2021

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI KEPULAUAN BANGKA BELITUNG

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 Bangka Belitung. 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*) pada tanggal 2 Desember 2021 kemudian dilakukan validasi pada 7 s.d. 8 Desember 2021 oleh Tim BSSN. Tim BSSN yang terlibat :

1) Marcelina Tri Nasiti Widayatmi, S.Sos.,M.Si (Han).
2) Irma Nurfitri Handayani, S.ST.
3) Ivan Bashofi, S.S.T.TP.
4) Ni Putu Ayu Lhaksmi Wulansari, S.Tr.TP.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Kepulauan Bangka Belitung

Alamat : Komplek Perkantoran Terpadu Pemprov Kepulauan Bangka Belitung, Pangkalpinang

Nomor Telp./Fax. : (0717) 4262141

Email : kominfo@babelprov.go.id

Narasumber Instansi/Lembaga :

1. Dr. Adhari, S.T.,M.E.
2. Muhammad Akbar, A.Md.
3. Alfian Zulkarnain, S.T.,M.E.
4. Riswanto, A.Md
5. Triady, S.AP.
6. Erman Arif, S.T.

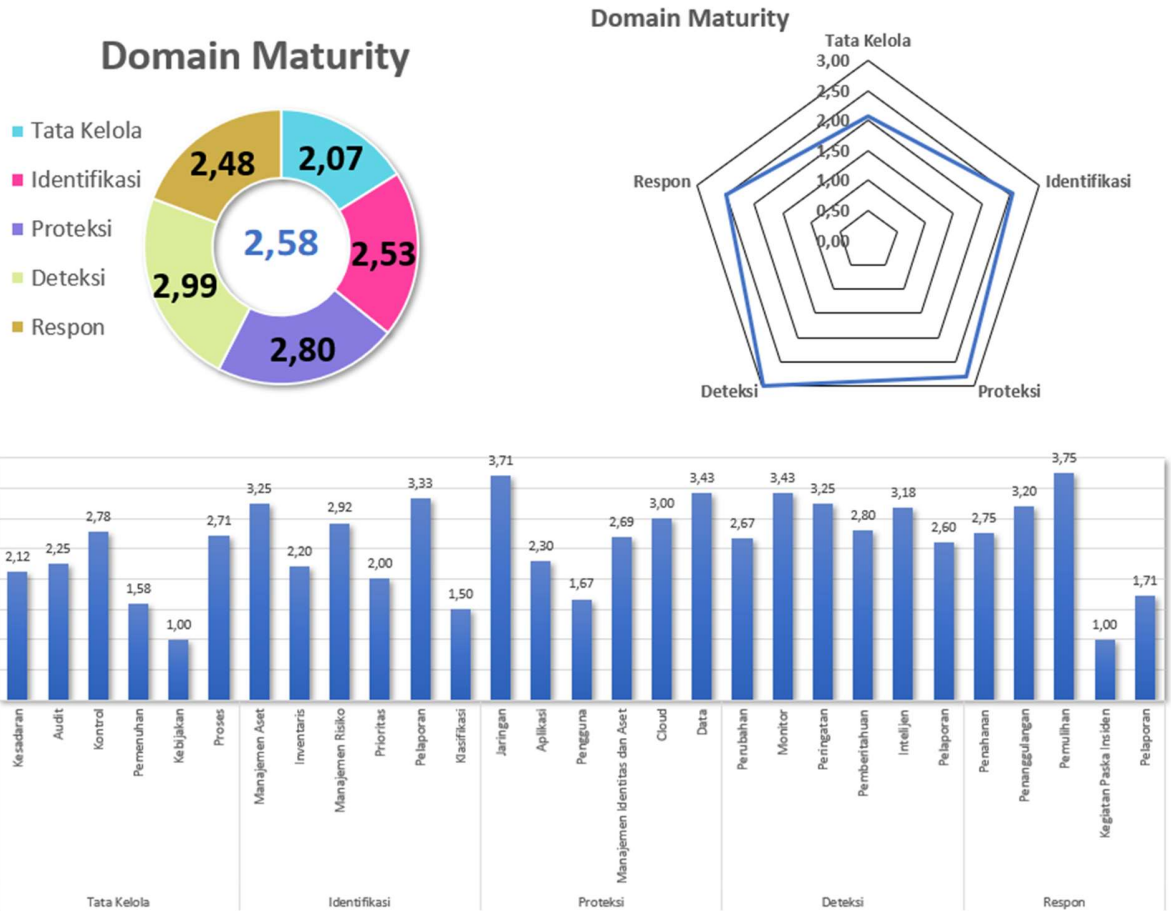
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja* : Dinas Kominfo Provinsi Kepulauan Bangka Belitung, Bidang Persandian dan Keamanan Informasi

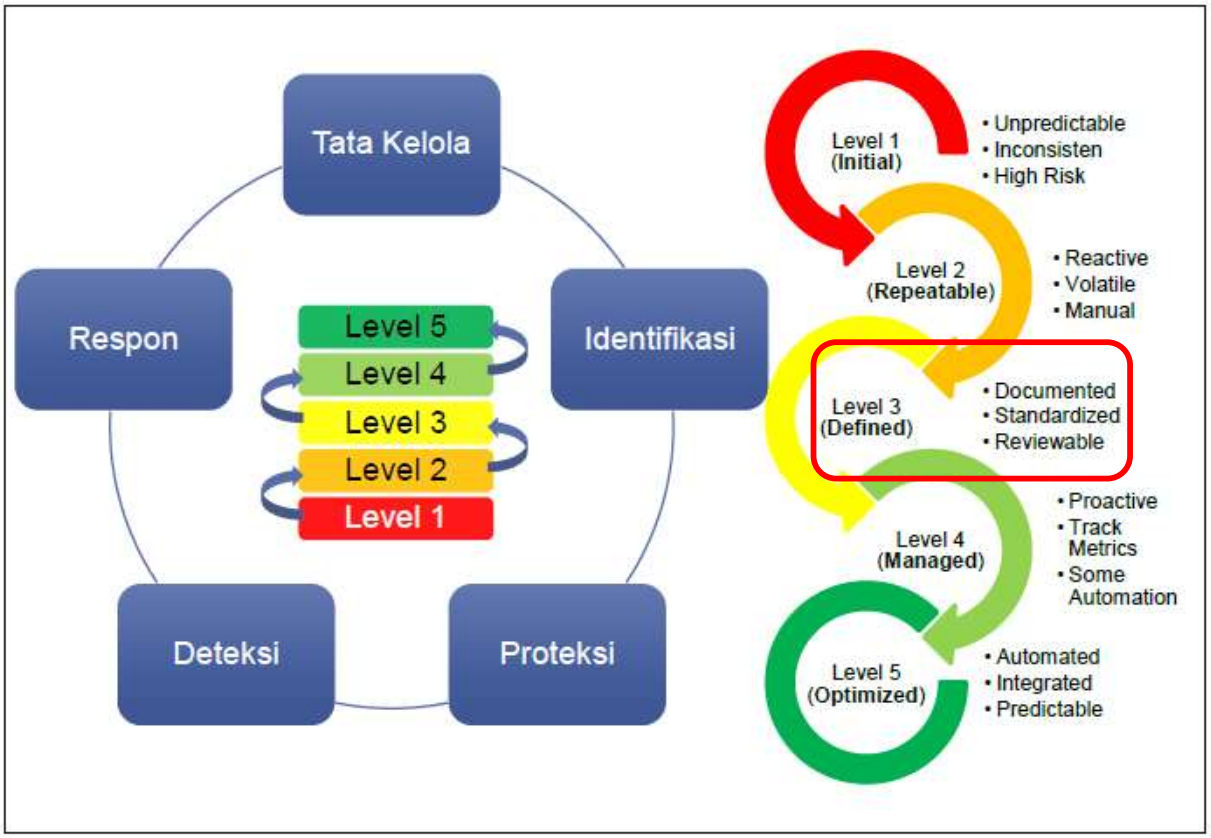
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,58,** 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 Bangka Belitung sudah terorganisir 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. Organisasi telah menerapkan manajemen kerentanan siber dan mitigasi terhadap kerentanan melalui CSIRT.

2. Organisasi sudah menerapkan pengamanan pada aplikasi web organisasi menggunakan *firewall* aplikasi web (WAFs).
3. Organisasi sudah menggunakan tool vulnerability scanning secara mandiri.
4. Personil yang terlibat dalam pengembangan software/aplikasi (telah mendapatkan pelatihan mengenai *secure code*.
5. Organisasi sudah menerapkan filterisasi terhadap seluruh jenis file lampiran email.
6. Organisasi sudah memiliki dokumentasi/diagram aliran data untuk sebagian sistem dan jaringan.
7. Organisasi sudah mendefinisikan peran dan tanggungjawab terkait keamanan informasi dan pembagian peran ke personil.
8. Organisasi melakukan *penetration testing* menggunakan pihak eksternal.
9. Dilakukan manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi router, switch dan firewall di lab/production.
10. Seluruh alamat IP internal dilindungi oleh NAT (Network Addresss Translation).

Identifikasi

1. Organisasi melakukan perencanaan kapasitas untuk memastikan bahwa pengadaan semua aset perangkat dan aplikasi dilakukan sesuai dengan kebutuhan.
2. Organisasi telah melakukan identifikasi dan inventarisasi data pada perangkat keras dan perangkat lunak.
3. Aspek keamanan mempertimbangkan kapasitas *server* dan perangkat jaringan secara menyeluruh.
4. Organisasi mempertimbangkan aspek keamanan dalam pengambilan keputusan TI.
5. Organisasi sudah menerapkan segmentasi jaringan.

Proteksi

1. Organisasi sudah memiliki IDS/IPS.
2. Sudah menerapkan *cloud system*.
3. Organisasi melindungi jaringan nirkabel dengan fitur enkripsi (password).
4. Pengaturan firewall atau ACL sudah menerapkan *implicit or explicit deny any rule*

5. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan *firewall* dan melakukan filtering pada *inbound* dan *outbound network traffic*
6. Organisasi menggunakan antivirus di semua perangkat endpoints termasuk server
7. Organisasi telah menerapkan IP reputation
8. Organisasi melakukan *backup* data dan disimpan di lokasi yang aman.

Deteksi

1. 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.
2. Organisasi sudah menerapkan *Enable Detailed Logging*.
3. Organisasi telah menerapkan SIEM (Security Information Event Monitoring).
4. 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.
5. 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.
6. Organisasi memiliki *ticketing system* dan sudah melakukan *escalation profile* untuk setiap *security event* yang ditemukan.
7. Organisasi bekerjasama dengan pihak – pihak terkait untuk memperoleh informasi dan update mengenai isu keamanan siber terkini.

Respon

1. Organisasi telah memiliki SOP dan form pelaporan penanganan insiden.
2. Organisasi mempunyai daftar kontak tim penanganan insiden internal dan eksternal.
3. Organisasi mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.

4. Organisasi memiliki peralatan sumber daya analisis insiden (daftar host, packet snifer, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat digital forensic dll)
5. Tim respon insiden memiliki kemampuan mendeteksi insiden, melakukan analisis, dan memberikan rekomendasi.
6. Organisasi sudah menerapkan mekanisme backup data pada pc/laptop karyawan ke cloud organisasi namun belum diimplementasikan oleh seluruh pegawai.
7. Tim respon insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis dalam hal ini BSSN.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum ada mekanisme atau proses pengarahan terkait keamanan informasi ke setiap karyawan baru.
2. Belum melakukan gap analisis untuk memahami *skill* dan *behavior* yang tidak dimiliki oleh pegawai, dan menggunakan informasi tersebut untuk membuat *roadmap* terkait *baseline* pendidikan dan pelatihan terkait keamanan informasi.
3. Organisasi belum menyelenggarakan pelatihan keamanan informasi secara terjadwal untuk semua pegawai.
4. Belum ada mekanisme sharing ke stakeholder/klien/konsumen/pelanggan tentang teknik atau kerentanan siber yang berkembang saat ini.
5. Organisasi tidak melakukan pemeriksaan background terhadap karyawan baru.
6. Organisasi tidak menggunakan akun khusus selain akun admin untuk melakukan vulnerability scanning.
7. Organisasi belum menerapkan manajemen risiko.
8. Belum adanya kebijakan dalam pengelolaan data stakeholder/ pegawai/ masyarakat/ pribadi.
9. Belum ada pemisahan environment antara sistem production dan development
10. Organisasi belum menerapkan software antivirus dan anti malware yang terpusat.

11. Organisasi belum menggunakan DLP (Data Loss Prevention) atau NAC (Network Access Control).
12. Organisasi belum menerapkan metode sandbox terhadap seluruh lampiran email.
13. Belum adanya penerapan kontrol kriptografi sesuai standar.
14. Organisasi belum melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi.
15. Organisasi belum memiliki kebijakan keamanan informasi yang mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.
16. Organisasi belum menyusun BCP dan DRP.

Identifikasi

1. *System configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak belum ada.
2. Identifikasi aset yang dimiliki belum disusun berdasarkan klasifikasi kritikalitas dan belum ada penetapan terkait penanggungjawab untuk setiap aset tersebut.
3. Belum ada dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
4. Belum ada kebijakan dan implementasi mengenai retensi data sensitif termasuk data stakeholder.
5. Standar terkait klasifikasi data, klasifikasi aset TI dan klasifikasi terhadap cyber threat belum disusun.
6. Dokumen risk register untuk semua aplikasi yang memproses data stakeholder belum ada.
7. *Business Impact Analysis* terhadap perangkat dan aplikasi TI belum disusun.

Proteksi

1. Perangkat jaringan belum menerapkan otentikasi terpusat.
2. Organisasi belum menerapkan *port access control* sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.

3. Organisasi belum mengatur terkait pembatasan fitur wireless, penerapan disable peer-to-peer pada wireless client, penerapan DNS filtering services dan belum ada pembatasan terkait aplikasi yang diperbolehkan untuk diunduh, diinstal dan dioperasikan.
4. Perangkat endpoints belum seluruhnya menggunakan antivirus.
5. Belum ada kebijakan terkait pembatasan penggunaan *scripting tools*.
6. Penggunaan *Multi Factor Authentication* belum diterapkan
7. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
8. Belum menerapkan IP *reputation* untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
9. Seluruh data stakeholder / klien / konsumen / pelanggan belum dienkripsi saat disimpan.

Deteksi

1. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
2. Belum memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data *sensitive*.
3. Belum melakukan *record* seperti Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.
4. Belum memiliki sistem untuk monitoring dan mencegah kehilangan data sensitif.
5. Belum ada mekanisme monitoring aktivitas pihak ketiga yang dilakukan di organisasi.
6. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
7. Organisasi belum menjalankan *vulnerability scanning tools* secara otomatis menggunakan *agent*/aplikasi yang diinstal pada *endpoint*.
8. Unit dalam organisasi belum menjalankan fungsi *Cyber Threat Intelligence* (CTI).
9. Organisasi belum memiliki *Metrik Security Event*.

Respon

1. Belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Organisasi belum melakukan reviu secara berkala terhadap dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar standar operasional prosedur (SOP) penanganan insiden.
3. Belum ada skema penilaian insiden dan prioritas berdasarkan potensial dampak.
4. Belum merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
5. Organisasi belum menerapkan mekanisme *scanning* ulang setelah dilakukan *patching* terhadap aplikasi yang ditemukan kerentanan.
6. 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 Kepulauan Bangka Belitung maka dapat dilakukan hal-hal sebagai berikut:
   a. Menerapkan manajemen risiko terhadap seluruh aset milik organisasi.
   b. Menyelenggarakan pelatihan keamanan informasi secara terjadwal untuk semua pegawai.
   c. Menyusun BCP dan DRP
   d. Membuat program atau kegiatan terkait *sharing knowledge* ke stakeholder/klien/konsumen/pelanggan tentang keamanan informasi khususnya tentang teknik atau kerentanan siber yang berkembang saat ini.
   e. Melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi.
   f. Mengimplementasi single ID yang unik untuk semua otentikasi.
   g. Menerapkan software antivirus dan anti malware yang terpusat

h. Menerapkan penggunaan akun khusus selain akun admin untuk melakukan *vulnerability scanning*.
i. Menerapkan metode sandbox terhadap seluruh lampiran email
j. Memprogramkan *threat hunting* secara berkala.
k. Menerapkan DLP (*Data Loss Prevention*) atau NAC (*Network Access Control*).

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
   a. Melakukan identifikasi aset TI yang dimiliki, menyusun menjadi sebuah dokumen yang berdasarkan klasifikasi kritikalitas dan mencantumkan penanggungjawab untuk setiap aset tersebut.
   b. Menyusun prosedur mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
   c. Menyusun kebijakan dan implementasi mengenai retensi data sensitif termasuk data stakeholder.
   d. Menyusun standar terkait klasifikasi data, klasifikasi aset TI dan klasifikasi terhadap cyber threat.
   e. Menyusun *Business Impact Analysis* terhadap perangkat dan aplikasi TI
   f. Menyusun dokumen risk register untuk seluruh aset milik organisasi
   g. 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 otentikasi terpusat pada perangkat jaringan.
   b. Menerapkan port access control sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.
   c. Menyusun kebijakan yang mengatur terkait pembatasan fitur wireless, penerapan disable peer-to-peer pada wireless client, penerapan DNS filtering services dan belum ada pembatasan terkait aplikasi yang diperbolehkan untuk diunduh, diinstal dan dioperasikan.
   d. Menerapkan penggunaan antivirus pada seluruh perangkat endpoints.

e. Menerapkan teknik kriptografi (enkripsi) untuk mengamankan data stakeholder/klien/pribadi yang disimpan.
f. Menerapkan penggunaan *Multi Factor Authentication*.
g. Menyusun kebijakan terkait pembatasan penggunaan scripting tools.
h. Menerapkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.

4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun prosedur *monitoring* terhadap akses dan perubahan pada data *sensitive*
   b. Menyusun standar operasional prosedur terkait monitoring aktivitas pihak ketiga yang dilakukan di organisasi.
   c. Menyusun *Metrik Security Event*
   d. Menerapkan *vulnerability scanning tools* secara otomatis menggunakan agent/aplikasi dan diinstal pada *endpoint*.
   e. Mengadakan atau menganggarkan pelatihan terkait *Cyber Threat Intelligence* kepada personil
5. Untuk meningkatkan aspek respon, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun kebijakan penanganan insiden.
   b. Merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
   c. Menyusun format laporan penanganan insiden dan membuat laporan penanganan insiden setiap kali terjadi insiden
   d. 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 Kepulauan Bangka Belitung, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Pangkal pinang, 8 Desember 2021

Kepala Bidang Persandian dan Keamanan Informasi	Koordinator Kelompok Pengembangan Ekosistem KSS Pemda
Ditandatangani secara elektronik oleh : KEPALA BIDANG PERSANDIAN DAN KEAMANAN INFORMASI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI KEPULAUAN BANGKA BELITUNG Adhari Pembina Tk.I/IV.b	Ditandatangani secara elektronik oleh : Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah **Marcelina Tri Nasiti Widayatmi, S.Sos., M.Si(Han)** Pembina (IV/a)
(Dr. Adhari, S.T.,M.E)	(Marcelina Tri Nasiti W., S.Sos., M.Si(Han))

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara