



2020

# LAPORAN

HASIL PENILAIAN  
*CYBER SECURITY MATURITY (CSM)*  
DINAS KOMUNIKASI DAN INFORMATIKA  
PROVINSI SUMATERA BARAT



# PENDAHULUAN

## I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat kematangan keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Sumatera Barat. Dengan adanya tingkat kematangan ini diharapkan dapat memberikan gambaran dan mempermudah organisasi untuk mengetahui kekuatan dan kelemahan yang perlu ditingkatkan pada setiap aspek keamanan siber sehingga Dinas Komunikasi dan Informatika Provinsi Sumatera Barat maupun Badan Siber dan Sandi Negara (BSSN) dapat menyusun strategi peningkatan kematangan *cyber security* dengan tepat sasaran.

## II. Ruang Lingkup Kegiatan

Ruang lingkup penilaian kematangan keamanan siber (*Cyber Security Maturity*) pada Dinas Kominfo Provinsi Sumatera Barat mencakup 5 aspek yaitu aspek tata kelola, aspek identifikasi, aspek proteksi, aspek deteksi, dan aspek respon.

## III. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen *Cyber Security Maturity* (CSM), wawancara/diskusi, dan melihat ketersediaan dokumen keamanan siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan kematangan setiap aspek keamanan siber.

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 (*Initial*) : Rentang Level Kematangan 0 % s.d. 20 %
- Level 2 (*Repeatable*) : Rentang Level Kematangan 21 % s.d. 40 %
- Level 3 (*Defined*) : Rentang Level Kematangan 41 % s.d. 60 %
- Level 4 (*Managed*) : Rentang Level Kematangan 61 % s.d. 80 %
- Level 5 (*Optimized*) : Rentang Level Kematangan 81 % s.d. 100 %

#### IV. Pelaksanaan Kegiatan

1. Pengisian setiap pertanyaan dari *Tools CSM* oleh responden dari Dinas Komunikasi dan Informatika Provinsi Sumatera Barat dengan asitensi BSSN dilakukan pada tanggal 23 November 2020.
2. Validasi Pemetaan CSM

Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen keamanan siber. Kegiatan validasi dilaksanakan pada 23 November 2020.



# HASIL KEGIATAN

## I. Informasi Stakeholder

Nama Instansi/Lembaga : Dinas Komunikasi Dan Informatika Provinsi Sumatera Barat

Alamat : Jalan Pramuka Raya No. 11A Padang. Provinsi Sumatera Barat 25136

Nomor Telp./Fax. : (0751) 89713615

Email : [diskominfo@sumbarprov.go.id](mailto:diskominfo@sumbarprov.go.id)

Pimpinan Unit Kerja : Drs Jasman  
Kepala Dinas Kominfo Provinsi Sumatera Barat

Narasumber Instansi/Lembaga :

1. Bapak Zulkifli, SE  
Kasie Sandi, Keamanan Informasi dan Telekomunikasi
2. Rio Bayu Sentosa, M.Kom  
IT Programmer
3. Ideva Gaputra, S.Kom  
IT Network

## II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :  
 Organisasi Keseluruhan     Regional, Kanwil, Cabang     Unit Kerja     Lainnya
2. Unit Kerja : Diskominfo Provinsi Sumatera Barat
3. Fungsi Kerja  
Dinas Komunikasi dan Informatika Pemerintah Provinsi Sumatera Barat memiliki tugas dan fungsi Uraian tugasnya diatur dalam Peraturan Gubernur Sumatera

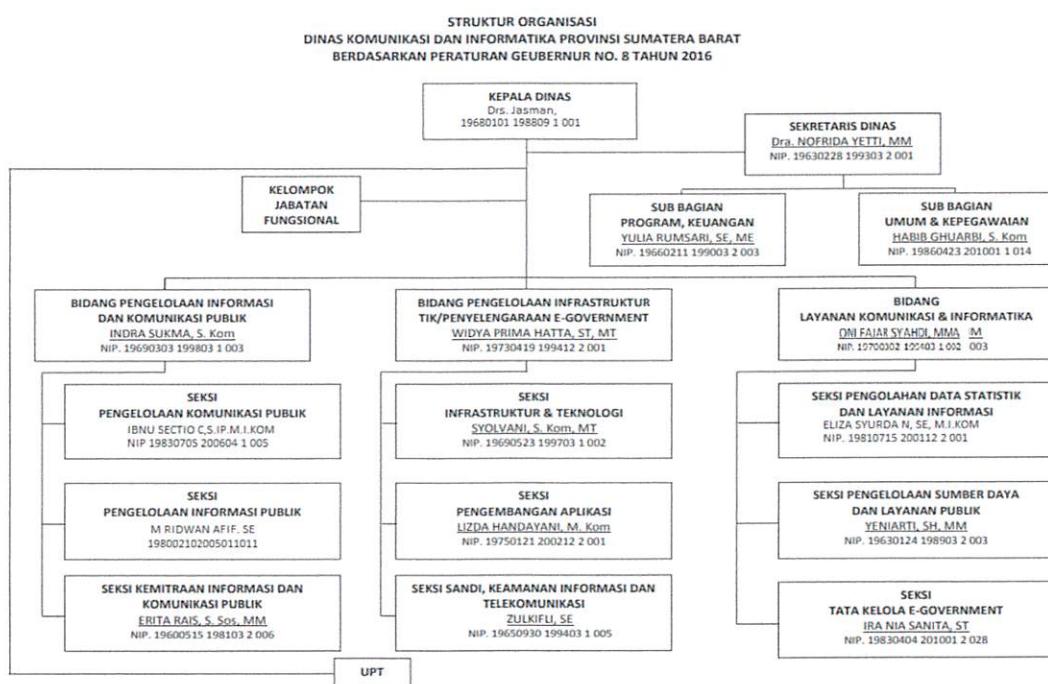


Barat Nomor 78 Tahun 2016 tentang Rincian Tugas Pokok Dan Fungsi Organisasi Perangkat Daerah Dinas Komunikasi dan Informatika Provinsi Sumatera Barat. Untuk menyelenggarakan tugas pokok Dinas Komunikasi dan Informatika Provinsi Sumatera Barat mempunyai fungsi sebagai berikut :

- a. Perumusan Kebijakan teknis bidang komunikasi dan informatika, statistik dan persandian;
- b. Penyelenggaraan urusan pemerintahan dan pelayanan umum bidang bidang komunikasi dan informatika, statistik dan persandian;
- c. Pembinaan dan fasilitasi bidang komunikasi bidang komunikasi dan informatika, statistik dan persandian lingkup Provinsi dan Kabupaten/Kota;
- d. Pelaksanaan kesekretariatan Dinas;
- e. Pelaksanaan tugas di bidang Pengelolaan Informasi dan Komunikasi Publik, Bidang Pengelolaan Infrastruktur TIK/Penyelenggaraan E-Government, dan Bidang Layanan Komunikasi dan Informatika serta Unit Pelaksana Teknis Daerah dan Fungsional KISS;
- f. Pemantauan, evaluasi dan pelaporan di bidang bidang komunikasi dan informatika, statistik dan persandian;
- g. Pelaksanaan tugas lain yang diberikan oleh Pimpinan

#### 4. Kondisi Umum

- a. Struktur organisasi satuan kerja dalam ruang lingkup



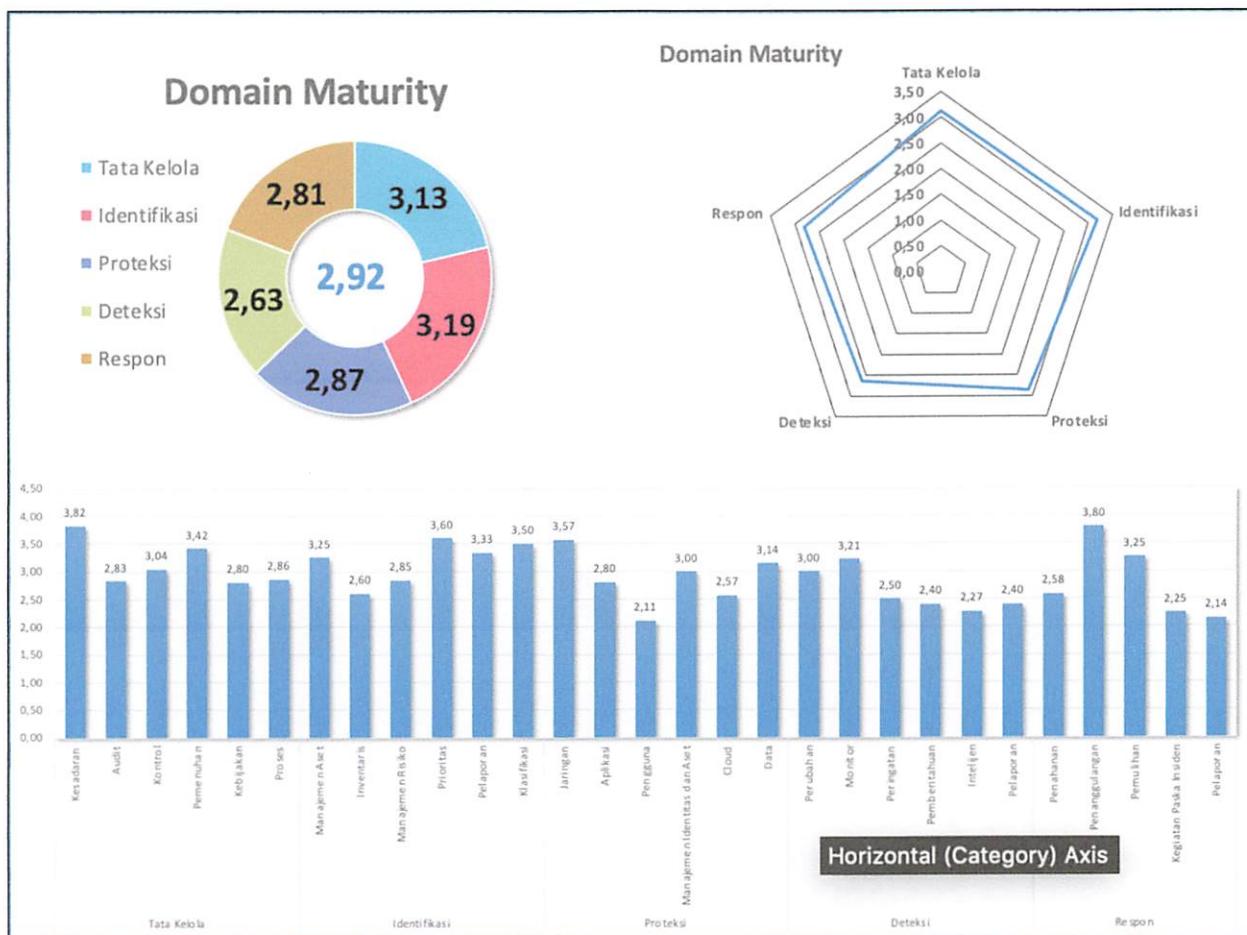


- b. SDM pengelola terdiri dari Total 95 orang, terdiri dari 44 pegawai ASN dan 51 pegawai Honorer.

### III. Hasil Penilaian CSM

Berdasarkan wawancara dan diskusi dalam rangka validasi pengisian *Cyber Security Maturity* diperoleh hasil sebagai berikut:

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
3,13		3,19		2,87		2,63		2,81	
Kesadaran	3,82	Manajemen Aset	3,25	Jaringan	3,57	Perubahan	3,00	Penahanan	2,58
Audit	2,83	Inventaris	2,60	Aplikasi	2,80	Monitor	3,21	Penanggulangan	3,80
Kontrol	3,04	Manajemen Risiko	2,85	Pengguna	2,11	Peringatan	2,50	Pemulihan	3,25
Pemenuhan	3,42	Prioritas	3,60	Manajemen Identitas dan Aset	3,00	Pemberitahuan	2,40	Kegiatan Paska Insiden	2,25
Kebijakan	2,80	Pelaporan	3,33	Cloud	2,57	Intelijen	2,27	Pelaporan	2,14
Proses	2,86	Klasifikasi	3,50	Data	3,14	Pelaporan	2,40		





Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

**Total Score Indeks Kematangan : 2,92**

Sehingga perhitungan penentuan Level Kematangan didapatkan tingkat level kematangan sebagai berikut :

**Tingkat Kematangan Level 3**

#### **IV. Kekuatan/Kematangan**

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kekuatan keamanan siber pada Pemerintah Provinsi Sumatera Barat sebagai berikut:

##### **Tata Kelola**

1. Organisasi secara berkala dan berkelanjutan telah menerapkan program awareness keamanan siber pada sebagian besar pegawai di organisasi.
2. Organisasi melaksanakan audit dan kontrol keamanan siber pada organisasi untuk mengetahui kekurangan dalam penerapan keamanan dan sebagai input untuk menerapkan perbaikan dengan melakukan kegiatan *vulnerability scanning* dan *risk assessment* telah dilakukan oleh tim keamanan aplikasi yang sudah dibentuk.
3. Organisasi telah memastikan penerapan keamanan siber telah sesuai dengan kebijakan, peraturan, dan kepatuhan keamanan siber yang telah ditetapkan.
4. Organisasi memiliki control keamanan informasi yang terkelola dan di review secara berkala. Kontrol keamanan informasi berupa alokasi penanggung jawab keamanan informasi, memastikan pegawai dan kontraktor menerapkan kebijakan dan prosedur organisasi, melakukan pemisahan lingkungan *production* dan *development*, melakukan pengujian komponen penting dari aplikasi, menerapkan NAT secara menyeluruh, filterisasi lampiran email, dan perbaruan dokumen peraturan sesuai dengan perubahan.



5. Organisasi secara formal membuat dan menyampaikan kebijakan perlindungan data pribadi, dan memastikan setidaknya setiap tahun direview.
6. Organisasi memastikan dalam pengembangan perangkat lunak/sistem informasi/aplikasi dilakukan analisis statis dan dinamis, dan memastikan versi yang dipakai masih memiliki dukungan pengembang.
7. Organisasi secara berkala melakukan analisis risiko keamanan fisik dan sistem elektronik.
8. Organisasi memiliki kebijakan yang disetujui manajemen yang dipublikasikan dan dikomunikasikan kepada pegawai dan pihak eksternal.
9. Organisasi telah memiliki pengaturan *Singe ID / Single Sign On* untuk melakukan akses kepada aplikasi milik organisasi.
10. Keamanan informasi di organisasi sudah mencakup fase perencanaan, pembangunan dan pengembangan. Pengembangan dilakukan dengan menerapkan praktik *secure coding* dan memastikan dilakukan pengecekan kesalahan pada semua input pada aplikasi.
11. Organisasi memiliki proses formal untuk manajemen perubahan perangkat jaringan.

#### Identifikasi

1. Organisasi telah melakukan manajemen asset secara terorganisir, dengan perencanaan kapasitas yang rutin dilakukan dan *update patch* terhadap asset.
2. Organisasi telah melakukan inventaris terhadap asset perangkat keras secara berkala dan konsisten.
3. Organisasi telah konsisten melakukan manajemen risiko dengan menerapkan *screening* terhadap pihak ketiga ketika menggunakan asset mereka pada jaringan organisasi. Selain itu, terdapat *risk register* yang didokumentasikan untuk semua aplikasi.
4. Organisasi telah konsisten menjadikan aspek keamanan menjadi pertimbangan dan diprioritaskan dalam beberapa pengambilan keputusan TI. Upaya remedasi telah



didasarkan pada level risiko serta dilakukan langkah proteksi untuk memprioritaskan data dan asset kritis.

5. Organisasi telah memastikan pelaporan mencakup prioritas kerentanan dan rencana mitigasinya.
6. Organisasi telak melakukan klasifikasi secara terorganisir dan berkelanjutan dalam klasifikasi TI dan *cyber threat* dengan metode/standar walaupun reviu masih belum dilakukan secara berkala

### Proteksi

1. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan *firewall* dan IPS beserta pengaturannya, mengkonfigurasikan sistem dan protokol terenkripsi, serta melakukan *filtering* pada *inbound /outbond network traffic* serta *filtering* terhadap layanan DNS.
2. Organisasi telah melakukan manajemen aplikasi yang dimiliki dengan konsisten, berupa *patching* aplikasi, memastikan aplikasi masih memiliki *update support* dan memastikan *master images server* tersimpan dengan aman.
3. Organisasi telah menerapkan pembatasan akun pengguna dan perlindungan user dengan menggunakan URL *filtering*, *device control*, dan *application control*.
4. Organisasi telah melakukan manajemen identitas dan akses dengan menggunakan identitas dan akses kengguna untuk pembatasan hak akses pada jaringan, *database*, transaksi dan data lain.
5. Organisasi telah melakukan perlindungan terhadap *cloud* yang dimiliki dengan menutup akses SSO menggunakan SSL VPN Tunnel.
6. Organisasi telah menerapkan perlindungan data dengan menyimpan log untuk mempermudah audit dan forensik, serta melakukan sinkronisasi secara otomatis untuk sinkronisasi waktu yang bermanfaat dalam sistem *backup* data.



## Deteksi

1. Organisasi telah melakukan *record* terhadap perubahan dengan deteksi perubahan konfigurasi perangkat jaringan secara otomatis.
2. Organisasi telah memiliki sistem monitoring yang aktif terhadap akses fisk dan logic, deteksi *wireless access point* dan mempersiapkan peningkatan keterampilan bagi tim monitoring.
3. Dalam hal peringatan, organisasi sudah dapat mendeteksi kegagalan login pada akun secara otomatis. Sistem *Ticketing* sudah mulai digunakan.

## 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 TI dan Sebagian besar pegawai mengenai tentang cara identifikasi, penanganan dan pelaporan suatu insiden.
3. Organisasi memastikan desain jaringan yang aman dengan pemisahan server DMZ ketika terjadi *compromise*.
4. Organisasi memiliki sumber daya redundan yang cukup untuk kondisi sistem kritis yang terganggu karena insiden siber.
5. Organisasi memiliki format baku untuk pencatatan respon insiden, dan tim respon dipastikan dapat melakukan pencatatan setiap langkah dalam penanggulangan insiden
6. Dalam kegiatan pasca insiden, organisasi dapat memastikan pencapaian SLA dalam penganganan insiden



## V. Kelemahan/Kekurangan

### Tata Kelola

1. Dalam pengembangan software/aplikasi di organisasi personel yang terlibat dalam pengembangan software/aplikasi belum mendapatkan pelatihan spesifik mengenai *secure coding*?
2. Organisasi belum memiliki atau belum melakukan reviu secara berkala mengenai kebijakan penerapan perlindungan data pribadi, akses pengguna, *security assessment* dan *risk treatment*,
3. Internal audit dalam keamanan informasi belum dilakukan secara berkala.
4. Organisasi belum dapat memastikan secara optimal sistem manajemen keamanan indormasi dalam pencapaian tujuan yang diharapkan.
5. Organisasi belum memiliki kontrol mengenai dokumentasi pengaturan akses supplier, penetapan vulnerability assessment dan pentest secara berkala.
6. Organisasi belum optimal dalam penggunaan IDS/IPS, *firewall* aplikasi web, software antivirus dan *anti malware* terpusat, *Sandbox*, *DLP*, *NAC* dan kebijakan yang mewajibakan *firewall* dan perlindungan sejenis pada perangkat pengguna.
7. Organisasi belum memiliki *risk register* yang komprehensif dengan risiko berdasarkan probabilitas dampak yang disesuaikan dengan kriteria organisasi.
8. Organisasi belum memiliki kebijakan dan prosedur untuk melindungi hak kekayaan intelektual serta prosedur dan BCP maupun DRP untuk perlindungan data pribadi.
9. Organisasi belum memiliki kebijakan metode penghapusan data, pengaturan tenggat waktu kadaluarsa akun, pengaturan akun terkait mutase pegawai serta dokumen BCP dan DRP.
10. Organisasi belum melakukan penetration testing untuk setiap aplikasi secara berkala, baik oleh internal maupun pihak eksternal.

### Identifikasi

1. Organisasi belum menggunakan perangkat otomatisasi dalam melakukan manajemen *asset*.



2. Organisasi belum optimal dalam melakukan inventarisasi perangkat lunak dan inventarisasi informasi berdasarkan klasifikasi informasinya.
3. Organisasi belum memiliki kebijakan dan pengaturan mengenai retensi data sensitif.
4. Organisasi belum memiliki kebijakan dalam pengaturan mengenai data dan pengaturan aplikasi yang berada pada perangkat pengguna.
5. Organisasi belum memiliki *Business Impact Analysis* terhadap perangkat dan aplikasi TI serta belum direview secara berkala.

#### Proteksi

1. Organisasi belum memiliki perangkat yang spesifik melakukan pemeriksaan *malware* dan eksploitasi terhadap kerentanan pada jaringan organisasi.
2. Pengaturan perangkat jaringan pengguna tidak ada atau masih belum efektif, misalkan pengaturan perangkat *wireless* pengguna, aplikasi yang diunduh, diinstall dan dioperasikan perangkat pengguna, pembatasan penggunaan *scripting tools*, kewajiban untuk menggunakan *antivirus* dan lainnya.
3. Sistem email milik organisasi belum memiliki pengecekan otomatis terhadap phising, malware dan spam
4. Organisasi belum secara optimal memanfaatkan *Multi-Factor Authentication* atau verifikasi *One Time Password (OTP)* melalui SMS, *WhatsApp Messenger*, Telepon, Elektronik Mail, *Google Authenticator*, atau media lainnya untuk transaksi yang berisiko tinggi.
5. Organisasi belum dapat melacak prilaku anomali yang dilakukan pegawai, melakukan verifikasi alamat IP dan menerapkan IP reputation untuk diizinkan melakukan transaksi.
6. Organisasi akan menggunakan *cloud storage* dan memerlukan pengaturan tambahan spesifik mengenai *cloud*.



## Deteksi

1. Organisasi belum menerapkan tim manajemen perubahan dan tidak ada review berkelanjutan yang melibatkan tim managemen perubahan.
2. Organisasi belum memiliki mekanisme monitoring terhadap akses dan perubahan pada data sensitive, pencegahan penggunaan enkripsi yang tidak sah serta pencegahan kehilangan data sensitif.
3. Organisasi belum menerapkan SIEM / tools analisis log, Perangkat anti malware atau kombinasi keduanya yang digunakan secara otomatis.
4. Organisasi belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat(24/7) untuk menangani kejadian dengan prioritas tinggi dan kritis.
5. Organisasi belum memiliki *Contact tree* untuk mengeskalasi dalam merespon suatu insiden.
6. Organisasi belum menerapkan *event notification* yang berbeda untuk setiap jenis eskalasi (berdasarkan prioritasnya)
7. Organisasi belum memiliki perangkat dan sarana pendukung untuk melakukan *Threat Intelligence*.
8. Organisasi tidak memiliki jadwal tetap dalam melakukan review metrik security event.

## Respon

1. Rencana respon insiden, DRP, BCP dan SOP penanganan insiden belum direview dan dijadwalkan secara berkala.
2. Organisasi belum melakukan tindakan pencegahan dari hasil review terhadap *root cause* suatu insiden siber.
3. Organisasi belum melakukan review terhadap rekapitulasi laporan insiden siber dan dilaporkan ke pimpinan serta melakukan review kontrol yang ada untuk perbaikan respon penanganan siber selanjutnya.
4. Organisasi belum menentukan standar terkait waktu pelaporan kejadian tidak wajar kepada tim penanganan insiden.



## VI. Rekomendasi

1. Untuk meningkatkan Tata Kelola keamanan siber di lingkungan Dinaskominfo Pemprov Sumbar maka dapat dilakukan hal-hal sebagai berikut:
  - a. Mengadakan pelatihan *secure coding* untuk *programmer* yang terlibat dalam pembangunan aplikasi.
  - b. Mengadakan pelatihan/workshop/bimtek kesadaran keamanan informasi untuk semua pegawai internal organisasi.
  - c. Menyusun kebijakan penerapan perlindungan data pribadi, prosedur *security assessment* dan *risk assessment*.
  - d. Melakukan penjadwalan audit internal secara berkala dan berkelanjutan
  - e. Mengoptimalkan SMKI dan memastikan Kebijakan SMKI mencakup semua area keamanan siber dan mendukung tujuan organisasi.
  - f. Perlu dibuat kebijakan atau prosedur terkait aturan turunan dari SMKI yang mengatur hak akses, penilaian kerentanan, pentesting, dan lainnya.
  - g. Diperlukan perangkat yang dapat mengotomasi pendekripsi serangan dan dukungan keamanan.
  - h. Diperlukan prosedur penilaian risiko yang komprehensif berdasarkan kriteria probabilitas dan dampak.
  - i. Diperlukan penyususan prosedur perlindungan HaKI milik organisasi.
  - j. Diperlukan Pembuatan BCP dan DRP.
  - k. Diperlukan pelaksanaan *security assessment*, penilaian risiko, penilaian kerentanan dan pentest secara berkala dan berkelanjutan.
2. Untuk meningkatkan area Identifikasi keamanan siber di lingkungan Diskominfo Pemprov Sumbar, maka dapat dilakukan hal-hal sebagai berikut:
  - a. Diperlukan pengadaan perangkat yang dapat mengotomatisasi dan memastikan perlindungan terhadap manajemen asset.
  - b. Diperlukan kebijakan/prosedur dan pelaksanaan klasifikasi informasi dan retensi informasi.



- c. Penyusunan kebijakan dalam pengaturan mengenai data dan pengaturan aplikasi yang berada pada perangkat pengguna
  - d. Diperlukan penyusunan dokumen *Business Impact Analysis* dari perangkat dan aplikasi TI serta direviu secara berkala.
3. Untuk meningkatkan area Proteksi keamanan siber di lingkungan Diskominfo Pemprov Sumbar, maka dapat dilakukan hal-hal sebagai berikut:
- a. Diperlukan penambahan perangkat yang mampu mendeteksi *malware*, perilaku anomali pengguna atau serangan secara otomatis.
  - b. Penyusunan Kebijakan yang mengatur mengenai penggunaan perangkat, jaringan dan aplikasi milik pengguna.
  - c. Pertimbangan untuk menggunakan *Multi-Factor Authentication* dan Verifikasi *One Time Password* untuk Sistem Informasi dengan transaksi berisiko tinggi.
  - d. Jika *Cloud storage* sudah diterapkan, maka diperlukan kebijakan dan prosedur teknis yang mengatur mengenai keamanan siber dan jaminan data privasi pengguna.
4. Untuk meningkatkan area Deteksi keamanan siber di lingkungan Diskominfo Pemprov Sumbar, maka dapat dilakukan hal-hal sebagai berikut:
- a. Membentuk tim manajemen perubahan dan memastikan tim manajemen perubahan melakukan reviu terhadap semua perubahan TI.
  - b. Diperlukan penyusunan Mekanisme monitoring terhadap jaminan keutuhan dan keaslian data sensitif,
  - c. Diperlukan pengadaan perangkat analisis Log, SIEM dan anti *malware* untuk merekam log dan mendeteksi terjadinya serangan.
  - d. Diperlukan pembentukan atau penyediaan layanan SOC yang menangani insiden dengan prioritas tinggi yang dapat dihubungi setiap saat (24/7)
  - e. Diperlukan penyusunan *Contact Tree* untuk memudahkan koordinasi ketika terjadi insiden.
  - f. Dalam tahap lebih lanjut, diperlukan perangkat pendukung dan mekanisme *threat intelligence* untuk mengetahui tren ancaman, dan bagaimana mencegah



ancaman dan melakukan sharing dengan pengguna mengenai pencegahan ancaman tersebut,

g. Diperlukan penjadwalan dalam melakukan reviu matrik *security event*.

5. Untuk meningkatkan area Respon keamanan siber di lingkungan Diskominfo Pemprov Sumbar, maka dapat dilakukan hal-hal sebagai berikut:

- a. Diperlukan penyusunan dokumen BCP dan DRP serta reviu secara berkala terhadap dokumen rencana respon Insiden, dan SOP penanganan insiden.
- b. Melakukan reviu terhadap root cause dari insiden siber dan memastikan Tindakan pencegahan diterapkan sesuai dengan hasil reviu.
- c. Secara rutin dilakukan reviu terhadap kontrol dan reviu rekapitulasi laporan insiden siber dan dilaporkan ke pimpinan.



# PENUTUP

Demikian disampaikan laporan kegiatan penilaian CSM pada Dinas Komunikasi dan Informatika Pemerintah Provinsi Sumatera Barat, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Padang, 24 November 2020

Kabid Pengelolaan Infrastruktur TIK  
/Penyelengaraan E-Government

  
( Widya Prima Hatta, ST.,MT )  
NIP. 19730419 199412 2 001

Ketua Tim BSSN

  
(Agus Indramawan, S.ST)  
NIP. 19830822 200312 1 005