2021

# LAPORAN

## HASIL PENILAIAN

## *CYBER SECURITY MATURITY* (CSM)

## DINAS KOMUNIKASI DAN INFORMATIKA
## PROVINSI SUMATERA SELATAN

# PENDAHULUAN

## I. Umum

Tingkat kesiapan keamanan siber di setiap organisasi berbeda-beda, sehingga masing-masing organisasi juga membutuhkan strategi yang berbeda-beda pula dalam menghadapi ancaman, serangan, maupun ancaman siber. Dalam implementasi keamanan siber, beberapa organisasi baru fokus terhadap perbaikan penerapan kontrol keamanan yang lebih proaktif, penyusunan peraturan dan kebijakan keamanan siber, dan penyusunan strategi keamanan berdasarkan hasil deteksi insiden. Selain itu, sebagian organisasi telah mendorong investasi teknologi sebagai kebutuhan keamanan serta telah memberikan dukungan personel di bidang keamanan siber yang kompeten, serta mempertimbangkan risiko siber serta mendorong budaya keamanan siber secara menyeluruh untuk keberlangsungan organisasinya.

Setiap organisasi harus memahami kelemahan dari proses keamanan siber yang dimiliki. Sehingga dapat menentukan target tingkat keamanan siber yang akan dicapai dan memastikan bahwa organisasi tersebut telah siap dalam menghadapi ancaman siber dalam bentuk apapun. Oleh karena itu diperlukan suatu metode pengukuran kematangan keamanan siber agar organisasi dapat melakukan peningkatan dalam pengelolaan proses keamanan siber dan memastikan bahwa telah dioptimalkan sepenuhnya dan berfungsi secara menyeluruh. Untuk itu, Badan Siber dan Sandi Negara (BSSN) telah membentuk suatu *framework* untuk mengukur *cyber security maturity* yang dapat digunakan sebagai metode untuk mengukur tingkat kematangan keamanan siber suatu organisasi.

*Tools Cyber Security Maturity* merupakan alat bantu yang digunakan untuk mengukur kematangan keamanan siber di organisasi. Sektor pemerintahan sebagai salah satu domain yang memanfaatkan ruang siber diharapkan turut melakukan peningkatan pengelolaan keamanan siber serta memastikan pengelolaan tersebut berjalan dengan optimal dan berfungsi secara menyeluruh.

## II. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Sumatera Selatan. 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 maturitas keamanan siber.

## III. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek penanganan insiden meliputi :

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

## IV. Metodologi Kegiatan

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

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

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

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 %

## V. Pelaksanaan Kegiatan

Pengisian Instrumen CSM dilakukan oleh internal *stakeholder* (*self assessment*) dilakukan pada 26 s.d. 27 Oktober 2021 dengan dipandu dan divalidasi oleh Tim BSSN.

# HASIL KEGIATAN

## I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Sumatera Selatan

Alamat : Jalan Merdeka No.10 Kec. Talang Semut, Palembang

Nomor Telp./Fax. : (0711) 5733273

Email : webmaster@sumselprov.go.id

Narasumber Instansi/Lembaga :

1. Marwanika, S.H. (Kepala Seksi Persandian)
2. Widyasmoro
3. Azwar Fernando
4. Arifin
5. Aan
6. Ferdinan

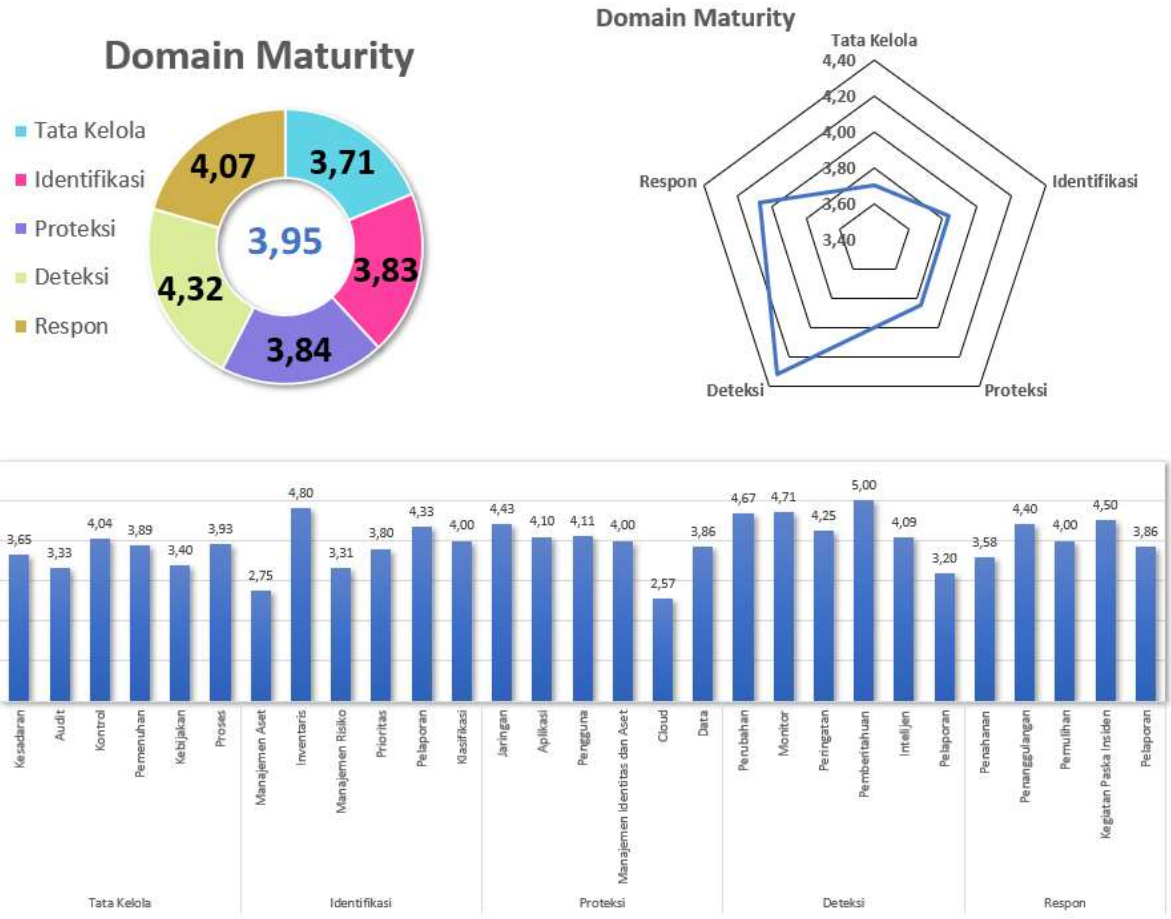
## II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

☐ Organisasi Keseluruhan ☐ Regional, Kanwil, Cabang √ Unit Kerja ☐ Lainnya

2. Instansi/Unit Kerja* : Dinas Kominfo Provinsi Sumatera Selatan, Bidang TIK dan Persandian Seksi Integrasi Data dan Informasi

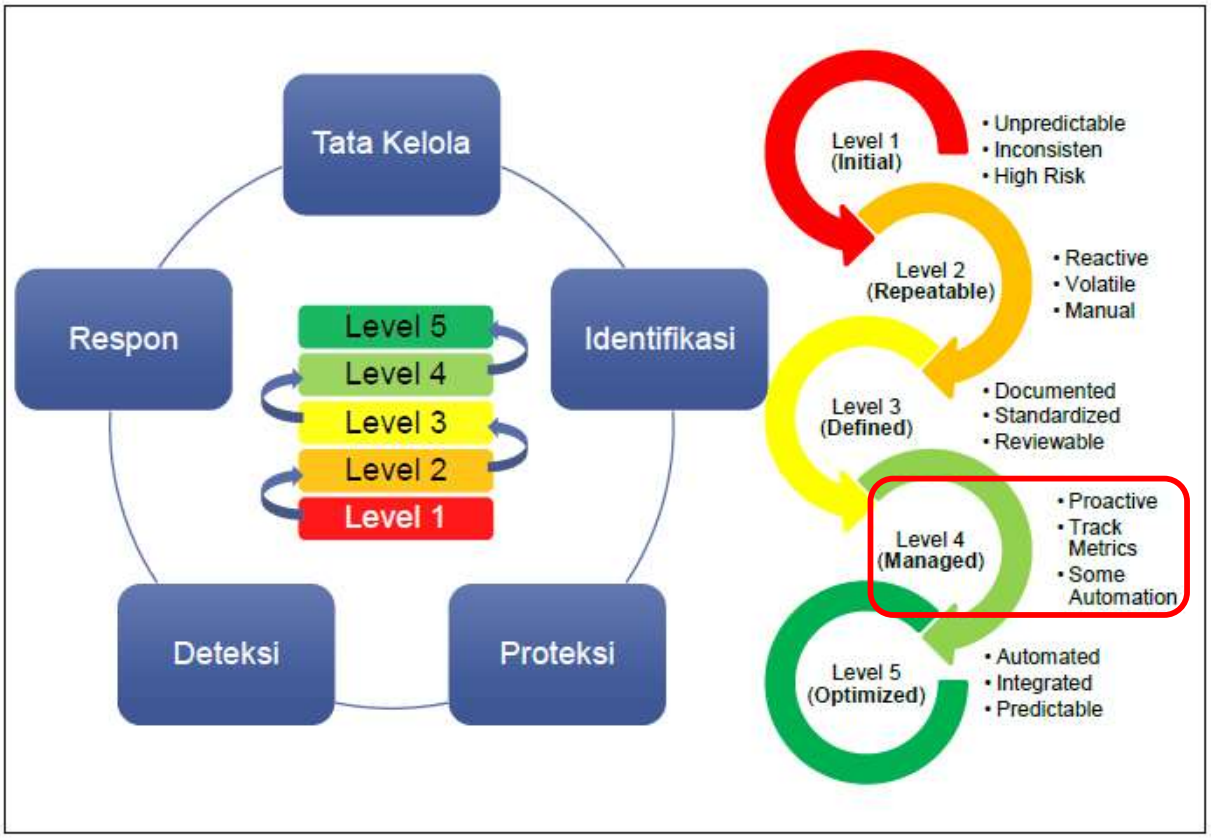
# III. Hasil Penilaian CSM




Gambar 1. Hasil Penilaian CSM

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**




Gambar 2. Capaian Level Kematangan

**Level Kematangan 4:**

Level kematangan 4 menunjukkan bahwa pengelolaan keamanan siber di Dinas komunikasi dan Informatika Provinsi Sumatera Selatan sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat format, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan.

# IV. Kekuatan/Kematangan

**Tata Kelola**

1. Organisasi telah memiliki program pemahaman kesadaran keamanan informasi yang menyasar pihak eksternal. Kegiatan berupa literasi ke pelajar atau masyarakat

umum. Kegiatan dilakukan secara berkelanjutan dan tema kegiatan diperbarui secara berkala.

2. Organisasi memberikan pengarahan mengenai keamanan informasi kepada karyawan melalui himbauan.
3. Organisasi telah melatih staf secara khusus tentang kewajiban data privasi.
4. Organisasi telah menerapkan manajemen kerentanan siber dan mitigasi terhadap kerentanan melalui CSIRT
5. Organisasi melakukan simulasi *phishing* secara berkala ke karyawan
6. Personil yang terlibat dalam pengembangan software/aplikasi (Bidang E-Government) telah mendapatkan pelatihan mengenai *secure code*.
7. Organisasi melakukan pemeriksaan *background* untuk semua karyawan.
8. Pengembangan software menggunakan algoritma enkripsi dan direviu secara berkala.
9. Organisasi sudah memiliki dokumentasi/diagram aliran data di seluruh sistem dan jaringan.
10. Organisasi sudah mendefinisikan peran dan tanggungjawab terkait keamanan informasi dan pembagian peran ke personil.
11. Web organisasi telah dilindungi firewall aplikasi web (WAFs).
12. Organisasi memiliki kebijakan keamanan informasi berupa Pergub SPBE yang dikembangkan dengan mengacu ke ISO 27001, SMKI dan Perpres 95 Tahun 2018.
13. Organisasi melakukan penetration testing menggunakan pihak eksternal dan internal.
14. Dilakukan manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi router, switch dan firewall di lab/development.

**Identifikasi**

1. Organisasi melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa pengadaan semua aset perangkat dan aplikasi dilakukan sesuai dengan kebutuhan melalui perencanaan pengadaan setiap tahun.

2. Organisasi telah melakukan identifikasi dan inventarisasi data pada perangkat keras dan perangkat lunak secara berkala dan telah disusun berdasarkan klasifikasi kritikalitas.
3. Organisasi sudah melakukan identifikasi perangkat yang tidak diizinkan dan menerapkan pembatasan akses terhadap perangkat tersebut.
4. Organisasi tidak memberikan izin untuk menggunakan aset Organisasi dan dibatasi aksesnya.
5. Aspek keamanan mempertimbangkan kapasitas *server* dan perangkat jaringan secara menyeluruh.
6. Organisasi mempertimbangkan aspek keamanan dalam pengambilan keputusan TI.
7. Dokumentasi alur informasi yang memproses data stakeholder / klien/konsumen/ pelanggan termasuk yang dikelola oleh pihak ketiga sudah disusun
8. Sudah ada kebijakan dan implementasi mengenai retensi data sensitif.
9. V*ulnerability scanning* dan/atau *penetration testing* sudah dilakukan secara menyeluruh terhadap semua aset perangkat dan aplikasi
10. Organisasi sudah menerapkan segmentasi jaringan dengan ditambahkan kontrol keamanan antar segmennya.

**Proteksi**

1. Organisasi melindungi jaringan nirkabel dengan fitur enkripsi (password).
2. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan *firewall*, melakukan filtering pada *inbound* dan *outbound network traffic*, DNS *filtering services*.
3. Organisasi telah menerapkan port access control.
4. Organisasi melakukan penonaktifan komunikasi antar workstation.
5. Organisasi telah menerapkan pembatasan terhadap aplikasi yang diunduh, diinstal dan dioperasikan
6. Patch pada aplikasi (operating system dan software) telah dikelola secara otomatis.

7. Organisasi telah menerapkan whitelist aplikasi.
8. Organisasi telah menerapkan Next Generation Endpoint Protection.
9. Organisasi menggunakan antivirus di semua perangkat endpoints termasuk server
10. Organisasi telah menerapkan URL Filtering, device control, dan application control pada semua perangkat endpoint pengguna
11. Media penyimpanan eksternal yang dimiliki organisasi telah dienkripsi dan diatur aksesnya (read/write).
12. Organisasi menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu.
13. Organisasi telah menerapkan identity and access management systems untuk seluruh operating system.
14. Organisasi telah menerapkan manajemen password yaitu pengaturan kompleksitas password dan penggantian password secara berkala dan otomatis terkhusus pada server.
15. Organisasi telah mengatur hak akses untuk akses ke data stakeholder.
16. Organisasi telah menerapkan IP reputation
17. Organisasi melakukan *backup* data secara berkala, melakukan pengujian data integrity terhadap data yang di*backup*, data yang disimpan dilindungi dengan fitur enkripsi dan disimpan di lokasi yang aman.

**Deteksi**

1. Organisasi telah menerapkan deteksi otomatis perubahan konfigurasi pada peralatan jaringan.
2. Organisasi telah melakukan monitoring terhadap penggunaan enkripsi yang tidak sah, akses dan perubahan pada data sensitif, aktivitas lalu lintas jaringan dan log dari perangkat security control, jaringan dan aplikasi.
3. Organisasi telah menerapkan SIEM (Security Information Event Monitoring).
4. Organisasi dapat mendeteksi *Wireless* Access *Point* yang terhubung ke jaringan *LAN*.

5. Organisasi dapat mendeteksi anomali pada jaringan dan anomali dan kegagalan login pada akun admin pada perangkat jaringan, server dan aplikasi dan secara otomatis ternotifikasi ke admin.
6. Organisasi melakukan pemantauan terhadap aktivitas pihak ketiga dan akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
7. Organisasi memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
8. Organisasi menerapkan automated port scan secara berkala terhadap semua sistem dan memberikan alert.
9. Organisasi memiliki *ticketing system*, sistem untuk mendeteksi ancaman siber dan sistem untuk melakukan Malicious Code Detection.
10. Organisasi memiliki SOC yang dapat dihubungi setiap saat (24x7).
11. Organisasi memiliki daftar kontak (contact tree) pihak terkait untuk eskalasi suatu event.
12. Organisasi bekerjasama dengan pihak – pihak terkait (MPPS/penyedia produk keamanan siber dan forum CSIRT) untuk memperoleh informasi dan update mengenai isu keamanan siber terkini.
13. Organisasi menerapkan DNS query logging.

**Respon**

1. Organisasi telah memiliki SOP dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait dan telah dilakukan reviu secara berkala.
2. Organisasi mempunyai daftar kontak tim penanganan insiden internal dan eksternal.
3. Organisasi telah melakukan latihan respon insiden dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
4. Organisasi mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.

5. Tim respon insiden memiliki kemampuan mendeteksi insiden, melakukan analisis, dan memberikan rekomendasi serta memiliki peralatan sumber daya analisis insiden.
6. Tim respon insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis dalam hal ini BSSN.
7. Laporan insiden di organisasi Anda dilaporkan ke top management dan ke pihak eksternal yang berkepentingan/wajib dilaporkan sesuai regulasi.

# V. Kelemahan/Kekurangan

**Tata Kelola**

1. Organisasi tidak menggunakan akun khusus selain akun admin untuk melakukan vulnerability scanning.
2. Organisasi belum menerapkan manajemen risiko.
3. Organisasi belum menerapkan software antivirus dan anti malware yang terpusat.
4. Organisasi belum menerapkan metode sandbox terhadap seluruh lampiran email
5. Organisasi belum melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi.
6. Organisasi belum memiliki kebijakan keamanan informasi yang mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.
7. Organisasi belum menyusun BCP dan DRP.
8. Organisasi belum melakukan *threat hunting* secara berkala.

**Identifikasi**

1. *System configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak belum ada.
2. Dokumen risk register untuk semua aplikasi yang memproses data stakeholder belum ada.
3. *Business Impact Analysis* terhadap perangkat dan aplikasi TI belum disusun.

**Proteksi**

1. Belum ada kebijakan terkait pembatasan penggunaan *scripting tools*.
2. Penggunaan *Multi Factor Authentication* belum diterapkan
3. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.

**Deteksi**

1. Organisasi belum melakukan *escalation profile* untuk setiap *security event* yang ditemukan.
2. Organisasi belum menjalankan *vulnerability scanning tools* secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
3. Unit dalam organisasi belum menjalankan fungsi Cyber Threat Intelligence (CTI).
4. Organisasi belum memiliki *Metrik Security Event*.

**Respon**

1. Organisasi belum melakukan reviu secara berkala terhadap dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar standar operasional prosedur (SOP) penanganan insiden.
2. Organisasi belum menerapkan mekanisme backup data pada pc/laptop karyawan ke cloud organisasi.
3. Tim respon insiden belum melakukan pencatatan langkah-langkah penanggulangan insiden menggunakan format baku.

# VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfo Pemprov Sumatera Selatan maka dapat dilakukan hal-hal sebagai berikut:
   a. Menerapkan manajemen risiko terhadap seluruh aset milik organisasi.
   b. Menyusun BCP dan DRP

c. Melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi
d. Mengimplementasi single ID yang unik untuk semua otentikasi
e. Menerapkan software antivirus dan anti malware yang terpusat
f. Menerapkan penggunaan akun khusus selain akun admin untuk melakukan *vulnerability scanning*.
g. Menerapkan metode sandbox terhadap seluruh lampiran email
h. Memprogramkan *threat hunting* secara berkala.

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun *Business Impact Analysis* terhadap perangkat dan aplikasi TI
   b. Menyusun dokumen risk register untuk seluruh aset milik organisasi
   c. Melakukan penerapan *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menerapkan penggunaan *Multi Factor Authentication*.
   b. Menyusun kebijakan terkait pembatasan penggunaan scripting tools.
   c. Menerapkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun *escalation profile* untuk setiap *security event*
   b. Menyusun *Metrik Security Event*
   c. Menerapkan *vulnerability scanning tools* secara otomatis menggunakan agent/aplikasi dan diinstal pada *endpoint*.
   d. Mengadakan atau menganggarkan pelatihan terkait Cyber Threat Intelligence kepada personil
5. Untuk meningkatkan aspek respon, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun format laporan penanganan insiden dan membuat laporan penanganan insiden setiap kali terjadi insiden

b. Menerapkan mekanisme backup data pada pc/laptop karyawan ke cloud organisasi
c. Menjadwalkan reviu secara berkala dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar standar operasional prosedur (SOP) penanganan insiden

# PENUTUP

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

Palembang, 28 Oktober 2021

| | |
|---|---|
| Kepala Bidang Teknologi Informasi, Komunikasi dan Persandian | Koordinator Kelompok Manajemen Risiko PTK KSS Pemda |
| (John Kenedy, M.Si.) | (Nurchaerani,S.E.) |