



2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY Maturity (CSM)

DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN,
DAN STATISTIK PROVINSI PAPUA BARAT



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 apa pun. 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, Informatika, Persandian, dan Statistik Provinsi Papua Barat pada tahun 2022. Dengan adanya perbaikan pada 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 hasil evaluasi tindak lanjut rekomendasi yang dilaksanakan meliputi ruang lingkup pemetaan kematangan keamanan siber yang 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:

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



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 %

V. Pelaksanaan Kegiatan

1. Pengisian Instrumen CSM

Pengisian Instrumen CSM dilakukan secara mandiri oleh *stakeholder* pada bulan Juli 2022.

2. Validasi Penilaian CSM

BSSN melakukan validasi pengisian instrumen CSM pada tanggal 18 - 21 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfotik Provinsi Papua Barat. Tim BSSN yang terlibat:

- 1) Nurchaerani, S.E.
- 2) Guruh Prasetyo Putro, S.ST., M.Si (Han).
- 3) Ikrima Galuh Nasucha, S.Tr.TP
- 4) Carissa Mega Yulianingrum, S.Tr.TP.



HASIL KEGIATAN

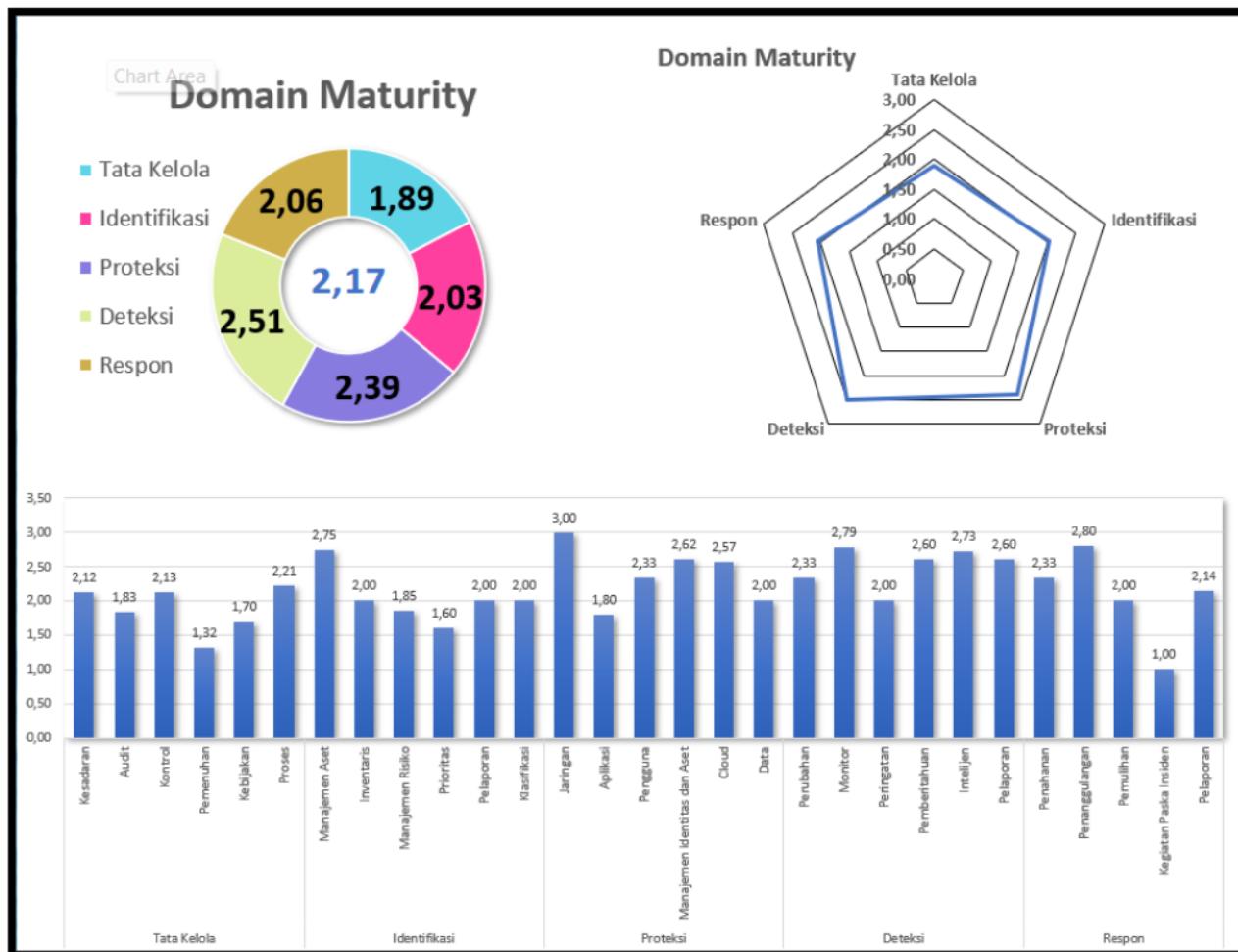
I. Deskripsi Ruang Lingkup Penilaian

Nama Instansi/Lembaga : Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat
Alamat : Jl. Abraham Atururi (Komplek Perkantoran Arfai)
Kabupaten Manokwari, Papua Barat 98315
Nomor Telp./Fax. : 082239048229
Email : diskominfo_persandian@papuabaratprov.go.id
Narasumber Instansi/Lembaga :
1) Zaenal Fanumbi, S.T.
2) Gusthyni Payuk, S.T., M.Si.
3) Yuliana Moututi, S.H.
4) Ahmad Ismail Samad, S.Kom.
5) Indra Arif Budi Sulistiawan, S.T.
6) Oktofianus R. Manupapami

II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :
 Organisasi Keseluruhan Regional, Kanwil, Cabang Unit Kerja Lainnya
2. Instansi/Unit Kerja* : Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat

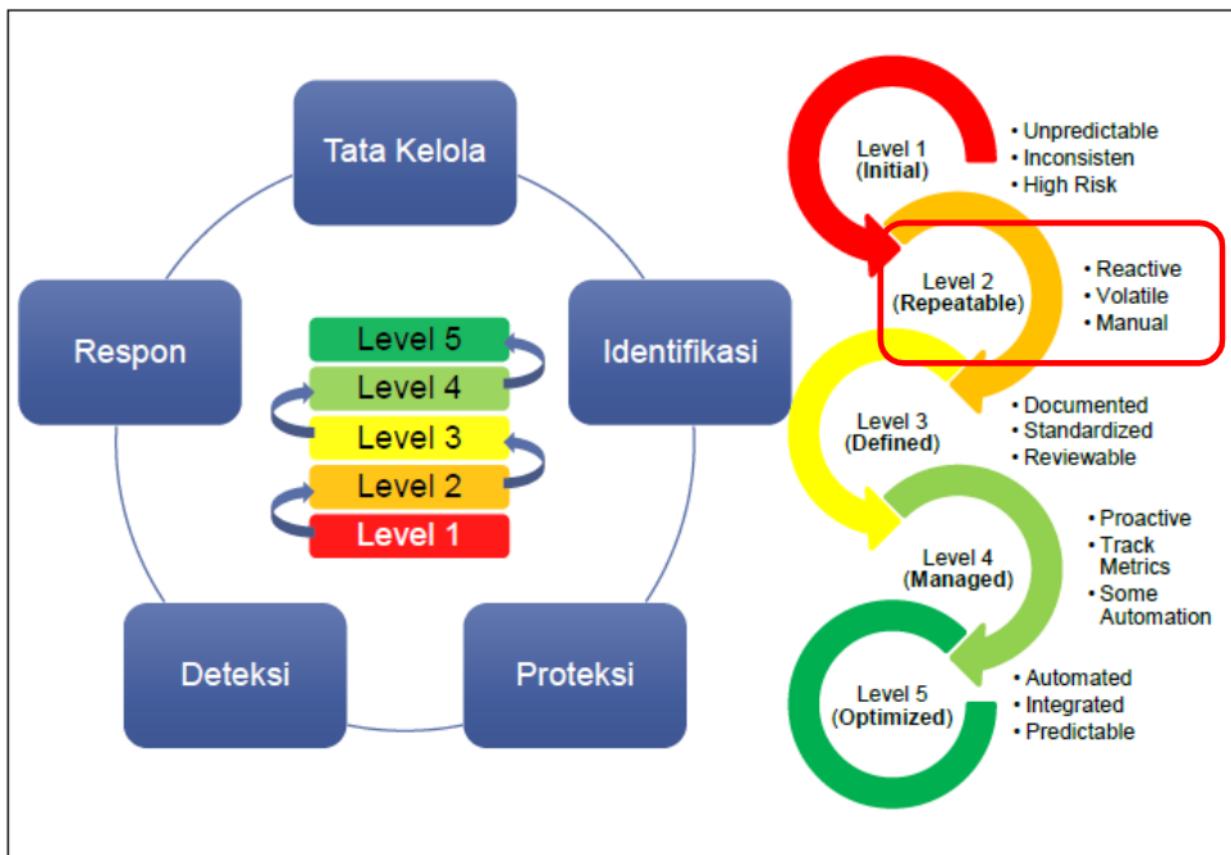
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,17**, sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :





Gambar 2. Capaian Level Kematangan

Level Kematangan 2:

Level kematangan 2 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat sudah terorganisir, bersifat informal, dilakukan secara berulang namun belum konsisten, penerapan perubahan belum dilakukan secara berkelanjutan, serta belum terukur dengan baik.



IV. Kekuatan/Kematangan

Tata Kelola

1. Diskominfoperstatik Provinsi Papua Barat memiliki program pemahaman kesadaran keamanan informasi yang telah dilakukan berupa sosialisasi peraturan yang ada untuk diketahui oleh seluruh kab/kota maupun OPD secara berkelanjutan setidaknya setahun sekali.
2. Telah melakukan pelatihan berupa bimbingan teknis terkait keamanan informasi ke sebagian besar karyawan.
3. Melakukan pemeriksaan *background* untuk semua karyawan baru.
4. Semua tanggungjawab keamanan informasi telah ditentukan dan dialokasi oleh organisasi.
5. Melakukan kerjasama dengan pihak ketiga yang tepercaya dalam pengembangan software oleh organisasi.
6. Sudah mengimplementasikan *software anti virus* dan *anti malware*, tetapi belum selalu *update*.
7. Diagram yang menggambarkan aliran data di seluruh sistem jaringan telah didokumentasikan.
8. Telah menerapkan standar konfigurasi (*port*, protokol, *service*), tetapi belum didokumentasikan.
9. Aplikasi web organisasi telah dilindungi menggunakan *firewall* aplikasi web (WAFs).

Identifikasi

1. Melakukan inventarisasi data yang ada pada semua aset, kecuali aset yang tidak berwujud seperti perangkat lunak.
2. Melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi.



3. Terdapat kebijakan dan implementasi mengenai retensi data sensitif termasuk data stakeholder / klien / konsumen / pelanggan di organisasi, namun tidak direviu.
4. Melakukan segmentasi jaringan berdasarkan fungsionalitas dengan kontrol keamanan antar segmen.

Proteksi

1. Sudah memiliki IDS/IPS.
2. Koneksi ke perangkat *server* dan jaringan di organisasi menggunakan protokol terenkripsi.
3. Penggunaan *firewall* telah dikonfigurasi seperti *implicit* atau *explicit deny any/any rule, inbound* dan *outbound network traffic*.
4. Menerapkan DNS *Filtering*.
5. Semua perangkat *endpoints* termasuk *server* menggunakan *anti virus*.
6. Melakukan penerapan *Multi-Factor Authentication* (MFA) yang digunakan untuk salah satu aplikasi.
7. Dapat melacak dan dapat mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun stakeholder.
8. *Critical system clocks* telah disinkronkan dengan metode otomatis seperti *Network Time Protocol*.

Deteksi

1. Sudah menerapkan monitoring (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan.
2. Menerapkan SIEM atau *Log Analytic Tools* untuk keperluan dokumentasi, korelasi, dan analisis *log*.
3. Dapat mendeteksi kegagalan *login* pada akun admin pada perangkat jaringan, server, dan aplikasi tanpa notifikasi otomatis.



4. Organisasi dapat mendeteksi aktivitas anomali *login* seperti waktu, lokasi, durasi.
5. Memiliki sistem untuk mendeteksi adanya *malicious code*.

Respon

1. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden.
2. Mempunyai daftar kontak tim penanganan insiden internal dan eksternal yang dapat dihubungi pada saat terjadi insiden.
3. Tim respon insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis.
4. Memiliki sumber daya redundan yang dapat langsung digunakan pada sistem penting/kritis yang down karena insiden siber.
5. Laporan insiden di organisasi dilaporkan ke top management dan ke pihak eksternal yang berkepentingan.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan secara berkelanjutan.
2. Belum melakukan simulasi *phising* setidaknya setiap tahun.
3. Belum menggunakan *tools vulnerability scanning* sebagai titik awal dalam melakukan *penetrating testing* secara rutin.
4. Belum memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi dan dilakukan proses reviu secara berkala.
5. Belum melakukan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.



6. Belum menetapkan program untuk *vulnerability assessment* atau *penetrating testing* pada aplikasi web, aplikasi *client-based*, aplikasi *mobile*, *wireless*, *server* dan perangkat jaringan.
7. Belum membentuk *Red Team* dan *Blue Team* serta belum melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.
8. Belum dilakukan pemisahan *environment* antara sistem *production* dan *development* dan mengizinkan akses kepada pengembang.
9. Belum ada kegiatan penelusuran yang memastikan bahwa data *stakeholder* yang disimpan adalah data yang akurat.
10. Belum memiliki *risk register* terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
11. Belum melakukan reviu *security risk assessment* dan *treatment*.
12. Belum dilakukan filterisasi terhadap seluruh jenis *file* lampiran *email*.
13. Peraturan, persyaratan kontrak, dan peraturan lainnya belum diidentifikasi dan didokumentasi.
14. Belum menerapkan kontrol kriptografi sesuai dengan peraturan yang berlaku.
15. Organisasi belum menerapkan praktik *secure coding* yang sesuai dengan bahasa pemrograman dan *development environment* yang digunakan.
16. *Source code* yang dibuat secara mandiri tidak dilakukan reviu kerentanannya terlebih dahulu oleh *developer* internal menggunakan teknis otomatis dan manual sebelum masuk ke *production*.
17. Belum terdapat prosedur otorisasi/ persetujuan untuk menambah/ mengubah/ menghapus hak akses ketika terjadi perpindahan karyawan.
18. Belum melakukan kegiatan pengukuran tingkat kepatuhan pengguna dalam implementasi kebijakan keamanan informasi.
19. Belum terdapat dokumen BCP dan DRP.



20. Belum mempunyai kebijakan yang menetapkan sanksi yang dijatuhkan saat terdapat pelanggaran dalam hal keamanan siber.
21. Belum memiliki kebijakan keamanan informasi mengatur mengenai *single ID* yang unik untuk melakukan semua otentifikasi.

Identifikasi

1. Aset yang diidentifikasi belum disusun berdasarkan klasifikasi kritikalitas (berdasarkan analisis risiko operasional, analisis bisnis, dan analisis strategis organisasi) serta belum ditetapkan penanggung jawab untuk setiap aset tersebut.
2. Belum terdapat kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
3. Belum terdapat dokumentasi alur informasi yang memproses data *stakeholder* termasuk yang dikelola pihak ketiga.
4. Belum memiliki kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
5. Belum memiliki *risk register* yang terdokumentasi untuk semua aplikasi yang memproses data stakeholder.
6. Belum memiliki *bussines impact analysis* terhadap perangkat dan aplikasi TI dan direviu secara berkala.
7. Organisasi tidak memiliki standar untuk klasifikasi aset TI.

Proteksi

1. *Email system* di organisasi (termasuk yang ada di *cloud*) belum memiliki pengecekan otomatis terhadap *spam/ phishing/ malware*.
2. Organisasi tidak membatasi aplikasi yang diunduh, diinstal, dan dioperasikan.
3. Belum menerapkan pengaturan akses (*read/write*) terhadap perangkat USB/media penyimpanan eksternal.



4. Belum memastikan penggunaan *password* yang kompleks untuk semua akses *login*.
5. Belum menambahkan verifikasi *On Time Password* (OTP) melalui SMS, whatsapp messenger, telepon, elektronik *mail*, *google authenticator*, atau media lainnya untuk transaksi yang berisiko tinggi.
6. Belum menerapkan *single sign-on* pada layanan *cloud*, karena belum memiliki *cloud* organisasi.
7. Belum semua data stakeholder dienkripsi saat disimpan.

Deteksi

1. Semua perubahan konfigurasi belum melalui proses *change management system* dan tidak dilakukan reviu secara berkelanjutan.
2. Setiap orang yang tergabung dalam tim *monitoring* pada organisasi belum mendapatkan peningkatan keterampilan.
3. Melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi namun ketika diketahui ada masalah.
4. Belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data *stakeholder*.
5. Belum melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan *data center (server)* untuk mendeteksi potensi kejadian keamanan siber.
6. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
7. Belum menjalankan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber menggunakan *agent/aplikasi* yang diinstal pada *endpoint*.



Respon

1. Belum terdapat dokumen rencana respon insiden atau *disaster recovery plan* (DRP).
2. Belum memberikan pelatihan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi untuk seluruh karyawan.
3. Belum melakukan perencanaan skenario penanganan insiden secara rutin kepada karyawan pengelola TI.
4. Belum memiliki *cloud* untuk menyimpan atau *backup data* karyawan.
5. Belum mendesain jaringan yang dapat memastikan apabila *server* DMZ terkena serangan siber, penyerang tidak dapat mengakses *server* yang lain.
6. Setelah ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*, belum dilakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup.
7. Tim respon insiden di organisasi belum melakukan pencatatan setiap langkah yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku (telah ditetapkan oleh organisasi).
8. Belum merancang standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.
9. Belum melakukan reviu terhadap rekap laporan siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan.



VI. Rekomendasi

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), disampaikan beberapa rekomendasi yang dapat dilakukan dalam rangka peningkatan kematangan siber pada Dinas Komunikasi, Informatika, Persandian, & Statistik Provinsi Papua Barat sebagai berikut:

1. Untuk meningkatkan aspek tata kelola, organisasi diharapkan:
 - a. Menerapkan manajemen risiko terhadap seluruh aset milik organisasi.
 - b. Menyusun dokumen BCP dan DRP.
 - c. Menyusun kebijakan untuk penerapan perlindungan data pribadi dan direview secara berkala.
 - d. Menyusun kebijakan keamanan informasi yang telah disetujui manajemen serta dikomunikasikan kepada karyawan dan pihak eksternal terkait dan dikembangkan sesuai dengan kerangka kerja dan standar yang diakui khususnya terkait dengan penerapan kriptografi, mekanisme penghapusan data, dan pengendalian terhadap aset informasi.
 - e. Menyusun kebijakan keamanan informasi mengatur mengenai *single ID* yang unik untuk melakukan semua otentikasi.
 - f. Menyusun prosedur otorisasi/ persetujuan untuk menambah/ mengubah/ menghapus hak akses ketika terjadi perpindahan karyawan.
2. Aspek Identifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
 - a. Menyusun *business impact analysis* terhadap perangkat dan aplikasi TI berdasarkan aspek kerahasiaan, keutuhan, ketersediaan, otentikasi dan anti penyangkalan sehingga dapat dirumuskan prioritas penanganan risiko.
 - b. Menyusun dokumen *risk register* untuk seluruh aset milik organisasi dan semua aplikasi yang memproses data *stakeholder* sesuai dengan kerangka kerja dan standar yang diakui dengan memetakan terkait aset, kerentanan,



- ancaman, kemungkinan, dampak, level risiko, proses mitigasi, dan penanggungjawab.
- c. Menyusun kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
 - d. Menyusun metode/standar untuk klasifikasi aset TI dan direviu secara berkala.
3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
- a. Menerapkan penggunaan *multi factor authentication* pada semua akses jaringan dan akses data sensitif.
 - b. Menerapkan otentikasi terpusat pada semua perangkat jaringan.
 - c. Membuat *cloud* organisasi dengan menerapkan *single sign-on*.
 - d. Memastikan penggunaan *password* yang kompleks untuk semua akses *login*.
 - e. Menerapkan enkripsi pada semua data *stakeholder* saat disimpan.
4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
- a. Melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan *data center (server)* untuk mendeteksi potensi kejadian keamanan siber.
 - b. Diharapkan setiap orang yang tergabung dalam tim *monitoring* pada organisasi mendapatkan peningkatan keterampilan.
 - c. Menerapkan *change management system* untuk semua perubahan konfigurasi dan dilakukan reviu secara berkelanjutan.
 - d. Melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi selama 24 jam sehari.
 - e. Memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
 - f. Menerapkan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber menggunakan agent/aplikasi yang diinstal pada *endpoint*.



5. Aspek Respon ditingkatkan dengan cara:

- a. Menyusun dokumen rencana respon insiden atau *disaster recovery plan* (DRP).
- b. Melakukan peningkatan kapasitas SDM terutama terkait dengan pengujian keamanan, mekanisme proteksi dan penanganan suatu insiden.
- c. Menetapkan format baku dalam melakukan dokumentasi penanganan insiden keamanan siber.
- d. Melakukan perencanaan skenario penanganan insiden secara rutin kepada karyawan pengelola TI.
- e. Melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi.
- f. Menyusun standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.



PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Papua Barat. Agar Pemerintah Daerah Provinsi Papua Barat 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 disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Papua Barat; dan
3. Sekretaris Daerah Provinsi Papua Barat.

Manokwari, 22 Juli 2022

Kepala Bidang Persandian
dan Statistik


Zaenal Fanumbi, S.T.
19810621 200909 1 002

Sandiman Madya pada Direktorat
Keamanan Siber dan Sandi Pemerintah
Daerah


Nurchaerani, S.E.
19650708 198710 2 003

Mengetahui,
Kepala Diskominfo Persandian dan Statistik
Provinsi Papua Barat

