2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI KEPULAUAN RIAU

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 Kepulauan Riau. 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 keamanan 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

1. Pengisian Instrumen CSM

   Pengisian Instrumen CSM dilakukan secara mandiri oleh *stakeholder* pada tanggal 13 s.d. 17 Juni 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 21 dan 22 Juni 2022, dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Kepri. Tim BSSN yang terlibat:

   1) Nurhaerani, S.E.
   2) Aris Munandar, S.S.T.MP.
   3) Mas Merdekadyarta, S.Tr.TP.
   4) Ni Putu Ayu Lhaksmi Wulansari, S.Tr.TP.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau

Alamat : Komplek Pusat Pemerintahan Provinsi Kepulauan Riau, Gedung Sultan Mahmud Riayat Syah (Gedung B2 Lantai III), Dompak, Tanjungpinang

Nomor Telp./Fax. : (0771) 4575023

Email : kominfo@kepriprov.go.id

Narasumber Instansi/Lembaga :

1. Didi Madjdi, S.E. (Kepala Bidang Statistik dan Persandian)
2. Donny Firmansyah, ST. (Sub Koordinator Keamanan Informasi E-Government dan Persandian)
3. Edi Wansyah, S.Tr. (Fungsional Sandiman Pertama)
4. Abduloh Ansorudin, A.Md. (Staf Infrastruktur dan Teknologi Informasi Komunikasi)

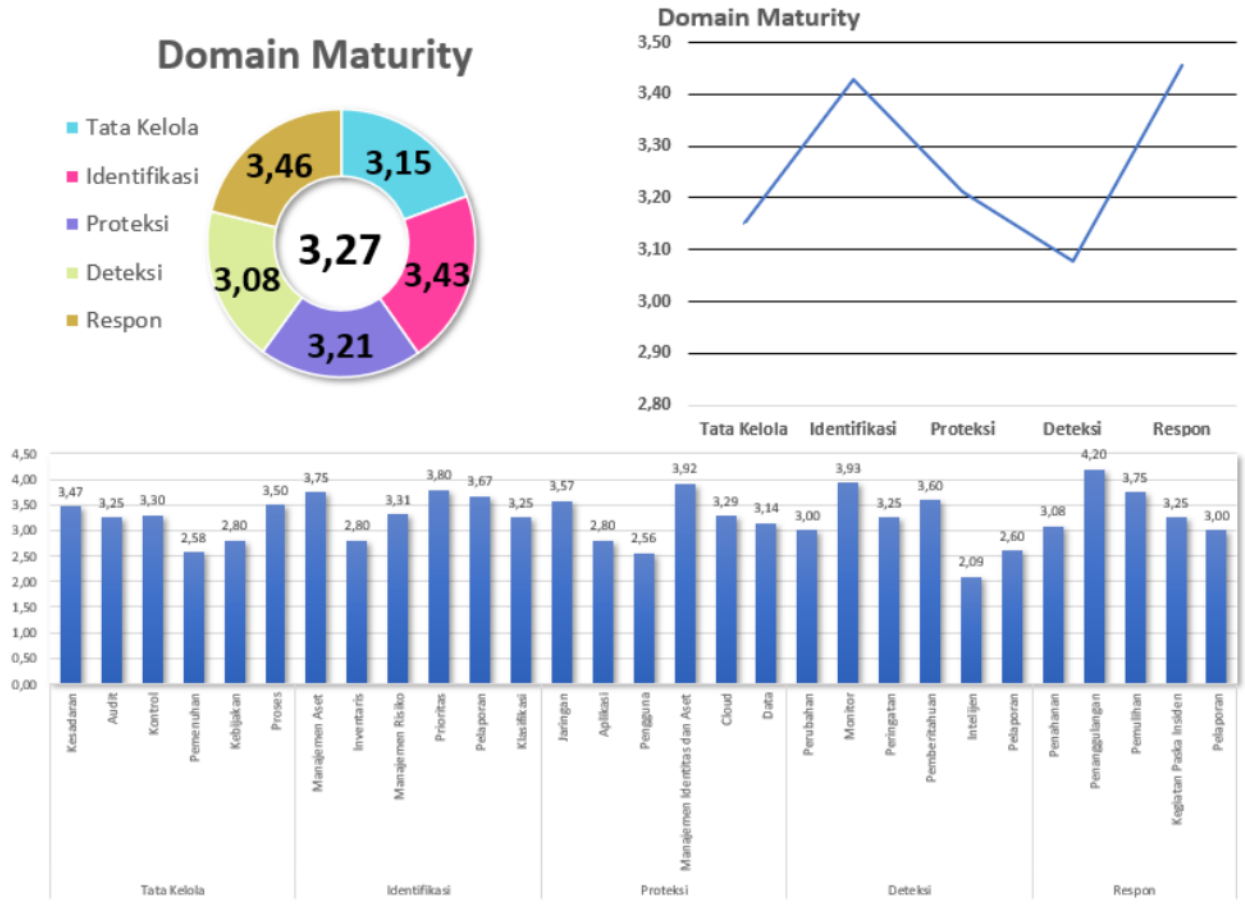
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja : Dinas Komunikasi dan Informatika Provinsi Kepri

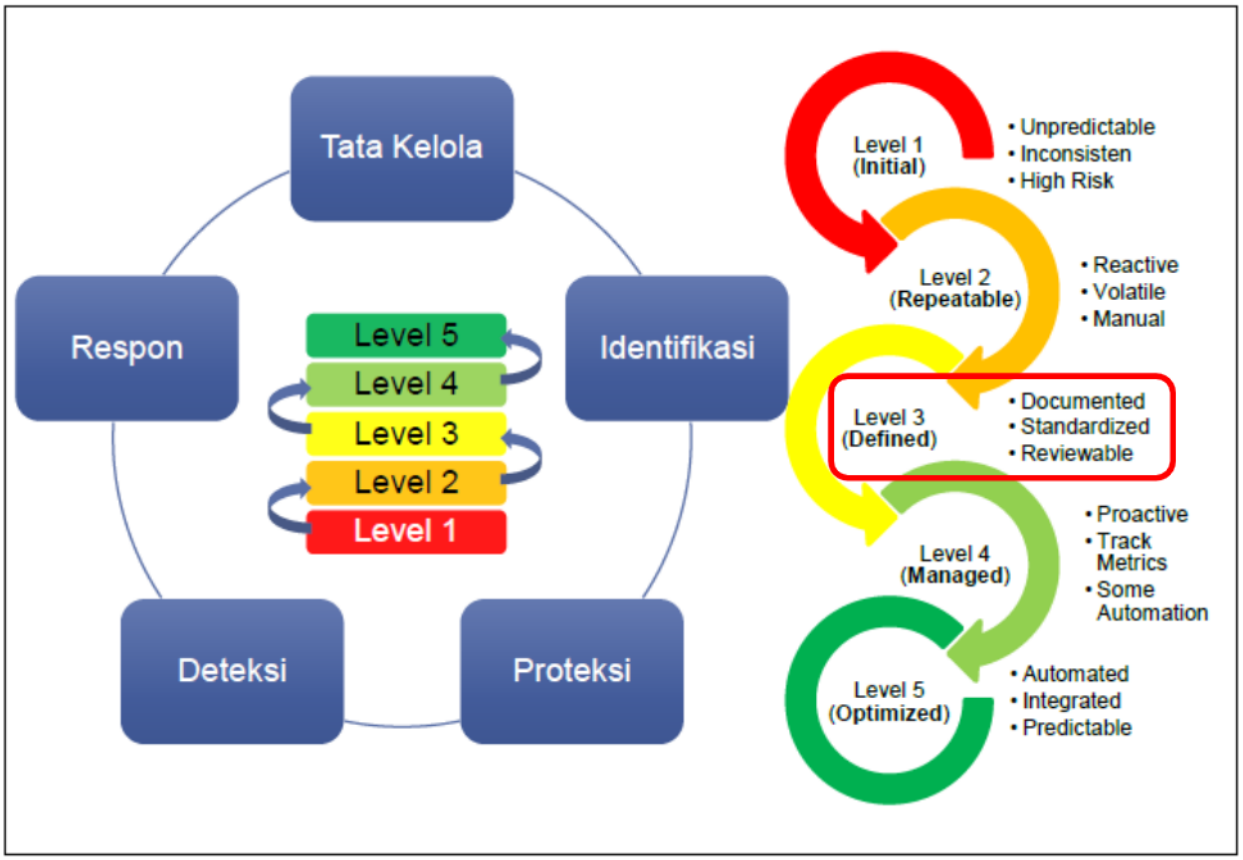
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan: 3,27,** sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut:

Level Kematangan Tingkat 3



Gambar 2. Capaian Level Kematangan

Level Kematangan 3:

Level kematangan 3 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau sudah terorganisasi dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan.

IV. Kekuatan/Kematangan

Tata Kelola

1. Telah menjalankan program pemahaman kesadaran keamanan informasi bagi karyawan
2. Memberikan pengarahan mengenai keamanan informasi kepada karyawan baru melalui penandatanganan NDA (*Non Disclosure Agreement*).
3. Dapat menggunakan *tool vulnerability scanning* secara mandiri.
4. Melakukan pemisahan environment antara sistem production dan development.
5. Menerapkan kontrol kriptografi sesuai dengan peraturan yang berlaku.
6. Menerapkan perlindungan sesuai dengan persyaratan dan peraturan terhadap dokumentasi yang dimiliki organisasi.
7. Kebijakan keamanan informasi dan hasil evaluasi pelaksanaan kebijakan keamanan informasi menjadi acuan pimpinan dalam menentukan strategi organisasi.
8. Menerapkan filterisasi pada email dinas.
9. Melaksanakan *penetration testing* menggunakan pihak eksternal dan internal.
10. Melindungi aplikasi web organisasi menggunakan *firewall* aplikasi web (WAFs).

Identifikasi

1. Aspek keamanan menjadi pertimbangan dan diprioritaskan dalam semua pengambilan keputusan TI, kapasitas server dan perangkat jaringan.
2. Melakukan inventarisasi data aset (perangkat keras maupun lunak) meskipun belum secara konsisten dilakukan.
3. Mengatur terkait izin pihak ketiga untuk menggunakan aset mereka pada jaringan organisasi setelah melalui screening oleh Bagian TI.
4. Menerapkan *patch* keamanan pada semua perangkat keras dan perangkat lunak saat ada *update patch* yang sudah dirilis.
5. Menerapkan segmentasi jaringan berdasarkan fungsionalitas.

Proteksi

1. Memiliki firewall dan IDS/IPS dan telah *menerapkan rules inbond dan outbond network traffic* serta telah menerapkan antivirus pada perangkat (server maupun *endpoint*).
2. Menerapkan sistem enkripsi pada akses nirkabel.
3. Melakukan backup data pada aplikasi secara berkala.
4. Menerapkan antivirus pada seluruh perangkat endpoint maupun server.
5. Menerapkan DNS Filtering services.
6. Koneksi ke perangkat server dan jaringan menggunakan protokol terenkripsi yaitu SSH.
7. Email system memiliki pengecekan otomatis terhadap spam/phising/malware.
8. Semua kritikal system clocks telah disinkronkan dengan metode otomatis seperti Network Time Protocol.

Deteksi

1. Memiliki SIEM atau Log Analytic Tools namun belum beroperasi secara optimal.
2. Memiliki ticketing system yang digunakan untuk melacak progress dari event post-notification.
3. Organisasi menjamin alokasi kapasitas penyimpanan log sesuai kebutuhan.
4. Melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center.
5. Memiliki contact tree untuk mengeskalasi dalam merespon suatu kejadian.

Respon

1. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.

2. Sebagian pegawai telah melakukan pelatihan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
3. Tim respon insiden memiliki kemampuan dalam mendeteksi insiden, melakukan analisis insiden dan memberikan rekomendasi penanganan insiden.
4. Tim respon insiden siber memiliki peralatan sumber daya analisis insiden.

V. Kelemahan/Kekurangan

Tata Kelola

1. Meningkatkan kegiatan program pemahaman kesadaran keamanan informasi dengan fokus/isu baik terkait dengan kebijakan yang telah ditetapkan maupun permasalahan keamanan informasi yang perlu dilakukan secara berkelanjutan.
2. Belum terdapat *Business Continuity Plan* dan *Disaster Recovery Plan* yang mencakup *backup* dan *restoration* dari data pribadi.
3. Belum adanya kebijakan dan implementasi dalam pelaksanaan reviu izin akses dari akun pengguna dan menerapkan *single* ID untuk otentikasi.
4. Belum mengimplementasikan antivirus dan antimalware secara terpusat dan selalu dipastikan update.
5. Belum melakukan internal audit keamanan informasi secara berkala.
6. Belum menyusun roadmap baseline pendidikan dan pelatihan terkait keamanan informasi bagi karyawan.
7. Belum pernah melakukan dan menguji skenario penanganan insiden secara mandiri (termasuk simulasi phishing).
8. Belum memiliki kebijakan perlindungan data pribadi.
9. Belum melakukan reviu security risk assessment secara berkala.
10. Belum menyusun risk treatment dan melakukan reviu terhadap risk treatment secara berkelanjutan.
11. Belum melakukan reviu izin akses dari akun pengguna secara periodik (setiap tiga bulan).

Identifikasi

1. Organisasi belum membuat/memperbarui *roadmap* keamanan TI organisasi dalam jangka waktu tertentu.
2. Belum tercantum pada risk register untuk semua aplikasi yang memproses data stakeholder/klien/konsumen/pelanggan.
3. Belum memiliki *system configuration management tools* otomatisasi konfigurasi perangkat keras dan perangkat lunak.
4. Belum dilakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman/standar/acuan organisasi.
5. Belum memiliki Business Impact Analysis (BIA) terhadap perangkat dan aplikasi TI.
6. Belum memiliki standar/pedoman/acuan untuk klasifikasi kritikalitas aset TI.

Proteksi

1. Belum menerapkan *Multi-Factor Authentication* (MFA) untuk mengakses data sensitif dan akses jaringan.
2. Belum menonaktifkan komunikasi antar workstation.
3. Belum memiliki pengaturan terkait pembatasan aplikasi yang dapat diunduh, diinstall dan dioperasikan pada perangkat milik organisasi.
4. Belum menambahkan verifikasi OTP untuk transaksi yang berisiko tinggi.
5. Belum melakukan pengujian data integrity secara berkala terhadap data yang dibackup.
6. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint.
7. Belum melakukan pembatasan terhadap penggunaan scripting tools.
8. Belum menerapkan enkripsi untuk data stakeholder/pengguna yang disimpan oleh organisasi dan enkripsi pada media penyimpanan eksternal.
9. Belum menerapkan SSO (Single Sign On) pada cloud organisasi.

Deteksi

1. Belum melakukan *record* seperti Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.
2. Belum memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data *sensitive*.
3. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
4. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
5. Belum menjalankan vulnerability scanning tools secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
6. Unit dalam organisasi belum menjalankan fungsi Cyber Threat Intelligence (CTI).
7. Organisasi belum memiliki Metrik Security Event.
8. Belum membuat escalation profile untuk setiap security event yang ditemukan.
9. Belum memiliki sistem untuk melakukan Malicious Code Detection untuk melindungi dari malicious code.
10. Mekanisme sharing informasi hasil deteksi belum ada.

Respon

1. Belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Belum merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
3. Belum menerapkan mekanisme backup data karyawan ke cloud organisasi.
4. Belum memiliki SLA (*Service Level Agreement*) dalam penanganan insiden.
5. Belum melakukan reviu rekap laporan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfo Provinsi Kepri maka dapat dilakukan hal-hal sebagai berikut:
   a. Meningkatkan kegiatan program pemahaman kesadaran keamanan informasi dengan fokus/isu baik terkait dengan kebijakan yang telah ditetapkan maupun permasalahan keamanan informasi yang perlu dilakukan secara berkelanjutan.
   b. Menerapkan dan mendokumentasikan standar konfigurasi (*port*, protokol, *service*) untuk semua sistem, seperti *operating system*, *software*/aplikasi.
   c. Menyusun *Business Continuity Plan* dan *Disaster Recovery Plan* yang mencakup *backup* dan *restoration* dari data pribadi.
   d. Menyusun kebijakan dan implementasi dalam pelaksanaan reviu izin akses dari akun pengguna dan menerapkan *single* ID untuk otentikasi.
   e. Mengimplementasikan antivirus dan antimalware secara terpusat dan memastikan selalu update.
   f. Melakukan internal audit keamanan informasi secara berkala.
   g. Menyusun *roadmap baseline* pendidikan dan pelatihan terkait keamanan informasi bagi karyawan.
   h. Menyelenggarakan dan melakukan uji skenario penanganan insiden secara mandiri (termasuk simulasi phishing).
   i. Menyusun kebijakan mengenai pelindungan data pribadi.
   j. Melakukan risk assessment secara berkala terhadap seluruh aset TI yang dikelola dan direviu.
   k. Menyusun risk treatment dan melakukan reviu terhadap risk treatment secara berkelanjutan.
   l. Menyusun peraturan mengenai akses pengguna dan melakukan reviu izin akses dari akun pengguna secara periodik (setiap tiga bulan).
   m. Mengimplementasikan praktik secure coding untuk setiap pembangunan aplikasi.

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
   a. Melakukan pembaharuan secara berkala dalam inventarisasi data aset (perangkat keras maupun lunak), dan disusun berdasarkan klasifikasi kritikalitas serta menentukan penanggung jawab aset.
   b. Menyusun/memperbarui roadmap keamanan TI organisasi dalam jangka waktu tertentu.
   c. Melakukan risk assessment secara berkala, mereviu dan memperbarui risk register untuk seluruh aset yang dikelola serta menyusun risk treatment plan.
   d. Menerapkan system configuration management tools otomatisasi konfigurasi perangkat keras dan perangkat lunak.
   e. Menerapkan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman/standar/acuan organisasi.
   f. Menyusun Business Impact Analysis (BIA) terhadap perangkat dan aplikasi TI.
   g. Menyusun standar/pedoman/acuan untuk klasifikasi kritikalitas aset TI.

3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menyimpan data *backup* telah dilindungi secara tepat, baik secara fisik maupun non fisik pada lokasi yang aman dan terenkripsi.
   b. Menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan serta penambahan OTP untuk otentikasi pada transaksi yang berisiko tinggi.
   c. Menyusun kebijakan terkait pembatasan penggunaan scripting tools.
   d. Menonaktifkan komunikasi antar workstation untuk mencegah serangan siber.
   e. Menyusun pengaturan terkait pembatasan aplikasi yang dapat diunduh, diinstall dan dioperasikan pada perangkat milik organisasi.
   f. Melakukan pengujian data integrity secara berkala terhadap data yang dibackup.
   g. Menerapkan disable peer-to-peer pada wireless client di perangkat endpoint.
   h. Menerapkan enkripsi untuk data stakeholder/pengguna yang disimpan oleh organisasi dan enkripsi pada media penyimpanan eksternal.

i. Menerapkan SSO (Single Sign On) pada cloud organisasi.

4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menerapkan *Change Management System* untuk melakukan perubahan konfigurasi.
   b. Menyusun *escalation profile* untuk setiap *security event* yang ditemukan.
   c. Menerapkan mekanisme *monitoring* terhadap akses dan perubahan pada data *sensitive* dan pendeteksian secara otomatis apabila ada perubahan konfigurasi pada peralatan jaringan.
   d. Membentuk SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
   e. Menjalankan vulnerability scanning tools secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
   f. Menerapkan fungsi Cyber Threat Intelligence (CTI).
   g. Menyusun Metrik Security Event.
   h. Menyusun escalation profile untuk setiap security event yang ditemukan.

5. Untuk meningkatkan aspek respon, dapat dilakukan hal-hal sebagai berikut:
   a. Merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
   b. Menyusun kebijakan penanganan insiden yang selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
   c. Menyusun laporan insiden sesuai format baku, merekap laporan insiden dan melakukan reviu terhadap rekap laporan insiden secara berkala.
   d. Menerapkan mekanisme backup data karyawan ke cloud organisasi.
   e. Menyusun dokumen rencana respon insiden atau disaster recovery plan (DRP) dan menjadwalkan reviu secara berkala.
   f. Menyusun SLA (Service Level Agreement) untuk penanganan insiden.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan siber pada Pemprov Kepulauan Riau. Agar Pemprov Kepulauan Riau melaksanakan tindak lanjut atas hasil observasi dan rekomendasi yang disampaikan pada Laporan Penilaian CSM ini dan melaporkan tindak lanjutnya kepada BSSN.

Laporan Penilaian CSM ini disusun rangkap 3 (tiga) untuk disampaikan kepada :

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Kepulauan Riau; dan
3. Kepala Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau.

Tanjung Pinang, 23 Juni 2022

Kepala Bidang Statistik dan Persandian	Koordinator Kelompok Manajemen Risiko Pengukuran Tingkat Kematangan KSS Pemda
	Ditandatangani secara elektronik oleh : SANDIMAN MADYA SELAKU KOORDINATOR KELOMPOK MANRIS PTK KEAMANAN SIBER DAN SANDI SEKTOR PEMDA **Nurchaerani, S.E.** Pembina (IV/a)
(Didi Madjdi, S.E.)	(Nurhaerani, S.E.)

Mengetahui,

Direktur Keamanan Siber dan Sandi Pemda

Ditandatangani secara elektronik oleh:
DIREKTUR
KEAMANAN SIBER DAN SANDI
PEMERINTAH DAERAH
Hasto Prastowo, S.Kom.,M.M.
Pembina Utama Muda (IV/c)

(Hasto Prastowo, S.Kom.,M.M.)