2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN, DAN STATISTIK PROVINSI SULAWESI 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 Sulawesi 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:

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

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 bulan Juli 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 1 – 5 Agustus 2022, dengan cara diskusi dengan perwakilan tim Diskominfotik Provinsi Sulawesi Barat. Tim BSSN yang terlibat:

   1) Dwi Kardono, S.Sos., M.A.
   2) Aris Munandar, S.S.T.MP
   3) Ivan Bashofi, S.S.T.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 Sulawesi Barat

Alamat : Kompleks Perkantoran Gubernur Sulawesi Barat Jln. H. Abd. Malik Pattana Endeng, Rangas - Mamuju Sulawesi Barat 91512

Nomor Telp./Fax. : -

Email : kominfo@sulbarprov.go.id

Pimpinan Instansi : Mustari Mula, S.Sos., M.A.P.

Narasumber Instansi :

1) Abdul Azis, S.Pd., M.M.
2) Wahida Yusuf, S.IP.
3) Taufan Harry Prasetyo, SE.M.Ec.Dev., M.Kom.
4) Madhur, ST.
5) Sudarmono, S.IP.

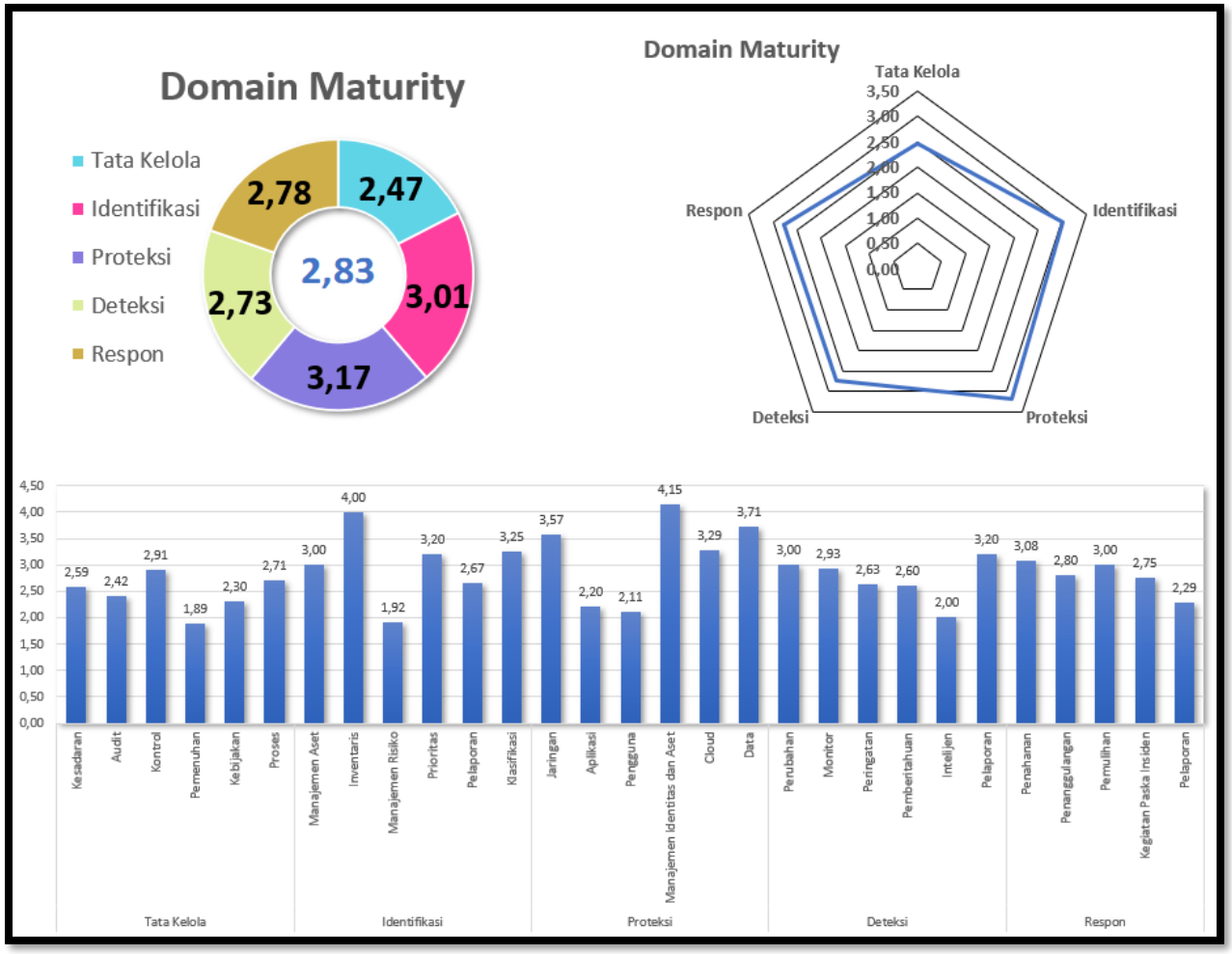
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja* : Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Sulawesi Barat

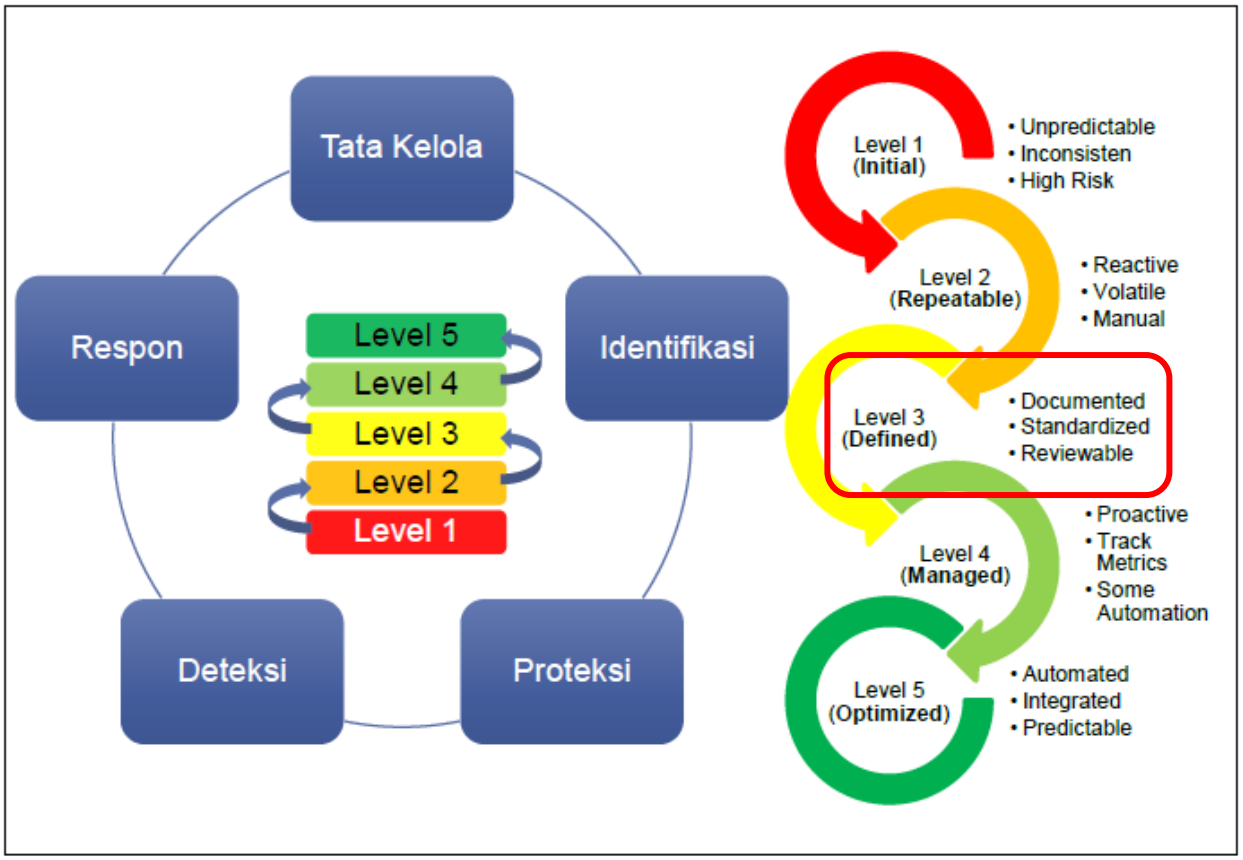
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,83**, 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, Informatika, Persandian, dan Statistik Provinsi Sulawesi Barat sudah sudah terorganisir dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan.

Catatan:

Berdasarkan hasil penilaian CSM yang telah dilakukan pada tahun 2020 dengan total skor indeks kematangan adalah 2,51, terdapat kenaikan 0,32 poin menjadi 2,83 dengan kategori level yaitu level 3.

IV. Kekuatan/Kematangan

Tata Kelola

1. Program untuk *vulnerability assessment* atau *penetrating testing* pada aplikasi web, aplikasi *client-based*, aplikasi *mobile*, *wireless*, *server* dan perangkat, jaringan telah dilaksanakan setidaknya 1 tahun sekali.
2. Dilakukan pemisahan *environment* antara sistem *production* dan *development* dan tidak mengizinkan akses kepada pengembang tanpa pengawasan dari bagian keamanan organisasi.
3. Aplikasi web organisasi telah dilindungi menggunakan *firewall* aplikasi web (WAFs).
4. Penggunaan IDS telah diterapkan untuk jaringan internal.
5. Sudah mengimplementasikan *software anti virus* dan *anti malware* secara terpusat.
6. Sudah melakukan *penetrating testing* menggunakan pihak eksternal dan internal secara berkala.

Identifikasi

1. Telah melakukan inventarisasi data yang ada pada semua perangkat keras dan perangkat lunak.
2. Melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi.
3. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
4. Melakukan segmentasi jaringan berdasarkan fungsionalitas dengan kontrol keamanan antar segmen.

Proteksi

1. Koneksi ke perangkat *server* dan jaringan di organisasi menggunakan protokol terenkripsi.
2. Penggunaan *firewall* telah dikonfigurasi dengan baik seperti *implicit* atau *explicit deny any/any rule*, *inbound* dan *outbound network traffic*.
3. Menerapkan DNS *Filtering*.
4. *Email system* di organisasi (termasuk yang ada di *cloud*) memiliki pengecekan otomatis terhadap *spam*/ *phishing*/ *malware*.
5. Semua perangkat *endpoints* termasuk *server* menggunakan *anti virus*.
6. Sudah menerapkan *Multi-Factor Authentication* (MFA) yang digunakan untuk semua akses jaringan VPN dan mengakses data sensitif.
7. Akses ke data *stakeholder* diatur dengan hak akses.
8. Dapat melacak dan dapat mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun *stakeholder*.
9. Semua data penting di organisasi Anda di-*backup* secara berkala.
10. *Critical system clocks* telah disinkronkan dengan metode otomatis seperti *Network Time Protocol*.

Deteksi

1. Perubahan konfigurasi pada peralatan jaringan terdeteksi secara otomatis.
2. Sudah menerapkan *monitoring* (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan secara manual.
3. Dapat mendeteksi *Wireless Access Point* yang terhubung ke jaringan LAN (*ethernet*).
4. Setiap orang yang tergabung dalam tim *monitoring* pada organisasi mendapatkan peningkatan keterampilan, akan tetapi tidak setiap tahun.
5. Aktivitas pihak ketiga dipantau untuk mendeteksi adanya potensi kejadian keamanan siber.

6. Memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
7. Dapat mendeteksi kegagalan *login* pada akun admin pada perangkat jaringan, server, dan aplikasi.
8. Organisasi dapat mendeteksi aktivitas anomali *login* seperti waktu, lokasi, durasi.
9. Organisasi menyimpan semua *log* terhadap URL yang diakses oleh karyawan.

Respon

1. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden.
2. Mempunyai daftar kontak tim penanganan insiden internal dan eksternal (misalnya penegak hukum, ambulance, pemadam kebakaran, dll) yang dapat dihubungi pada saat terjadi insiden.
3. Jika terdapat laporan terjadinya infeksi *malware*, membutuhkan waktu 10 menit saja untuk melakukan diskoneksi segmen jaringan untuk mencegah penyebaran *malware*.
4. Sudah mendesain jaringan yang dapat memastikan apabila *server* DMZ terkena serangan siber, penyerang tidak dapat mengakses *server* yang lain.
5. Melakukan *backup data* yang ada di pc/laptop karyawan ke *cloud* organisasi.
6. Setelah ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*, dilakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup.
7. Jika terjadi insiden siber di organisasi Anda yang menyebabkan *server down*/tidak berfungsi, organisasi dapat memastikan *server* dari *backup* dapat digunakan dalam kurun waktu kurang dari 3 jam.

V. Kelemahan/Kekurangan

Tata Kelola

1. Program pengarahan dan pemahaman kesadaran keamanan informasi telah dilakukan namun belum secara berkelanjutan untuk diketahui oleh seluruh karyawan.
2. Pelatihan terkait keamanan informasi seperti penggunaan *secure authentication*, identifikasi serangan *social engineering*, membuat *secure code* masih dilakukan sebagian kecil pegawai dan tidak terjadwal rutin.
3. Belum melakukan simulasi *phising* setidaknya setiap tahun.
4. Belum memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi dan dilakukan proses reviu secara berkala.
5. 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.
6. Belum memiliki *risk register* terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
7. Belum terdapat dokumen *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP), khususnya yang mencakup *backup* dan *restoration* dari data pribadi.
8. Belum memiliki kebijakan keamanan informasi mengatur mengenai *single* ID yang unik untuk melakukan semua otentikasi.
9. Belum melakukan *threat hunting* secara berkala.

Identifikasi

1. Belum mendokumentasikan proses dan prosedur untuk manajemen *patch* semua aset perangkat dan aplikasi.

2. Belum terdapat kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
3. Belum memiliki *risk register* yang terdokumentasi untuk semua aplikasi yang memproses data *stakeholder*.
4. Belum memiliki *Bussines Impact Analysis* terhadap perangkat dan aplikasi TI dan direviu secara berkala.

Proteksi

1. Belum memiliki IPS.
2. Belum semua perangkat jaringan menggunakan otentikasi terpusat.
3. Organisasi belum menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu serta tidak membatasi aplikasi yang diunduh, diinstal, dan dioperasikan.
4. Belum menambahkan verifikasi *On Time Password* (OTP) melalui SMS, WhatsApp *Messenger*, Telepon, Elektronik *Mail*, *Google Authenticator*, atau media lainnya untuk transaksi yang berisiko tinggi.
5. Belum menerapkan *single sign-on* pada layanan *cloud*.
6. Belum semua data *stakeholder* dienkripsi saat disimpan dan dikirim.

Deteksi

1. Semua perubahan konfigurasi belum melalui proses *change management system* dan tidak dilakukan reviu secara berkelanjutan.
2. Belum ada mekanisme *monitoring* terhadap akses dan perubahan pada data sensitif.
3. Melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi namun ketika diketahui ada masalah.
4. Belum memiliki sistem untuk me*monitoring* dan mencegah kehilangan data sensitif termasuk data *stakeholder*.

5. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
6. Belum terdapat unit yang berfungsi untuk melakukan *Cyber Threat Intelligence* (CTI).

Respon

1. Belum memiliki *disaster recovery plan* (DRP) dan melakukan reviu secara berkala terhadap dokumen rencana respon insiden.
2. Belum memberikan pelatihan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi untuk seluruh karyawan secara rutin.
3. Melakukan perencanaan skenario penanganan insiden kepada karyawan pengelola TI tetapi tidak secara rutin.
4. Tim respon insiden siber di organisasi belum memiliki peralatan sumber daya analisis insiden.
5. Tim respon insiden di organisasi belum melakukan pencatatan setiap langkah yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku (telah ditetapkan oleh organisasi).
6. 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.
7. Laporan insiden di organisasi belum dilaporkan sampai ke *top management* dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi.

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 Sulawesi Barat sebagai berikut:

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
    a. Menyusun program pemahaman kesadaran keamanan informasi yang dilakukan secara berkelanjutan.
    b. Mengusulkan pemberian pelatihan terkait keamanan informasi kepada pegawai secara rutin setidaknya setahun sekali.
    c. Menerapkan manajemen risiko terhadap seluruh aset milik organisasi dengan membuat *risk register* terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
    d. Menyusun dokumen dokumen *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP).
    e. Melakukan simulasi *phising* setidaknya setiap tahun.
    f. Menyusun kebijakan untuk penerapan perlindungan data pribadi dan direviu secara berkala.
    g. 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.
    h. Menyusun kebijakan keamanan informasi mengatur mengenai *single* ID yang unik untuk melakukan semua otentikasi.
    i. Melakukan *threat hunting* secara berkala.

2. Aspek Identifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
    a. 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.
    b. Menyusun *Business Impact Analysis* terhadap perangkat dan aplikasi TI berdasarkan aspek kerahasiaan, keutuhan, ketersediaan, otentikasi dan anti penyangkalan sehingga dapat dirumuskan prioritas penanganan risiko.
    c. Menyusun kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
    d. Menyusun proses dan prosedur manajemen *patch* untuk semua aset perangkat dan aplikasi.

3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
    a. Pertimbangan untuk menggunakan IPS.
    b. Menerapkan otentikasi terpusat pada semua perangkat jaringan.
    c. Menerapkan *single sign-on* pada *cloud* organisasi.
    d. Menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu serta membatasi aplikasi yang diunduh, diinstal, dan dioperasikan.
    e. Menambahkan verifikasi *On Time Password* (OTP) melalui SMS, WhatsApp *Messenger*, Telepon, Elektronik *Mail*, *Google Authenticator*, atau media lainnya untuk transaksi yang berisiko tinggi.
    f. Menerapkan enkripsi pada semua data *stakeholder* saat disimpan dan dikirim.

4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
    a. Menerapkan *change management system* semua untuk semua perubahan konfigurasi dan dilakukan reviu secara berkelanjutan.
    b. Menyusun mekanisme *monitoring* terhadap akses dan perubahan pada data sensitif.
    c. Melakukan *monitoring* terhadap log dari perangkat *security control*, jaringan, dan aplikasi selama 24 jam sehari.
    d. Pertimbangan memiliki sistem untuk me*monitoring* dan mencegah kehilangan data sensitif termasuk data *stakeholder* seperti penggunaan DLP (*Data Loss Prevention*).
    e. Pertimbangan terdapat unit manajemen teknis atau SOC yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
    f. Pertimbangan terdapat unit yang berfungsi untuk melakukan *Cyber Threat Intelligence* (CTI).

5. Aspek Respon ditingkatkan dengan cara:
    a. Melakukan reviu secara berkala terhadap dokumen rencana respon insiden.
    b. Melakukan peningkatan kapasitas SDM terutama terkait dengan pengujian keamanan, mekanisme proteksi, mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
    c. Melakukan perencanaan skenario penanganan insiden kepada karyawan pengelola TI secara rutin.
    d. Menyediakan peralatan sumber daya analisis insiden misalnya daftar host, packet snifer, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat digital forensic untuk digunakan oleh tim respon insiden.

e. Menetapkan format baku dalam melakukan dokumentasi penanganan insiden keamanan siber dengan mencatat setiap langkah yang dilakukan dalam rangka penanggulangan insiden.

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.

g. Melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi serta laporan insiden dilaporkan sampai ke *top management* dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Sulawesi Barat ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Sulawesi Barat. Agar Pemerintah Daerah Provinsi Sulawesi 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 Sulawesi Barat;
3. Kepala Dinas Kominfo Persandian dan Statistik Provinsi Sulawesi Barat; dan
4. Direktur Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III, BSSN.

Mamuju, 3 Agustus 2022

Kepala Bidang TIK, Persandian dan Statistik	Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemda
Abdul Azis, S.Pd., M.M.	Dwi Kardono, S.Sos., M.A.
19700509 199501 1 001	19710218 199110 1 001