	LAPORAN **VERIFIKASI INDEKS KAMI**	

Instansi/Perusahaan: DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA BARAT	**Narasumber Instansi/Perusahaan:** 1. Hermin Wijaya, ST, M.Kom 2. Rizki Hustiniasari, ST 3. M. Mulyadi 4. Dandi M Iqbal 5. Hannif Izzatul I
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:** Setiaji ST, M.Si **NIP 19740608 199803 1 003**

A. Ruang Lingkup:

Layanan Infrasrtuktur (Data Center, NOC, SOC, Jaringan, Server), Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika Provinsi Jawa Barat

B. Instansi/Unit Kerja:

Dinas Komunikasi dan Informatika Provinsi Jawa Barat

C. 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

D. Nama /Jenis Layanan Publik:
   a. Layanan wifi area publik
   b. Ruang layanan internet publik
   c. Layanan informasi website jabarprov.go.id

E. Aset TI yang kritikal:
   1. Informasi :
      -Data pegawai
      -Data keuangan
      -Data Jaringan Komunikasi

-Data Konfigurasi Sistem

2. Aplikasi:
   -E-monev
   -Simpeg/SIAP
   -SIPKD
   -SKP/PEER-Review
   -K-MOB
   -SAPAWARGA
   -SIRAMPAKSEKAR
   -Aplikasi Perijinan
   -Website Jabarprov.go.id
   -Website diskominfo
   -Website Satu Data
   -Website Open Data

3. Server:
   -server e-budgeting
   -server e-Monev
   -server Simpeg
   -server SIPKD
   -server SKP
   -server Perijinan
   -server website jabarprov.go.id
   -server e-SAKIP
   -Server Mail
   -Server Hosting

4. Infrastruktur Jaringan/Network:
   - Telkom dan ICON+

F. DATA CENTER (DC):

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

V ADA, dalam ruangan khusus
 ADA, jadi satu dengan ruang kerja

G. DISASTER RECOVERY CENTER (DRC):

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

V ADA Dikelola Internal V Dikelola vendor : ICON+ dan telkom

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

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Peraturan Gubernur Jawa Barat No 60 Tahun 2018 tentang Tugas, Fungsi, Rincian

Tugas Unit dan Tata Kerja Dinas Komunikasi dan Informatika
2. Rencana Strategis Dinas Komunikasi dan Informatika Tahun 2018 sd tahun 2023
3. Road Map Bidang Persandian Keamanan Informasi Dinas Komunikasi dan Informatika JABAR 2020 sd 2030
4. K01/SMKI Kebijakan Keamanan Informasi Diskominfo
5. K02/SMKI Kebijakan Manajemen Risiko Teknologi Informasi
6. K03/SMKI Kebijakan Ruang Lingkup Sertifikasi & SOA
7. K04/SMKI Kebijakan Kelangsungan Layanan Data Center dan
8. K05/SMKI Kebijakan Peran dan Tanggung Jawab Keamanan Informasi
9. K06/SMKI Kebijakan Standar Kompetensi SMKI
10. PR-01/SMKI Prosedur Pengendalian Dokumen
11. PR-02/SMKI Prosedur Pengendalian Rekaman
12. PR-03/SMKI Prosedur Audit Internal
13. PR-04/SMKI Prosedur Komunikasi Internal dan Eksternal
14. PR-05/SMKI Prosedur Manajemen Review
15. PR-06/SMKI Prosedur Tindakan Perbaikan dan Improvement
16. PR-07/SMKI Prosedur Monitoring dan Evaluasi Vendor
17. PR-08/SMKI Prosedur Pengelolaan dan Penghancuran Removable Media
18. PR-09/SMKI Prosedur Penanganan Pelabelan dan Pertukaran Informasi (termasuk disposal)
19. PR-10/SMKI Prosedur Pengendalian Perubahan TI
20. PR-11/SMKI Prosedur Pengelolaan Insiden Keamanan Informasi
21. PR-12/SMKI Prosedur Instalasi dan Kepatuhan Lisensi Software
22. SOP-01/eGov SOP Backup dan Restore
23. SOP-02/eGov SOP Penempatan (Co-location) Server
24. SOP-03/eGov SOP Pemberian Hak Akses Pengunjung Data Center
25. SOP-04/eGov SOP Hosting Aplikasi dan Web
26. SOP-05/eGov SOP Monitoring & Pemeliharaan Data Center
27. SOP-06/eGov SOP Pengunggahan Konten Release
28. SOP-07/eGov SOP Penerbitan Sub Domain
29. SOP-08/eGov SOP Pemeriksaan Rutin Suhu Ruangan Server
30. SOP-09/eGov SOP Raised Floor Ruang Server, NOC dan Ruang Telco
31. SOP-10/eGov SOP Pemeriksaan Kabel Perangkat Data Center dan Jaringan Komunikasi
32. SOP-11/eGov SOP Penanganan Permasalahan Jaringan Komputer
33. SOP-12/eGov SOP Layanan Video Conference
34. SOP-13/eGov SOP Monitoring dan Pemeliharaan CCTV
35. SOP-14/eGov SOP Pemeriksaan Jaringan VPN
36. SOP-15/eGov SOP Alarm Fire
37. SOP-16/eGov SOP Pengelolaan Insiden Keamanan Informasi Jabarprov-CSIRT
38. SK Pengelola SOC dan SK Admin.

Bukti-bukti (rekaman/arsip) penerapan SMKI:

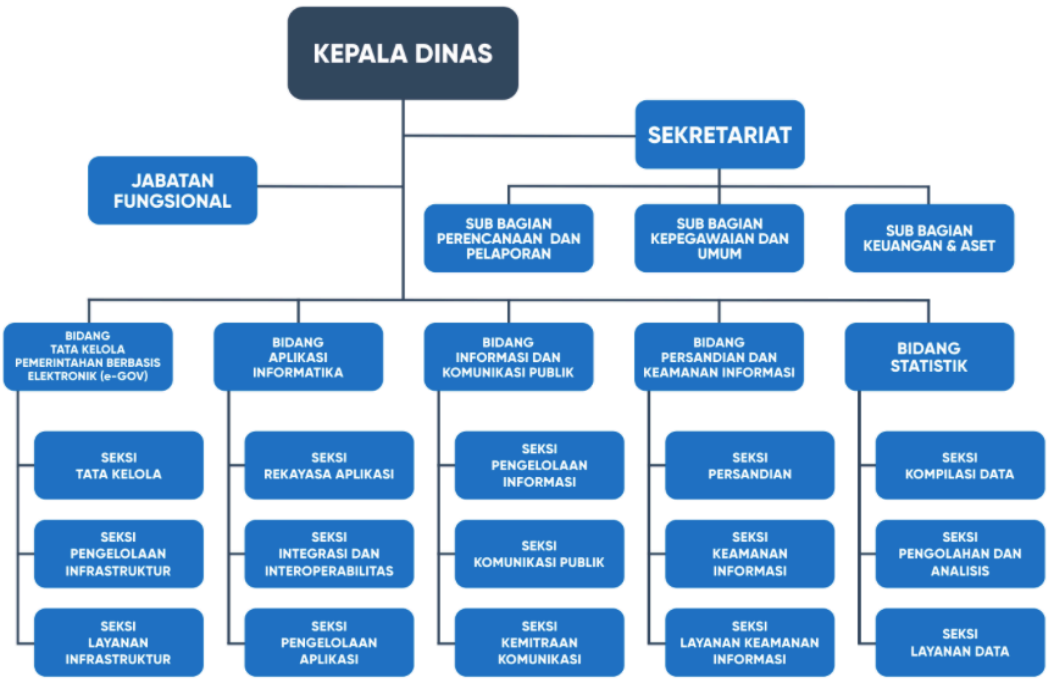
a. Rekaman video Edukasi Pencegahan dan Penaggulangan Kebakaran
b. Rekaman video Latihan Evakuasi Bencana
c. Daftar Induk Dokumen
d. Dokumentasi Jaringan
e. Daftar aset
f. Risk Register
g. Laporan pendampingan Persiapan ISO27001 (Sucofindo)
h. Standard Kompetensi Jabatan
i. Risalah Rapat Tinjauan Manajemen (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 82 personil PNS, dan sekitar 76 personil outsourcing. Sedangkan jumlah pegawai di Bidang Persandian dan Keamanan Informasi sebanyak 9 personil PNS.

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. Sedangkan dalam asesmen indeks KAMI pada tahun 2019 ini, ruang lingkup yang digunakan adalah Aplikasi dan Infrastruktur. Berdasarkan verifikasi terhadap Hasil Self Assessment isian file indeks KAMI diperoleh hasil sebagai berikut :

Total Score Sebelum Verifikasi: 512 (ref. file Indeks KAMI sebelum Verifikasi)

Indeks KAMI (Keamanan Informasi)

Responden:
Dinas Komunikasi dan Informatika Provinsi Jawa Barat

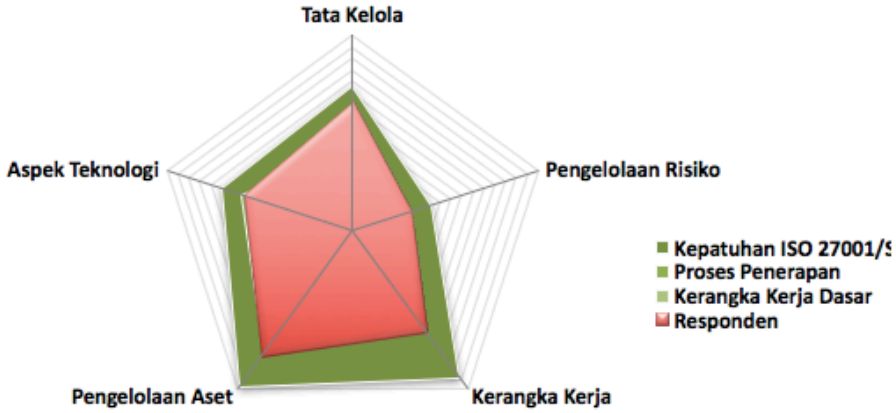
Jl. Taman Sari No 55 Bandung 40132

(022) 2502898
Bid.pkami@jabarprov.go.id
27/12/2018

Hasil Evaluasi Akhir: Cukup

Tingkat Kelengkapan Penerapan Standar ISO27001 512

Skor Kategori SE	: 32	Kategori SE	Tinggi
Tata Kelola	: 112	Tk Kematangan	III+
Pengelolaan Risiko	: 54	Tk Kematangan	III
Kerangka Kerja Keamanan Inform	: 111	Tk Kematangan	II
Pengelolaan Aset	: 136	Tk Kematangan	III
Teknologi dan Keamanan Informas	: 99	Tk Kematangan	II+



Total Score Setelah Verifikasi: 571 (ref. file Indeks KAMI pasca Verifikasi)

Indeks KAMI (Keamanan Informasi)

Responden:
Dinas Komunikasi dan Informatika Provinsi Jawa Barat

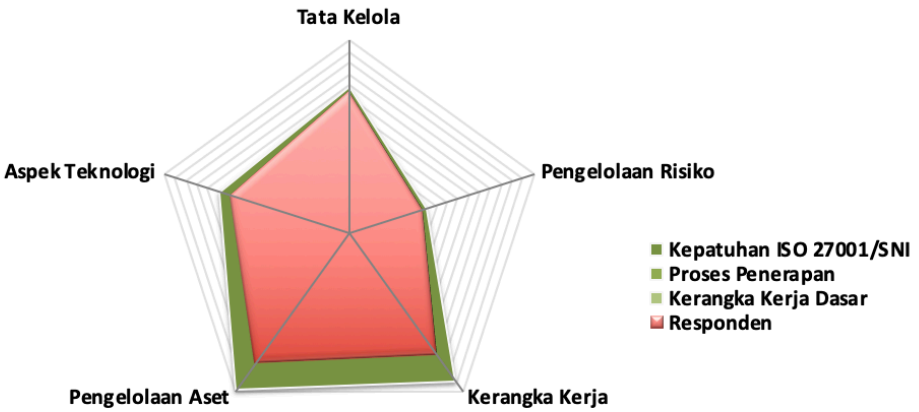
Jl. Taman Sari No 55 Bandung 40132

(022) 2502898
Bid.pkami@jabarprov.go.id
10/12/2018

Hasil Evaluasi Akhir: Cukup

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori 571

Skor Kategori SE	: 35	Kategori SE	Strategis
Tata Kelola	: 125	Tk Kematangan:	III+
Pengelolaan Risiko	: 66	Tk Kematangan:	IV+
Kerangka Kerja Keamanan Informasi	: 130	Tk Kematangan:	II+
Pengelolaan Aset	: 140	Tk Kematangan:	III
Teknologi dan Keamanan Informasi	: 110	Tk Kematangan:	III+



II.ASPEK TATA KELOLA:

1. Kekuatan dan Kematangan

a. Sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab pimpinan diantaranya sudah adanya penetapan kebijakan keamanan informasi. Salah satu hal ini adalah dengan dibuktikan terkait program keamanan informasi dalam ITSP atau inisiatif-inisiatif program terkait.
b. Sudah menetapkan fungsi secara spesifik mengenai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memasikan kepatuhannya.
c. Pejabat/petugas pelaksana pengamanan informasi sudah ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang sudah dituangkan ke dalam analisis jabatan.
d. Alokasi sumber daya baik sumber daya manusia ataupun dalam bentuk anggaran terkait pelaksanaan program keamanan informasi.
e. Peran fungsi pelaksana pengamanan informasi sudah dipetakan pada kebutuhan program keamanan informasi, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan dan dibuktikan dengan surat keterangan pengelola admin aplikasi, pengelola SOC.
f. Sudah mendefinisikan persyaratan/standar kompetensi dan keahlian yang dibuktikan dengan analisis jabatan dan peta jabatan yang sudah di definisikan dari pejabat eselon, fungsional maupun staf.
g. Sudah merencanakan dan menerapkan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi baik untuk internal pegawai atau OPD dan Kabupaten Kota di Pemerintah Provinsi Jawa Barat.
h. Seluruh persyaratan keamanan informasi yang terdapat dalam standard yang berlaku sudah terintegrasi kedalam proses kerja yang ada dan dibuktikan dengan aplikasi *service desk* dimana aplikasi tersebut menerima layanan baik itu gangguan aplikasi atau jaringan internet, hosting aplikasi, permintaan pentest yang sudah terintegrasi dengan muncul notifikasi pada email pegawai diskominfo.
i. Sudah mengidentifikasikan data pribadi yang dikelola oleh kepegawaian yang didalamnya terdapat Nama, NIP, jabatan, data keluarga dll.
j. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi sudah mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal sudah dilakukan dengan melakukan nota dinas terkait pelaksanaan audit internal terhadap respon dari hasil sertifikasi ISO 27001:2013.
k. Koordinasi antara fungsi pengelola keamanan informasi dengan satker terkait dan pihak eksternal dalam menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak yang dibuktikan dengan aplikasi service desk dan berkoordinasi dengan BSSN.
l. Sudah menetapkan tanggung jawab untuk merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat.
m. Fungsi pengelola keamanan informasi sudah melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi dengan menggunakan aplikasi e monev dan peer-review yang berisi mengenai laporan capaian kegiatan dan kinerja individu.
n. Setiap permasalahan keamanan informasi yang terjadi di Diskominfo Jabar sudah menjadi bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang dibuktikan dengan aplikasi e-moev dan peer-review.
o. Sudah menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi dengan melakukan penilaian menggunakan indeks KAMI yang dijadikan IKU pada tahun 2019.
p. Metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi

sudah didefinisikan melalui casescading yang di dalamnya terdapat output kegiatan, target kegiatan, eskalasi pelaporan ketika terdapat permasalahan.

q. Sudah mendefinisikan dan menerapkan program penilaian kinerja terkait penerapan proses kaminfo bagi individu (pejabat & petugas) pelaksananya sebagai bagian dari proses evaluasi tingkat pemahaman individu tersebut terhadap pengelolaan keamanan informasi di organisasi dengan menggunakan K-mob dan peer-review.
r. Target dan sasaran pengelolaan keamanan informasi, mengevaluasi pencapaiannya secara rutin, menerapkan perbaikan untuk mencapai sasaran yang ada dan pelaporan status dengan aplikasi e-monev yang didalamnya terdapat progress report untuk mengevaluasi capaian program, permasalahan yang ada serta solusi dari permasalahan tersebut yang dilakukan per bulan dalam bentuk capaian kinerja.
s. Sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan daftar induk dokumen di kebijakan SMKI yang berbentuk list peraturan yang selama ini diacu dan diimplementasikan yang salah satunya penerapan indeks kami pada Permenkominfo No 4 Tahun 2016.

2. Kelemahan/Kekurangan

a. Semua pelaksana pengamanan informasi di Diskominfo Jabar sudah memiliki kompetensi dan keahlian yang memadai sesuai dengan standar yang dibuktikan dengan anjab (analisis jabatan). Namun belum ada data rekapitulasi keseluruhan pemenuhan kompetensi teknis bagi pelaksana keamanan informasi terhadap persyaratan kompetensi teknis yang diuraikan di anjab.
b. 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.

II.ASPEK RISIKO:

1. Kekuatan dan Kematangan

a. Sudah memiliki program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan sudah ditentukan penanggung jawab manajemen risiko dalam eskalasi pelaporan sampai dengan tingkat pimpinan
b. Kerangka kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dalam dokumen metodologi manajemen risiko sehingga dapat digunakan secara resmi.
c. Kerangka kerja pengelolaan risiko ini sudah mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfo Jabar.
d. Ambang batas tingkat risiko yang dapat diterima sudah ditetapkan (resiko rendah) pada kerangka kerja manajemen risiko keamanan informasi
e. Sudah terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut yang ditunjukan di dalam risk register.
f. Pada proses analisa risiko sudah ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama termasuk ancaman dan kelemahan yang timbul terkait dengan aset informasi.
g. Sudah melaksanakan analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi untuk mengidentifikasi langkah mitigasi.
h. Langkah-langkah mitigasi dan penanggulangan risiko yang ada sudah disusun secara sistematis dan memadai.
i. Sudah diterapkan proses evaluasi melalui proses yang objektif/terukur dengan melaksanakan management review termasuk pengkajian ulang terkait langkah mitigasi untuk memastikan akurasi dan validitasnya dengan melakukan update mitigasi.

2. Kelemahan atau Kekurangan

a. Belum melakukan review terhadap kerangka kerja pengelolaan risiko termasuk pengkajian secara berkala untuk memastikan ataupun meningkatkan efektifitasnya.
b. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian objektif kinerja

efektifitas pengamanan yang dapat ditunjukan dengan pemenuhan *Risk treatment Plan* menjadi bagian dari penilaian terhadap karyawan atau bagian.

IV KERANGKA KERJA:

1. Kekuatan dan Kematangan

a. Kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan didokumentasikan dengan jelas, termasuk peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya dan sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
b. Mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya sudah diatur dalam SOP pengendalian dokumen.
c. proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga yang terdapat pada dokumen prosedur komunikasi internal dan eksternal.
d. Kebijakan keamanan informasi sudah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang telah ditetapkan.
e. Sudah adanya proses untuk mengidentifikasi sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang dibuktikan dengan dokumen prosedur pengelolaan insiden keamanan informasi.
f. Aspek keamanan informasi sudah diidentifikasi untuk beberapa aktivitas proyek selama proses manajemen proyek yang dilakukan sudah dilaksanakan yang dibuktikan dengan pembahasan aspek keamanan pada pemilihan firewall, melakukan pentest pada setiap aplikasi yang akan di rilis.
g. Proses pengembangan sistem yang aman (Secure SDLC) sudah menerapkan prinsip atau metode sesuai standar platform teknologi yang digunakan yang terdapat pada kebijakan SMKI pada poin X terkait pengadaan, pengembangan sistem.
h. Strategi penerapan keamanan informasi sudah direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi namun belum dievaluasi.
i. Sudah terdapat proses dalam melakukan analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
j. Sudah melaksanakan audit internal untuk mengevaluasi langkah pembenahan yag sudah dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan.
k. Sudah 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.
l. Rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) belum seluruhnya direalisasikan secara konsisten.

2. Kelemahan atau Kekurangan

a. Belum adanya keseragaman terkait kontak dengan pihak ketiga pada setiap bidang yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI,tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
b. Belum ada dokumen yang berisi tentang laporan monitoring patch release dan prosedur operasional untuk mengelola implementasi instalasi patch.
c. Konsekwensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga. Contohnya pada fungsi penerimaan tamu tidak berjalan sesuai aturan dan belum dimasukan ke dalam risk register sebagai salah satu risiko.
d. Belum ada proses yang baku untuk mengevaluasi risiko terkait rencana pembelian

(atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul dengan menggunakan cost benefit analysis terkait rencana implementasi sistem baru.

e. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfo belum memiliki proses ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya.
f. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) sudah didefinisikan pada kebijakan SMKI bagian XIII terkait rencana kelangsungan layanan TI tetapi sampai dengan saat ini belum terdapat dokumen BCP.
g. Belum adanya perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dan uji coba pemulihan bencana terhadap layanan TIK yang dapat dibuktikan dengan kebijakan keberlangsungan usaha pada data center dan data recovery center termasuk dokumen uji coba dan dokumen evaluasi hasil uji coba/simulasi, dan perbaikan sesuai dengan hasil evaluasi.
h. Hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah didokumentasi pada saat pelaksanaan management review, hanya saja pelaksanaan manajemen review belum dilaksanakan.
i. Dari *risk register* yang diperbaharui tahun 2018 ke 2019, tidak ada hasil penilaian risiko yang tinggi. Namun terdapat risk register bidang Aptika pada tahun 2018 yang memiliki beberapa penilaian hasil risiko yang tinggi yang belum dijadikan strategi atau bagian dari rencana kerja untuk menurunkan risiko tersebut.

V PENGELOLAAN ASET

1. kekuatan dan Kematangan

a. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi sudah didokumentasikan secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
b. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku sudah didefinisikan.
c. Sudah adanya definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Diskominfo Jabar.
d. Sudah ada tata tertib penggunaan komputer, email, internet dan intranet.
e. Telah ada proses mengenai pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya.
f. Beberapa sistem sudah ditetapkan persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
g. Telah ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data namun belum dilaksanakan secara sistematis.
h. Sudah ada ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
i. Sudah tersedianya proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
j. Telah ada prosedur mengenai proses back-up namun belum diatur mekanisme uji coba pengembalian data (restore).
k. Sudah berjalannya proses pengecekan latar belakang SDM.
l. Sudah dilakukan mekanisme terkait pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib namun belum tertuang dalam dokumentasi.
m. Telah ada prosedur penghancuran data/aset yang sudah tidak diperlukan.
n. Pengamanan fasilitas fisik (lokasi kerja) sudah diterapkan sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
o. Sudah formalnya proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.

p. Infrastruktur komputasi telah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya dan telah terlindungi dari gangguan pasokan listrik atau dampak dari petir.
q. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sudah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai.
r. Sudah adanya proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
s. Proses pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga sudah ada namun aturan baku terhadap hal ini belum ditetapkan.
t. Sudah ada proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan yang ditunjunkan dengan prosedur pemberian hak akses pengunjung data center

2. <u>Kelemahan atau Kekurangan</u>

a. Belum tersedianya proses pengelolaan konfigurasi yang diterapkan namun belum terdokumentasi secara konsisten.
b. Belum adanya tata tertib pengamanan dan penggunaan aset terkait HAKI dan instalasi piranti lunak di aset TI milik instansi.
c. Ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya sudah diterapkan namun belum terdokumentasi.
d. Ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya sudah diidentifikasi namun belum terdokumentasi secara jelas.
e. Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya belum didokumentasikan.
f. Belum ada daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya yang sudah tercatat.
g. Sudah didefinisikan pengamanan 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), hanya saja peraturan dan tata tertibnya belum disahkan.
h. Belum ditetapkannya peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor).
i. Belum ditetapkannya proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).

<u>VI TEKNOLOGI</u>

1. <u>kekuatan dan Kematangan</u>

a. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan
b. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll).
c. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sebagian sudah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
d. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
e. Setiap perubahan dalam sistem informasi sebagian sudah direkam pada suatu log

pada sistem.
f. Upaya akses oleh yang tidak berhak sebagian sudah terekam di dalam log.
g. Sudah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
h. Pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya sudah diterapkan.
i. Akses yang digunakan untuk mengelola sistem (administrasi sistem) sudah menggunakan bentuk pengamanan khusus yang berlapis.
j. Sistem dan aplikasi yang digunakan sebagian sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses.
k. Pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi sudah diterapkan namun belum dievaluasi berkala.
l. Sudah ada proses untuk menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan namun belum dikaji secara periodik.
m. Beberapa rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis sudah tersimpan.
n. Sudah ada proses pelaporan penyerangan virus/malware yang gagal/sukses yang ditindaklanjuti dan diselesaikan.
o. Keseluruhan jaringan, sistem dan aplikasi sebagian sudah tersinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
p. Lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun telah diterapkan dan sudah melibatkan pihak independent untuk mengkaji kehandalan keamanan informasi baik dengan komunitas dan BSSN.

2. Kelemahan atau Kekurangan

a. Analisa kepatuhan penerapan konfigurasi standar yang ada belum dianalisa secara berkala.
b. Jaringan, sistem dan aplikasi yang digunakan secara rutin belum dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
c. Belum ada sistem dan aplikasi yang sudah secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
d. Belum semua desktop dan server telah dilindungi dari penyerangan virus (*malware*).
e. Belum semua sistem operasi untuk setiap perangkat desktop dan server sudah dimutakhirkan dengan versi terkini.
f. Aplikasi yang ada belum memiliki dokumentasi mengenai spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba. (masih dalam bentuk RAPERGUB).

VII. REKOMENDASI:

1. Tata Kelola

a. Pembuatan rekapitulasi keseluruhan pemenuhan kompetensi teknis bagi pelaksana keamanan informasi terhadap persyaratan kompetensi teknis yang diuraikan di anjab.
b. 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.

2. Risiko

a. Melakukan review terhadap kerangka kerja pengelolaan risiko termasuk pengkajian secara berkala untuk memastikan ataupun meningkatkan efektifitasnya;

b. Menjadikan Pengelolaan risiko sebagai bagian dari kriteria proses penilaian objektif kinerja efektifitas pengamanan yang dapat ditunjukan dengan pemenuhan Risk treatment plan menjadi bagian dari penilaian terhadap karyawan atau bagian.

3. <u>Kerangka Kerja</u>

a. Membuat keseragaman terkait kontak dengan pihak ketiga pada setiap bidang yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI,tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
b. Membuat dokumen yang berisi tentang laporan monitoring patch release dan prosedur operasional untuk mengelola implementasi instalasi patch.
c. Mendefinisikan konsekwensi dari pelanggaran kebijakan keamanan informasi, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.
d. Membuat proses yang baku untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul dengan menggunakan cost benefit analysis terkait rencana implementasi sistem baru.
e. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfo belum memiliki proses ini, termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya.
f. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) sudah didefinisikan pada kebijakan SMKI bagian XIII terkait rencana kelangsungan layanan TI tetapi sampai dengan saat ini belum terdapat dokumen BCP.
g. Melaksanakan perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dan uji coba pemulihan bencana terhadap layanan TIK yang dapat dibuktikan dengan kebijakan keberlangsungan usaha pada data center dan data recovery center termasuk dokumen uji coba dan dokumen evaluasi hasil uji coba/simulasi, dan perbaikan sesuai dengan hasil evaluasi.
h. Melaksanakan manajemen review terhadap hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*)
i. Memperbaharui risk register dari setiap bidang (bukan hanya risk register yang berkaitan dengan data center) untuk dijadikan strategi dan rencana kerja untuk menurunkan risiko.

4. <u>Pengelolaan Aset</u>

a. Membuat dokumentasi proses pengelolaan konfigurasi yang diterapkan dan implementasinya harus lebih konsisten.
b. Membuat tata tertib pengamanan dan penggunaan aset terkait HAKI dan instalasi piranti lunak di aset TI milik instansi.
c. Membuat dokumentasi terkait pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada.
d. Membuat dokumentasi mengenai ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
e. Membuat dokumentasi terkait daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya.
f. Membuat daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya yang sudah tercatat.

5. <u>Teknologi</u>

a. Membuat analisa kepatuhan penerapan konfigurasi standar secara berkala.
b. Membuat otomatisasi terhadap sistem dan aplikasi pada saat menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
c. Melindungi semua desktop dan server agar terhindar dari penyerangan virus (malware).
d. Memutakhirkan sistem operasi untuk setiap perangkat desktop dan server dengan

versi terkini.

e. Membuat dokumentasi mengenai spesifikasi dan fungsi keamanan pada saat pengembangan aplikasi yang diverifikasi/validasi pada saat proses pengembangan dan uji coba. (masih dalam bentuk RAPERGUB).

Jakarta, 29 November 2019	
Narasumber Instansi/Perusahaan:	Assessor Indeks KAMI:
Dinas Komunikasi dan Informatika Provinsi Jawa Barat	1. Fajarudin Setio Utomo, S.ST., M.AP.
1. Hermin Wijaya, ST, M.Kom	2. Johanes Widhi Candra, S.Tr.MP
2. Rizki Hustiniasari, ST	3. Herison Metinaro, M.M.
3. M. Mulyadi	
4. Dandi M Iqbal	
5. Hannif Izzatul I	