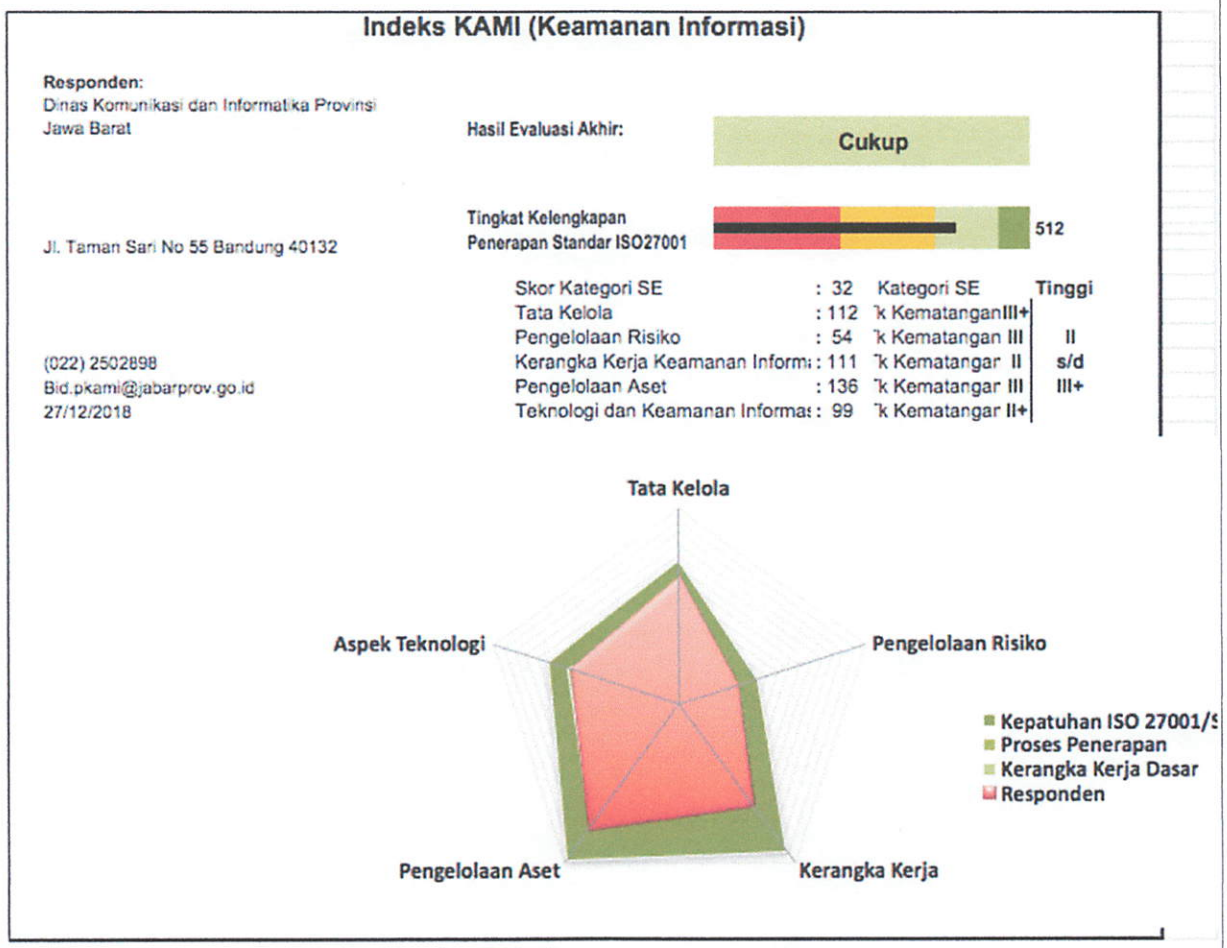
Jumlah pegawai di Dinas Kominfo adalah 98 personil PNS, dan sekitar 50 personil outsourcing. Sedangkan jumlah pegawai di Bidang Persandian dan Keamanan Informasi sebanyak 9 personil PNS.

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

Total Score Sebelum Verifikasi: 416 (ref. file Indeks KAMI sebelum Verifikasi)



Total Score Setelah Verifikasi: 512 (ref. file Indeks KAMI pasca Verifikasi)



II.KEKUATAN/KEMATANGAN:

Dinas Kominfo Jawa Barat telah menunjukkan komitmen yang kuat terhadap penerapan program keamanan informasi sesuai Peraturan Menteri Kominfo nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI).

Dinas Kominfo Jabar telah menjalani audit Sertifikasi ISO 27001:2013, dan dinyatakan memenuhi syarat untuk mendapatkan Sertifikat ISO 27001:2013 dengan ruang lingkup pengamanan fisik dan lingkungan Data Center

a. **Aspek Ketersediaan Kerangka Kerja**

1. Pimpinan secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, termasuk penetapan kebijakan terkait
2. Instansi sudah memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab mengelola keamanan informasi dan menjaga kepatuhannya
3. Penanggungjawab pelaksanaan pengamanan informasi sudah diberikan alokasi sumber daya yang cukup untuk mengelola dan menjamin kepatuhan program keamanan informasi
4. Instansi sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhan bagi semua pihak terkait
5. Instansi sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi
6. Instansi sudah mengintegrasikan sebagian keperluan persyaratan keamanan informasi dalam

proses kerja yang ada

7. Pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal, Umum, Keuangan, dsb) dan pihak eksternal yang berkepentingan untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak
8. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan
9. Penanggungjawab pengelolaan keamanan informasi sudah melaporkan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan instansi secara resmi meskipun belum rutin
10. Sebagian kondisi dan permasalahan keamanan informasi di instansi sudah menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di instansi
11. Pimpinan satuan kerja di instansi sudah menerapkan program khusus untuk mematuhi sebagian tujuan dan sasaran kepatuhan pengamanan informasi
12. Instansi sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi pejabat dan petugas pelaksana
13. Instansi sudah menerapkan sebagian target dan sasaran pengelolaan keamanan informasi untuk beberapa area, meskipun belum mengevaluasi pencapaiannya secara rutin
14. Instansi sudah mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan
15. Instansi sudah mempunyai sebagian kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan
16. Instansi sudah menetapkan sebagian ambang batas tingkat risiko yang dapat diterima
17. Instansi sudah mendefinisikan kepemilikan dan pihak pengelola sebagian asset meskipun masih terbatas pada aset fisik
18. Ancaman dan kelemahan yang terkait dengan aset informasi sudah teridentifikasi meskipun belum secara menyeluruh
19. Sudah memiliki Kebijakan Keamanan Informasi, kebijakan manajemen risiko, dan mayoritas dokumen yang dipersyaratkan dalam indeks KAMI
20. Kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan pada semua pegawai
21. Sudah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanan
22. Sebagian kebijakan dan prosedur keamanan informasi yang ada sudah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi
23. Sudah tersedia proses untuk mengidentifikasi sebagian kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan
24. Sudah tersedia daftar inventaris aset informasi dan asset yang berhubungan dengan proses teknologi informasi, mesipun belum dilakukan menyeluruh
25. Sudah tersedia definisi klasifikasi aset informasi yang sesuaid engan peraturan perundangan yang berlaku
26. Sudah tersedia proses yang mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya meskipun belum mencakup proses evaluasi
27. Sudah ada tata tertib penggunaan email
28. Sudah ada prosedur backup server meskipun belum mencakup ujicoba pengembalian data (restore)
29. Sudah ada prosedur untuk user yang mutasi/keluar serta tenaga kontrak yang habis masa kerjanya

b. Aspek Penerapan

1. Sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang
2. Sudah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik
3. Infrastruktur komputasi sudah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya
4. Infrastruktur komputasi yang terpasang sudah terlindungi dari gangguan pasokan listrik atau dampak dari petir
5. Sudah tersedia peraturan pengamanan perangkat komputasi milik Instansi apabila digunakan di luar lokasi kerja resmi
6. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sudah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (pemadam api, pengatur suhu dan kelembaban) yang sesuai
7. Sudah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting
8. Sudah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga
9. Sudah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga, meskipun belum konsisten dalam pelaksnaannya
10. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan
11. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)
12. Sudah tersedia konfigurasi standar untuk keamanan sistem bagi aset jaringan yang dimutakhirkan sesuai kebutuhan dan perkembangan standar industri yang berlaku
13. Jaringan, system dan aplikasi yang digunakan sudah dipindai untuk menfidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi
14. Sebagian infrastruktur jaringan, sistem dan aplikasi sudah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan
15. Setiap perubahan dalam sistem informasi sudah secara otomatis terekam dalam log
16. Upaya akses yang tidak berhak secara otomatis sudah terekam dalam log
17. Sudah menerapkan enkripsi untuk melindungi aset informasi
18. Sudah ada standar dalam menggunaan enkripsi
19. Sebagian sistem dan aplikasi sudah secara otomatis mendukung dan menerapkan penggantian password
20. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeout dan lockout setelah gagal login
21. Sudah menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi
22. Sudah menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi
23. Setiap desktop dan server sudah dilindungi dari penyerangan virus (malware)
24. Sudah ada laporan penyerangan virus/malware yang ditindaklanjuti
25. Keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada
26. Setiap aplikasi telah memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi
27. Instansi sudah menerapkan lingkungan pengembangan dan ujicoba yang disesuaikan dengan standar platform teknologi
28. Instansi sudah melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin

III. KELEMAHAN/KEKURANGAN:

a. Aspek Kerangka Kerja

1. Instansi belum mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku
2. Kerangka kerja pengelolaan risiko belum dikaji secara berkala
3. Konsekuensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan
4. Belum tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi
5. Instansi belum menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan
6. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala
7. Instansi 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 pembenahan yang diperlukan, telah diterapkan secara efektif
8. Instansi belum mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten

b. **Aspek Penerapan**

1. Belum ada peraturan penggunaan data pribadi yang mensyaratkan pemberian izin tertulis oleh pemilik data pribadi
2. Belum tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga termasuk memastikan aspek HAKI dan pengamanan akses yang digunakan
3. Instansi belum secara rutin menganalisis kepatuhan penerapan konfigurasi standar yang ada
4. Semua log belum dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isisnya (untuk kepentingan jejak audit dan forensik)
5. Sistem operasi untuk perangkat desktop dan server belum semua dimutakhirkan dengan versi terkini, karena terjadi konflik dengan aplikasi yang berjalan

IV. REKOMENDASI:

1. Melengkapi standar dan prosedur, serta bukti implementasi Kebijakan SMKI yang belum disusun
2. Menetapkan dan merilis standar dan prosedur yang sudah disusun dalam bentuk draft
3. Memenuhi aktivitas yang masih dalam perencanaan maupun baru dilaksanakan sebagian di Aspek Kerangka Kerja, antara lain:
    1. Perlu memetakan secara lengkap peran pelaksana pengamanan informasi yang mencakup semua keperluan, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan
    2. Seluruh pelaksana pengamanan informasi di instansi sebaiknya memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku
    3. Instansi perlu mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku
    4. Instansi perlu mendefinisikan tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK
    5. Instansi perlu mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)
    6. Instansi perlu menyusun langkah mitigasi dan penanggulangan risiko
    7. Langkah mitigasi perlu disusun sesuai tingkat prioritas dan target penyelesaian dan penanggungjawabnya
    8. Status penyelesaian langkah mitigasi risiko perlu dipantau secara berkala untuk memastikan penyelesaian atau kemajuan kerja
    9. Penyelesaian langkah mitigasi perlu diterapkan dan dievaluasi melalui proses yang

obyektif dan terukur untuk memastikan konsistensi dan efektivitasnya

10. Profil risiko dan mitigasinya perlu dikaji ulang secara berkala
11. Kerangka kerja pengelolaan risiko perlu dikaji secara berkala
12. Pengelolaan risiko harus menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan
13. Perlu menyusun proses (mencakup pelaksana, mekanisme, jadwal, materi dan sasaran) untuk mengkomunikasikan kebijakan keamanan informasi dan perubahannya kepada semua pihak terkait, termasuk pihak ketiga
14. Konsekuensi dari pelanggaran kebijakan keamanan informasi perlu didefinisikan, dikomunikasikan dan ditegakkan
15. Perlu menyusun prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi
16. Perlu menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangan dan melaporkannya
17. Instansi sebaiknya menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul
18. Instansi perlu menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan
19. Perlu ada proses untuk menanggulangi ketidakpatuhan atau risiko baru yang timbul akibat penerapan suatu sistem, termasuk penerapan pengamanan baru
20. Perlu menetapkan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK
21. Rancangan perencanaan pemulihan bencana terhadap layanan TIK tersebut perlu mendefinisikan komposisi, peran, wewenang dan tanggung jawab tim
22. Sebaiknya ada uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) yang dilakukan sesuai jadwal
23. Perlu mendokumentasikan hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan)* dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada
24. Seluruh kebijakan dan prosedur keamanan informasi sebaiknya dievaluasi kelayakannya secara berkala
25. Instansi perlu memiliki strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirnanya disesuaikan dengan kebutuhan dan perubahan profil risiko
26. Pelaksanaan audit internal perlu mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi
27. Instansi perlu 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 pembenahan yang diperlukan, telah diterapkan secara efektif
28. Instansi perlu mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten.

4. Memenuhi aktivitas yang masih dalam perencanaan maupun baru dilaksanakan sebagian di Aspek Penerapan, antara lain:
   1. Perlu menyusun definisi tingkatan akes yang berbeda dari setiap klasifikasi asset informasi dan matriks yang merekam alokasi akses tersebut
   2. Perlu menyusun proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten
   3. Perlu menyusun proses pengelolaan konfigurasi yang diterapkan secara konsisten
   4. Perlu menyusun proses untuk merilis asset baru ke dalam lingkungan operasional dan memutakhirkan inventarisasi asset informasi
   5. Perlu menyusun peraturan penggunaan data pribadi yang mensyaratkan pemberian izin

tertulis oleh pemilik data pribadi

6. Perlu menyusun prosedur penggunaan perangkat pengolah informasi milik pihak ketiga termasuk memastikan aspek HAKI dan pengamanan akses yang digunakan
7. Instansi sebaiknya secara rutin menganalisis kepatuhan penerapan konfigurasi standar yang ada
8. Semua log perlu dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)
9. Meningkatkan manajemen insiden keamanan informasi yang terkait pelaporan, pencatatan, pengarsipan insiden keamanan informasi

5. Meningkatkan Aspek pengamanan fisik Data Center, antara lain :
    1. Menerapkan prosedur akses masuk pihak ketiga/ tamu secara konsisten baik untuk masuk ke lingkungan Diskominfo, maupun khusus ke Data Center
    2. Memasang smoke detector dalam ruangan data center
    3. Melengkapi fasilitas gedung dengan sistem hydran pemadam kebakaran
    4. Memperhatikan/menyesuaian tata letak APAR dengan merujuk PermenakertransnRI No 4/MEN/1980 tentang syarat-syarat Pemasangan dan Pemeliharaan Alat Pemadan Api Ringan

Jakarta, 28 Desember 2018

Narasumber Instansi/Perusahaan:

1. HERMIN WIJAYA, ST, M.Kom
   19730916 199803 2 002

2. RIZKI HUSTINIASARI, ST
   19840213 201503 2 003

3. IWAN GUNAWAN, SE, Msi
   19610523 199203 1 005

4. BAMBANG INDRA RACHMAWAN, A.Md
   19690115 199803 1 003

Assessor Indeks KAMI:

1. Assessor Utama:
   BAMBANG HERU TJAHJONO

2. Assessor Pendamping:
   BESUS NUGROHADI