



2020

# LAPORAN

HASIL PENILAIAN  
TINGKAT MATURITAS PENANGANAN INSIDEN (TMPI)  
DINAS KOMUNIKASI DAN INFORMATIKA  
PEMERINTAH PROVINSI JAWA BARAT



# DAFTAR ISI

DAFTAR ISI .....	2
PENDAHULUAN .....	3
I. Tujuan Kegiatan.....	3
II. Ruang Lingkup Kegiatan.....	3
III. Metodologi Kegiatan.....	3
IV. Pelaksanaan Kegiatan .....	4
HASIL KEGIATAN .....	5
I. Informasi Stakeholder.....	5
II. Deskripsi Ruang Lingkup Penilaian .....	5
III. Hasil Penilaian TMPI .....	8
IV. Kekuatan/Kematangan.....	9
V. Kelemahan/Kekurangan .....	11
VI. Rekomendasi .....	12
VII. Hasil Penilaian CSM.....	14
VIII. Kekuatan/Kematangan.....	15
IX. Kelemahan/Kekurangan .....	17
X. Rekomendasi .....	18
PENUTUP.....	19



# PENDAHULUAN

## I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas *stakeholder* dalam penanganan insiden siber (TMPI) dan menilai tingkat maturitas keamanan siber (CSM) di lingkungan Pemerintah Provinsi Jawa Barat. Dengan adanya tingkat maturitas ini diharapkan dapat memberikan gambaran mengenai apa yang harus menjadi tindak lanjut baik oleh *stakeholder* maupun Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan kemampuan tingkat maturitas keamanan siber.

## II. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek penanganan insiden meliputi :

1. Fase 1 : Persiapan
2. Fase 2 : Respon
3. Fase 3 : Tindak Lanjut

Dan untuk mengukur CSM / tingkat maturitas keamanan siber, aspek pemetaannya meliputi :

1. Aspek Tata Kelola
2. Aspek Identifikasi
3. Aspek Proteksi
4. Aspek Deteksi
5. Aspek Respon

## III. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen pemetaan TMPI & CSM, wawancara/diskusi, dan melihat ketersediaan dokumen penanganan insiden siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas tiap fase penanganan insiden.

Penentuan Level Kematangan diukur berdasarkan Indeks Kematangan yang didapat. Konversi Indeks Kematangan menjadi Level Kematangan menggunakan formula:

$$\text{Level Kematangan (\%)} = \frac{\text{Indeks Kematangan}}{5} \times 100\%$$



Nilai Level Kematangan dikategorikan menjadi :

- Level 1 (*Foundation*) : Rentang Level Kematangan 0 % s.d. 20 %
- Level 2 (*Emerging*) : Rentang Level Kematangan 21 % s.d. 40 %
- Level 3 (*Establishing*) : Rentang Level Kematangan 41 % s.d. 60 %
- Level 4 (*Dynamic*) : Rentang Level Kematangan 61 % s.d. 80 %
- Level 5 (*Optimise*) : Rentang Level Kematangan 81 % s.d. 100 %

#### IV. Pelaksanaan Kegiatan

1. Pengisian Instrumen Pemetaan TMPI dan CSM oleh internal *stakeholder* (*self assessment*)

Pengisian Instrumen oleh internal *stakeholder* dilakukan pada tanggal 26 Oktober 2020.

2. Validasi Pemetaan TMPI dan CSM

Validasi Pemetaan TMPI dilaksanakan untuk pengecekan hasil *self assessment* isian instrumen. Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen pendukung penanganan insiden siber. Kegiatan validasi dilaksanakan pada 26 s.d 27 Oktober 2020.



# HASIL KEGIATAN

## I. Informasi Stakeholder

Nama Instansi : Pemerintah Provinsi Jawa Barat  
Alamat : Jl. Tamansari No.55, Lb. Siliwangi, Kecamatan Coblong, Kota Bandung, Jawa Barat  
Email : bid.pkami@jabarprov.go.id  
Narasumber Instansi :  
1. Tiomaida Seviana Hh, S.H., M.A.P.  
Kepala Bidang Persandian Dan Keamanan Informasi;  
2. Hermin Wijaya, St., M.Kom.  
Kepala Seksi Keamanan Informasi  
3. Asep Denny Surbakti, St., Mt.  
Kepala Seksi Layanan Keamanan Informasi  
4. Mumul Mulyadi,  
Staff  
5. Waseso Wibisono,  
Staff

## II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :  
 Organisasi Keseluruhan     Regional, Kanwil, Cabang     Unit Kerja     Lainnya
2. Instansi/Unit Kerja\* : Dinas Komunikasi dan Informatika Provinsi Jawa Barat
3. Lokasi Aset : a. Kantor Dinas Komunikasi dan Informatika, Provinsi Jawa Barat
4. 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  
 TIDAK ADA

5. Status Ketersediaan Dokumen Penanganan Insiden Siber



No	Nama Dokumen	Ada	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	<b>Kebijakan, Sasaran, Petunjuk, Standar</b>			
1	Kebijakan SMKI Dinas Kominfo Provinsi Jawa Barat K01/SMKI	✓		R.2018
2	Framework Manajemen Risiko Keamanan Informasi	✓		R.2018
3	Kebijakan Ruang Lingkup Sertifikasi & SOA	✓		R.2018
4	Kebijakan Kelangsungan Layanan Data Center	✓		R.2018
5	Kebijakan Peran dan Tanggung Jawab Keamanan Informasi R0.0	✓		R.2018
6	Kebijakan Standar Kompetensi SMKI	✓		R.2018
7	Kebijakan Penggunaan Perangkat TI Milik Pihak Eksternal	✓		R.2019
8	Kebijakan Perlindungan Data Pribadi	✓		R.2019
9	ISO 27001	✓		R.2020
	<b>Prosedur- Prosedur</b>			
1	Sop Pemeriksaan Jaringan Vpn	✓		R.2018
2	Sop Backup Dan Restore	✓		R.2018
3	Sop E-Gov	✓		R.2018
4	Sop Pengendalian Prosedur Dokumen.	✓		R.2018
5	Sop Audit Internal	✓		R.2018
6	Sop Komunikasi Internal Dan Eksternal	✓		R.2018
7	Sop Manajemen Review	✓		R.2018
8	Sop Tindakan Perbaikan Dan Infrovement	✓		R.2018
9	Sop Monitoring Dan Evaluasi Vendor	✓		R.2018
10	Sop Penanganan Insiden Keamanan Informasi	✓		R.2018
11	Sop Instalasi Dan Kepatuhan Lisensi Sofware	✓		R.2018

Tabel 1. Checklist Ketersediaan Dokumen

Dokumen yang diperiksa:

1. Data Daftar Aset Diskominfo Provinsi Jawa Barat;
2. Data Risk Register Diskominfo Provinsi Jawa Barat;
3. Kebijakan SMKI Dinas Kominfo
4. Framework Manajemen Risiko Keamanan Informasi
5. Kebijakan Ruang Lingkup Sertifikasi & SOA;
6. Kebijakan Kelangsungan Layanan Data Center;
7. Kebijakan Peran dan Tanggung Jawab Keamanan Informasi;



8. Kebijakan Standar Kompetensi SMKI;
9. Kebijakan Penggunaan Perangkat TI Milik Pihak Eksternal;
10. SOP bidang Sandi Keamanan Informasi;
11. SOP Bidang E-Government;
12. Laporan Penanganan Insiden Siber;
13. Kebijakan Perlindungan Data Pribadi;
14. Laporan Kegiatan Simulasi Penanganan Insiden Siber;
15. SK Gubernur tentang Tim Tanggap Insiden Siber Jabarprov-CSIRT;
16. Dokumen Sumber Daya Penyelenggaraan CSIRT;
17. Dokumentasi pencatatan log Server;
18. Daftar Point of Contact (PoC) Konstituen Jabarprov-CSIRT;
19. TMPI Provinsi Jawa Barat 2019.

### III. Hasil Penilaian TMPI

Berdasarkan hasil penilaian TMPI, diperoleh hasil sebagai berikut:

**Total Score Indeks Kematangan : 3,54**

Sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

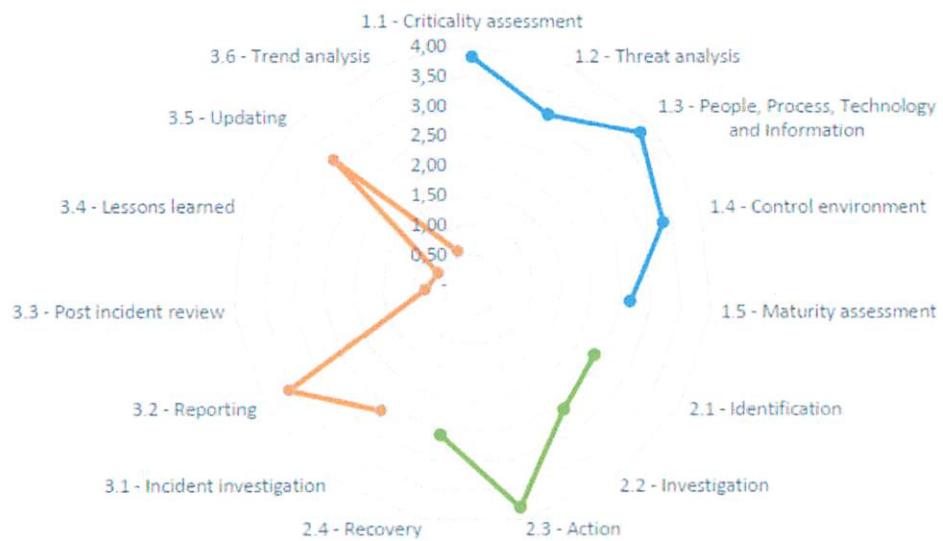
#### Level Kematangan Tingkat 4

Rekapitulasi Hasil Penilaian

Fase	Langkah	TK 1	TK 2	TK 3	TK 4	TK 5	Rata2	Rata2 per Fase
1	1 Penilaian kritikalitas	5,00	3,00	3,00	3,00	5,00	3,80	4,25
1	2 Analisis ancaman	5,00	5,00	3,00	3,00	0,60	3,32	
1	3 Orang, proses, teknologi, dan informasi	5,00	5,00	4,67	4,20	4,33	4,64	
1	4 Lingkungan kontrol	5,00	5,00	4,50	4,00	5,00	4,70	
1	5 Penilaian kematangan	5,00	5,00	5,00	5,00	4,00	4,80	
2	1 Identifikasi	5,00	5,00	5,00	3,00	-	3,60	3,26
2	2 Penyelidikan	1,00	4,00	4,00	3,00	1,00	2,60	
2	3 Aksi	5,00	5,00	5,00	4,20	0,50	3,94	
2	4 Pemulihan	5,00	3,40	2,67	3,00	0,50	2,91	
3	1 Identifikasi	5,00	5,00	3,00	3,00	1,00	3,40	2,33
3	2 Pelaporan	5,00	5,00	5,00	2,33	3,00	4,07	
3	3 Review pasca insiden	3,00	-	1,67	1,00	0,50	1,23	
3	4 Pembelajaran yg didapat	3,00	3,00	1,00	-	-	1,40	
3	5 Pemperbarui informasi	1,00	2,00	1,50	5,00	3,00	2,50	
3	6 Analisis trend	3,00	1,00	1,00	1,00	1,00	1,40	3,28
							Rata-rata	

Perhitungan Indeks Kematangan

Fase	Kontribusi Indeks					Jumlah
	TK 1	TK 2	TK 3	TK 4	TK 5	
Bobot per Tingkat	30%	25%	20%	15%	10%	100%
Fase Persiapan	1,50	1,15	0,81	0,58	0,38	4,41
Fase Aksi	1,20	1,09	0,83	0,50	0,05	3,67
Fase Tindak Lanjut	1,00	0,67	0,44	0,31	0,14	2,56
					Indeks Kematangan	3,54



## IV. Kekuatan/Kematangan TMPI

### 1. Fase Persiapan

- a. Pendaftaran aset dan penanggungjawab telah disusun secara sistematis;
- b. Aset yang didata telah disusun berdasarkan klasifikasi kritikalitas berbasis analisis resiko operasional
- c. Organisasi telah melakukan analisis ancaman keamanan siber, termasuk potensi kerentanan dan mendokumentasikannya
- d. Penyusunan skenario simulasi penanganan insiden siber telah dilakukan;
- e. Sumber Daya Manusia (SDM) lebih dari 1 (satu) dan telah memperoleh pelatihan di bidang keamanan siber;
- f. SDM Jabarprov-CSIRT memiliki kemampuan penanganan insiden siber;
- g. Tim Tanggap Insiden Siber telah dibentuk yang dituangkan dalam SK Jabarprov-CSIRT;
- h. Tim respon respon insiden siber di Diskominfo memiliki kemampuan mendeteksi insiden tingkat lanjut (misalnya pencurian data, ilegal akses, penyusupan, aktivitas ilegal, dll)
- i. Tim respon insiden siber di organisasi memiliki peralatan sumber daya analisis insiden
- j. Kontak pihak-pihak terkait dalam penanganan insiden siber telah dimiliki;
- k. Program kegiatan kesadaran keamanan infoirmasi rutin diselenggarakan untuk konstituen;



- l. Tim respon insiden siber di organisasi memiliki berbagai metode pencatatan setiap insiden yang terjadi.
  - m. Tim respon respon insiden siber di organisasi memiliki kemampuan mendeteksi insiden tingkat lanjut (misalnya pencurian data, ilegal akses, penyusupan, aktivitas ilegal, dll)
  - n. JabarProvCsirt Sudah memiliki sertifikasi ISO 27001, sehingga kebijakan dan prosedur SMKI sudah tersedia.
  - o. Peraturan tentang penyelenggaraan keamanan siber telah dimiliki;
  - p. Panduan/petunjuk teknis pengelolaan insiden keamanan informasi telah dimiliki;
  - q. Perangkat dan tools monitoring dan respon insiden siber telah dimiliki;
  - r. Perangkat dan sistem kontrol pemantauan keamanan siber telah diterapkan;
  - s. Kontrol keamanan telah diterapkan pada perangkat monitoring & firewall;
  - t. pencatatan/perekaman log telah dikelola dengan baik oleh SIEM.
2. Fase Respon
- a. Sumber informasi insiden siber telah mencakup informan dari dalam dan luar instansi;
  - b. Identifikasi insiden siber pada kasus insiden yang terkait infrastruktur yang dikelola instansi telah dilakukan;
  - c. Telah memiliki tools monitoring dan analisa insiden berupa Sistem Monitoring Sensor, Firewall, NMS, SIEM, Honeynet.
  - d. Dukungan bantuan penanganan insiden siber berasal dari luar instansi tersedia misalkan komunitas, dll;
  - e. Titik berat penanganan insiden siber berfokus pada keberlangsungan operasional;
  - f. Titik berat keamanan informasi/siber pada perlindungan aset penting instansi;
  - g. Pengamanan data dan sistem TIK diterapkan di ruang SOC dan Disaster Recovery Center (DRC);
  - h. Pertahanan siber telah diterapkan pada firewall, SIEM, Monitoring Sensor;
  - i. Telah dilakukan implementasi DMZ, sistem back up/ HA (high availability) serta back up konfigurasi untuk ketahanan siber.
  - j. Telah dilakukan implementasi DC di jaringan internal dan pengaturan prosedur akses
3. Fase Tindak Lanjut.
- a. JabarprovCSIRT telah melakukan identifikasi dari berbagai kasus insiden yang terjadi;
  - b. JabarprovCSIRT telah membuat laporan insiden untuk setiap insiden siber;



- c. JabarProvCSIRT telah melaporkan laporan insiden sesuai dengan format standar
- d. Data rekapitulasi penanganan insiden siber telah disusun;
- e. Secara rutin dan berkala laporan insiden dilaporkan ke kepala Dinas;
- f. Tim JabarprovCSIRT merekap laporan insiden yang terjadi dalam suatu periode;
- g. Laporan insiden dan review disusun menjadi materi pembelajaran sebagai bahan Sosialisasi.

## V. Kelemahan/Kekurangan TMPI

- 1. Fase Persiapan
  - a. skenario penanganan insiden siber yang ada telah disusun, namun belum disimulasikan secara berkala;
  - b. Belum memiliki Dokumen SLA khusus penanganan insiden;
- 2. Fase Respon
  - a. Belum memiliki tim managemen insiden krisis;
  - b. Analisa Penyelidikan insiden keamanan siber belum sampai pada tahap simulasi lanjutan dan belum sampai mengungkap motif pelaku;
  - c. Analisis keterhubungan terhadap beberapa kasus insiden siber yang pernah terjadi belum dilakukan;
  - d. Tahapan analisa dan akuisisi Forensik masih belum disusun;
  - e. Belum ada kerja sama dengan pihak penegak hukum terkait dengan tindakan kejahatan siber yang memiliki dampak besar.
- 3. Fase Tindak Lanjut
  - a. laporan insiden Belum memuat aspek biaya kerugian dan pemulihan;
  - b. Review Pasca insiden siber belum dilakukan;
  - c. *Lesson Learned* belum membahas sampai dengan level strategic;
  - d. Evaluasi terhadap waktu yang dibutuhkan penanganan insiden siber berdasarkan hasil pengalaman penanganan insiden siber belum diterapkan;
  - e. Simulasi penanganan insiden siber dengan melibatkan pihak Konstituen belum diterapkan;

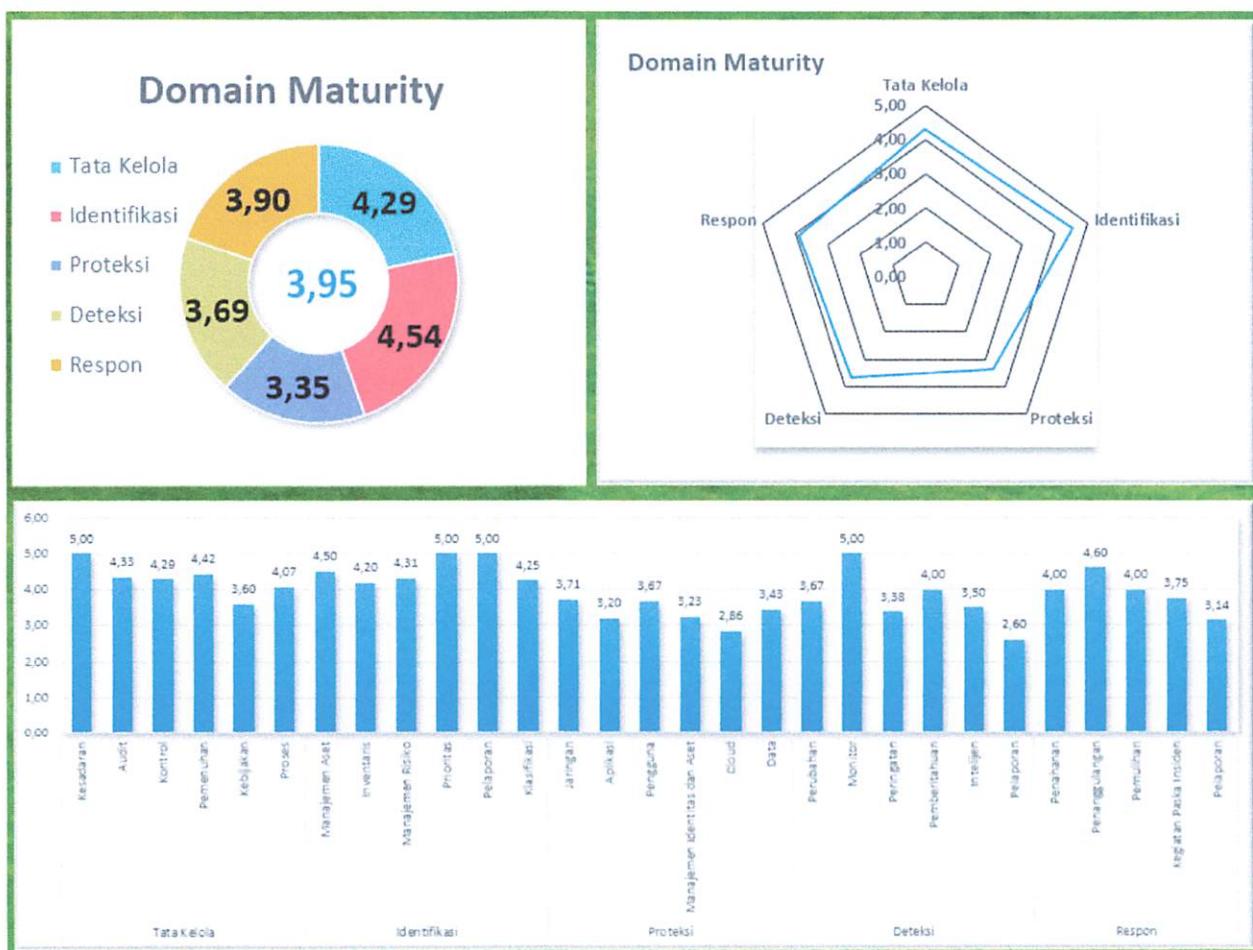
## VI. Rekomendasi TMPI



1. Penyusunan skenario penanganan insiden yang mencakup berbagai macam platform serta mengacu pada potensi risiko insiden atas aset penting dan perubahan ancaman siber baru;
2. Peningkatan kompetensi Sumber Daya Manusia di bidang forensik digital dan analisis malware;
3. Peningkatan perangkat analisis forensik digital;
4. Menyusun layanan SLA Penanganan insiden siber;
5. Penyusunan Analisis insiden siber mencakup informasi yang terungkap, dampak bisnis dan hukum;
6. Penyusunan analisis keterhubungan terhadap beberapa kasus insiden siber yang pernah terjadi;
7. Pemberlakuan mekanisme pembaruan kontrol keamanan berdasarkan hasil pengalaman penanganan insiden siber;
8. Penyusunan analisis Trend insiden siber;
9. Penerapan *Lesson Learned*;
10. Penerapan evaluasi Pasca Insiden siber;
11. Penerapan evaluasi terhadap waktu yang dibutuhkan dalam penanganan insiden siber berdasarkan hasil pengalaman penanganan insiden siber belum diterapkan;
12. Simulasi penanganan insiden siber (Drill test/ cyber security Exercise) dengan melibatkan Konstituen;
13. Penerapan informasi pasca insiden siber digunakan untuk melakukan pembaruan atas skenario penanganan insiden siber, metodologi manajemen insiden, kontrol risiko, *Business Continuity Management* (BCM).

## VII. Hasil Penilaian CSM / Tingkat Maturitas Keamanan Siber

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
4,29		4,54		3,35		3,69		3,90	
Kesadaran	5,00	Manajemen Aset	4,50	Jaringan	3,71	Perubahan	3,67	Penahanan	4,00
Audit	4,33	Inventaris	4,20	Aplikasi	3,20	Monitor	5,00	Penanggulangan	4,60
Kontrol	4,29	Manajemen Risiko	4,31	Pengguna	3,67	Peringatan	3,38	Pemulihan	4,00
Pemenuhan	4,42	Prioritas	5,00	Manajemen Identitas dan Aset	3,23	Pemberitahuan	4,00	Kegiatan Paska Insiden	3,75
Kebijakan	3,60	Pelaporan	5,00	Cloud	2,86	Intelijen	3,50	Pelaporan	3,14
Proses	4,07	Klasifikasi	4,25	Data	3,43	Pelaporan	2,60		



Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

**Total Score Indeks Kematangan : 3,95**

Sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

**Level Kematangan Tingkat 4**

## VIII. Kekuatan/Kematangan CSM

### Tata Kelola

- Organisasi telah memilik kesadaran keamanan informasi secara optimal, yang dapat dilihat berdasarkan kebijakan, sumber daya, dan peningkatan kompetensi karyawan.
- Organisasi telah melakukan audit keamanan informasi secara teknologi artinya adalah kegiatan vulnerability scanning dan risk treatment telah dilakukan secara berkala dan berkelanjutan.



3. Organisasi memiliki control keamanan informasi yang terkelola dan di review secara berkala. Kontrol keamanan informasi berupa latar belakang karyawan, supplier, serta control pada asset yang diimiliki.
4. Organisasi memiliki pemenuhan terhadap perjanjian, undang-undang, dan peraturan yang berlaku
5. Organisasi memiliki kebijakan keamanan informasi yang telah disetujui oleh manajemen
6. Organisasi memiliki kebijakan dan prosedur yang sesuai dengan standar yang diakui.

### Identifikasi

1. Organisasi telah melakukan manajemen asset secara optimal, dengan menerapkan update perencanaan kapasitas dan update patch terhadap semua asset.
2. Organisasi telah melakukan inventaris asset berdasarkan klasifikasi kritikalitas dan informasi
3. Organisasi telah melakukan manajemen resiko berupa pembatasan akses, retensi data sensitive, dan adanya risk register.
4. Organisasi telah menentukan profil keamanan informasi yang mencakup prioritas kerentanan dan rencana mitigasinya
5. Organisasi telah memiliki standar untuk melakukan klasifikasi dara, asset, dan cyber threat

### Proteksi

1. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan firewall, melakukan filtering pada inbound dan outbound network traffic, DNS filtering services
2. Organisasi telah melakukan manajemen terhadap aplikasi yang dimiliki, berupa pembatasan aplikasi yang diinstal, aplikasi masih memiliki update support, dan add-on serta plugin yang digunakan.
3. Organisasi telah menerapkan pembatasan akun pengguna dan perlindungan user dengan menggunakan URL filtering, device control, and application control.
4. Organisasi telah melakukan manajemen identitas dan akses, berupa manajemen password, identifikasi setiap perangkat yang bertransaksi, dan pembayasan akses database.
5. Organisasi telah melakukan perlindungan terhadap cloud yang dimiliki berupa adanya DRC yang letaknya terpisah secara geografis.



6. Organisasi telah menerapkan perlindungan data internal dan melakukan perlindungan data terhadap data konstituen dengan backup data secara fisik maupun non fisik.

#### Deteksi

1. Organisasi telah menerapkan monitoring terhadap aktivitas lalu lintas jaringan, log perangkat, dan akses pengguna.
2. Organisasi telah memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat untuk menangani kejadian prioritas tinggi dan mampu mendeteksi anomali.

#### Respon

1. Organisasi telah memiliki SOP dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Organisasi telah melakukan latihan respon insiden secara rutin dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
3. Tim respon insiden telah memiliki peralatan sumber daya analisis insiden dan kemampuan penanganan insiden.
4. Tim respon insiden dalam menangani insiden dapat dengan cepat mendapat bantuan dan mengakses informasi dari pihak ketiga.

## IX. Kelemahan/Kekurangan CSM

1. Organisasi belum memiliki kebijakan yang mengatur single ID unik dan otentifikasi terpusat untuk semua perangkat jaringan.
2. Organisasi tidak membatasi aplikasi yang diunduh, diinstal, dan dioperasikan oleh *end user*.
3. Organisasi belum memfasilitasi penerapan enkripsi pada perangkat mobile (misal: laptop dan handphone) milik pegawai dan media penyimpanan eksternal.a
4. Organisasi belum memiliki verifikasi On Time Password (OTP) melalui SMS, WhatsApp Messenger, Email, dsb untuk transaksi yang beresiko tinggi.
5. Organisasi belum melakukan evaluasi terhadap efisiensi operasional pengelolaan TI.
6. Terhadap suatu insiden siber yang terjadi, organisasi belum melakukan pencegahan terhadap root cause yang menyebabkan insiden tersebut.



7. Organisasi belum melakukan perhitungan biaya yang dikeluarkan / kerugian finansial yang diakibatkan oleh suatu insiden siber.

## X. Rekomendasi CSM

1. Untuk meningkatkan keamanan data di lingkungan Dinaskominfo Pemprov Jabar maka dapat dilakukan hal-hal sebagai berikut:
  - a. Menerapkan kebijakan yang mengatur single ID unit dan otentikasi terpusat untuk semua perangkat jaringan
  - b. Membatasi aplikasi yang dapat diunduh, diinstal, dan dioperasikan oleh *end user*
  - c. Memfasilitasi penerapan enkripsi pada perangkat mobile (misal: laptop dan handphone) milik pegawai dan media penyimpanan eksternal.
  - d. Menambahkan verifikasi On Time Password (OTP) melalui SMS, WhatsApp Messenger, Email, dsb untuk transaksi yang beresiko tinggi
2. Untuk meningkatkan efektifitas dan efisiensi operasional keamanan informasi di lingkungan Diskominfo Pemprov Jabar, maka dapat dilakukan hal-hal sebagai berikut:
  - a. Melakukan evaluasi terhadap efisiensi operasional pengelolaan TI.
  - b. Mencari tahu *root cause* dari suatu insiden siber yang terjadi, sehingga dapat dilakukan pencegahan yang efektif terhadap berulangnya insiden siber tersebut di masa mendatang.
  - c. Melakukan perhitungan biaya yang dikeluarkan / kerugian finansial yang diakibatkan akibat insiden siber pada aset tertentu, sehingga dapat diketahui skala prioritas mitigasi dari daftar aset.



## PENUTUP

Demikian hasil penilaian tingkat maturitas insiden siber dan di Dinas Komunikasi dan Informatika Provinsi Jawa Barat sebagai gambaran kesiapan Pemerintah Provinsi Jawa Barat dalam menangani insiden keamanan siber di lingkungan internalnya.

Kepala Bidang Persandian dan Keamanan  
Informasi Diskominfo Provinsi Jawa Barat

Tiomaida Seviana HH, S.H., M.A.P.

Bandung, 27 Oktober 2020  
Kepala Subdirektorat Penanggulangan dan  
Pemulihan Pemerintah Daerah Wilayah I

Sriyanto, S.Sos., M.M.