



2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY Maturity (CSM)

DINAS KOMUNIKASI INFORMATIKA STATISTIK DAN
PERSANDIAN PROVINSI SULAWESI 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, Informatika, Statistik dan Persandian Provinsi Sulawesi 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 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:



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 Juni 2022.

2. Validasi Penilaian CSM

BSSN melakukan validasi pengisian instrumen CSM pada tanggal 14 s.d. 15 Juni 2022, dengan cara diskusi dengan perwakilan tim Diskominfo-SP Provinsi Sulawesi Selatan. Tim BSSN yang terlibat:

- 1) Lukman Nul Hakim, S.E.,M.M.
- 2) Diah Sulistyowati, S.Kom.
- 3) Mochamad Jazuly, S.S.T.TP.
- 4) Ni Putu Ayu Lhaksmi W.,S.Tr.TP.



HASIL KEGIATAN

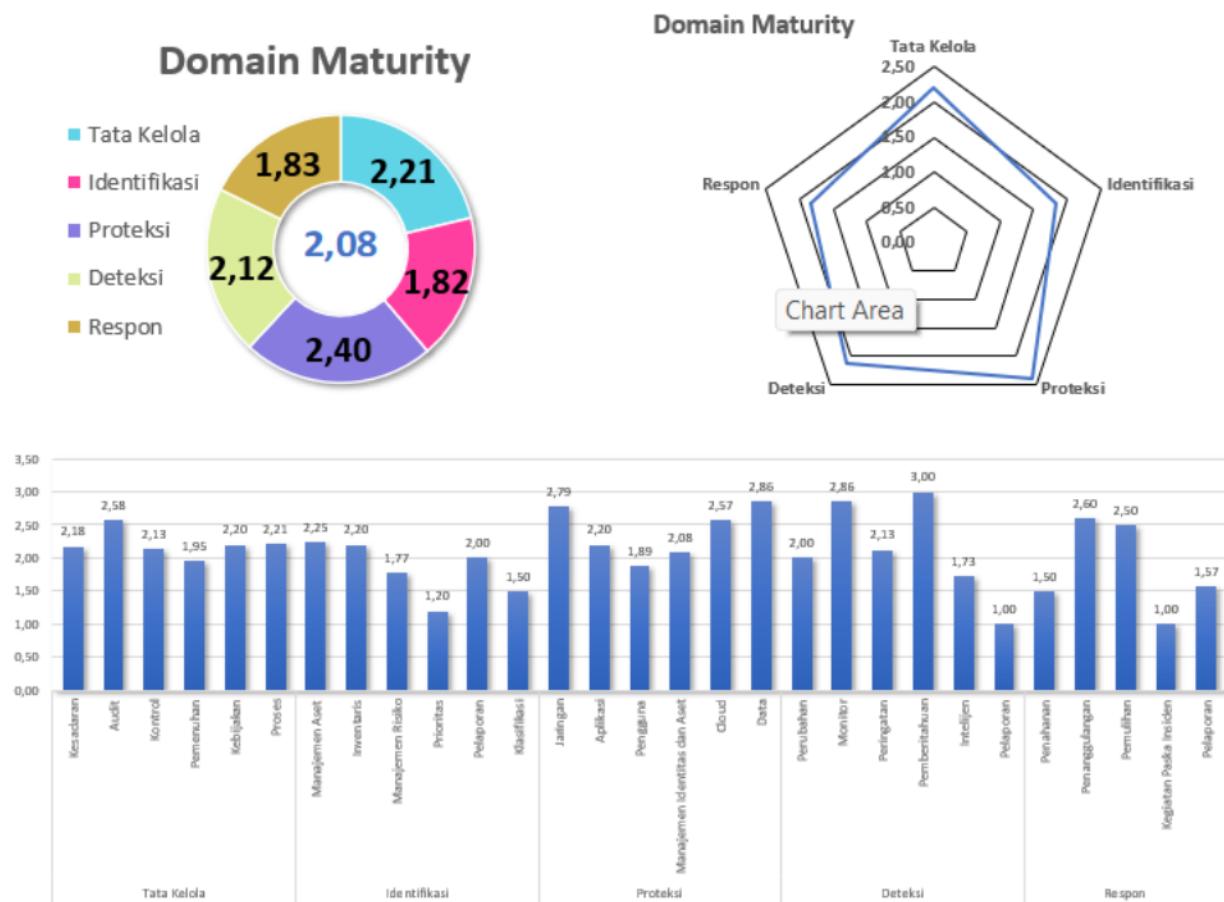
I. Informasi Stakeholder

Nama Instansi/Lembaga : Dinas Komunikasi Informatika Statistik dan Persandian Provinsi Sulawesi Tengah
Alamat : Jl. Urip Sumoharjo No.269, Makassar, Sulsel
Nomor Telp./Fax. : (0441) 453203
Email : persandian.dkisp@sulselprov.go.id
Narasumber Instansi/Lembaga :
1. Riswan, S.Sos., M.M. (Kepala Bidang Persandian)
2. Irvan, S.STP.,M.Adm.,SDA (Kepala Bidang Aptika)
3. Suriany, S.H. (Fungsional Manggala Informatika Ahli Madya)
4. Hasanuddin, S.Kom. (Fungsional Manggala Informatika Ahli Muda)
5. Muhammad Danial Rapi, S.Kom. (Fungsional Pranata Komputer Ahli Muda)
6. Mohammad Rizki Soetrisno,S.T.,M.T. (Fungsional Pranata Komputer Ahli Muda)
7. Andi Paisal, S.Sos. (Fungsional Pranata Komputer Ahli Muda)
8. Ahmad Tasyrif Arief,S.T.,MT (Fungsional Sandiman Pertama)
9. A.Achmad Paulangi, S.Sos, M.M (Fungsional Sandiman Pertama)
10.Putrawal Daha, S.Kom. (Tim IT Bidang Aptika)

II. Deskripsi Ruang Lingkup Penilaian

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

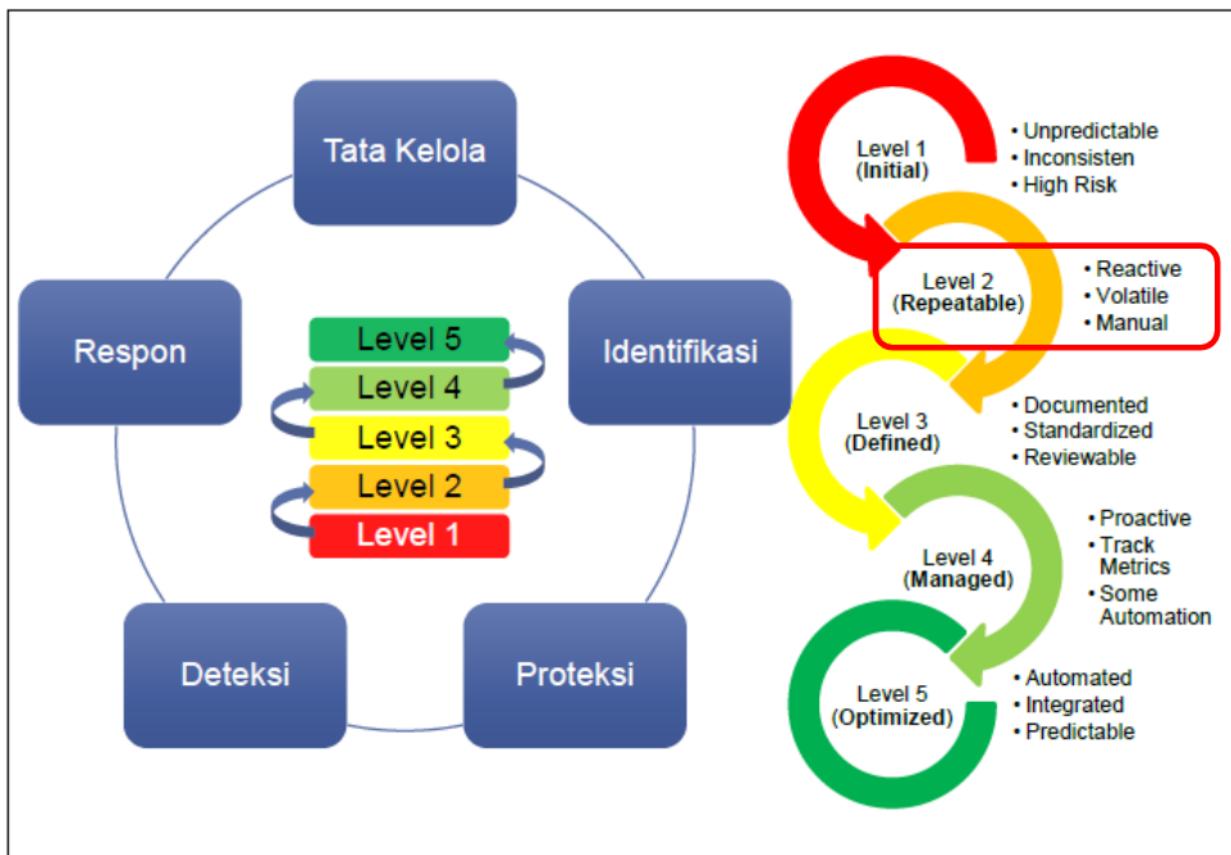
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,08**, sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat 2



Gambar 2. Capaian Level Kematangan

Level Kematangan 2:

Level kematangan 2 menunjukkan bahwa pengelolaan keamanan siber di Diskominfo-SP Provinsi Sulsel sudah terorganisir, bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan.



IV. Kekuatan/Kematangan

Tata Kelola

1. Telah menjalankan program pemahaman kesadaran keamanan informasi bagi karyawan dan juga stakeholder yang dipublikasikan melalui media sosial.
2. Telah melakukan manajemen kerentanan siber.
3. Dapat menggunakan tool vulnerability scanning secara mandiri.
4. Melakukan pemisahan environment antara sistem production dan development.
5. Menerapkan risk analisis untuk keamanan TI pada sebagian sistem elektronik.
6. Menyusun risk register terkait keamanan informasi pada sebagian aset.
7. Menerapkan kontrol kriptografi sesuai dengan peraturan yang berlaku.
8. Menerapkan perlindungan sesuai dengan persyaratan dan peraturan terhadap dokumentasi yang dimiliki organisasi.
9. Kebijakan keamanan informasi dan hasil evaluasi pelaksanaan kebijakan keamanan informasi menjadi acuan pimpinan dalam menentukan strategi organisasi.
10. Melaksanakan *penetration testing* menggunakan pihak eksternal dan internal.

Identifikasi

1. Melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa pengadaan semua aset perangkat dan aplikasi dilakukan sesuai dengan kebutuhan melalui perencanaan pengadaan setiap tahun.
2. Telah melakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman/standar/acuan organisasi.
3. Menerapkan segmentasi jaringan berdasarkan fungsionalitas

Proteksi

1. Akses nirkabel dikonfigurasikan menggunakan sistem enkripsi.
2. Koneksi ke perangkat server dan jaringan menggunakan protokol terenkripsi yaitu SSH.



3. Menerapkan port access control sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.
4. Menonaktifkan komunikasi antar workstation untuk mencegah potensi serangan siber.
5. Email system memiliki pengecekan otomatis terhadap spam/phising/malware.
6. Semua kritis system clocks telah disinkronkan dengan metode otomatis seperti Network Time Protocol.

Deteksi

1. Mengaktifkan Enable Detailed Logging yang mencakup informasi terperinci.
2. Organisasi menjamin alokasi kapasitas penyimpanan log sesuai kebutuhan.
3. Melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center.
4. 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. Tim respon insiden memiliki kemampuan dalam mendeteksi insiden.
3. Memiliki daftar kontak tim penanganan insiden internal dan eksternal.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum seluruh karyawan mengetahui dan menerapkan kebijakan keamanan informasi.
2. Belum melakukan pemeriksaan *background* untuk semua karyawan baru.
3. Belum ada mekanisme pengarahan mengenai keamanan informasi kepada setiap karyawan baru.
4. Belum melakukan gap analisis terkait skill dan behavior karyawan.



5. Belum membuat roadmap baseline pendidikan dan pelatihan terkait keamanan informasi.
6. Karyawan belum mendapat pelatihan mengenai kewajiban menjaga data privasi dan melindungi data sensitif stakeholder.
7. Belum pernah melakukan simulasi phishing.
8. Personil yang terlibat dalam pengembangan software belum mendapatkan pelatihan mengenai secure coding.
9. Belum memiliki kebijakan perlindungan data pribadi.
10. Belum melakukan reviu security risk assessment secara berkala.
11. Belum menyusun risk treatment dan melakukan reviu terhadap risk treatment secara berkelanjutan.
12. Belum melakukan reviu izin akses dari akun pengguna secara periodik (setiap tiga bulan).
13. Belum membuat persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi.
14. Belum menetapkan program untuk vulnerability assessment secara berkala.
15. Belum memiliki Red Team dan Blue Team.
16. Belum menerapkan firewall aplikasi web (WAFs).
17. Tidak memiliki IDS/IPS.
18. Belum menerapkan metode sandbox terhadap seluruh lampiran email.
19. Belum memiliki BCP (Business Contonuity Plan) dan DRP (Disaster Recovery Plan).
20. Otentikasi menggunakan single ID unik belum diatur.

Identifikasi

1. Belum mendokumentasikan proses dan prosedur untuk manajemen patch semua aset perangkat dan aplikasi.
2. Belum memiliki system configuration management tools otomatisasi konfigurasi perangkat keras dan perangkat lunak.



3. Belum tercantum pada risk register untuk semua aplikasi yang memproses data stakeholder / klien / konsumen / pelanggan.
4. Business Impact Analysis terhadap perangkat dan aplikasi TI belum disusun.
5. Identifikasi aset belum disusun berdasarkan klasifikasi kritikalitas dan belum ada penetapan terkait penanggungjawab untuk setiap aset tersebut.
6. Belum ada dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
7. Belum ada kebijakan dan implementasi mengenai retensi data sensitif termasuk data stakeholder.
8. Standar terkait klasifikasi data, klasifikasi aset TI dan klasifikasi terhadap cyber threat belum disusun.
9. Belum dilakukan identifikasi dan pembatasan akses perangkat yang tidak diizinkan oleh organisasi.
10. Belum melakukan klasifikasi informasi dan melakukan inventaris informasi.
11. Belum melakukan analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.
12. Belum ada kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
13. Dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga belum ada.
14. Belum ada kebijakan dan implementasi mengenai retensi data sensitif termasuk data stakeholder sesuai dengan kebijakan regulasi dan kebutuhan bisnis.
15. Roadmap keamanan TI organisasi belum ada.

Proteksi

1. Log disimpan kurang dari 1 tahun sehingga akan mempersulit ketika dilakukan audit dan forensik.
2. Belum menggunakan penyedia *cloud* atau menerapkan *cloud system*.



3. Belum menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan.
4. Perangkat jaringan belum menerapkan otentikasi terpusat.
5. Organisasi belum menerapkan port access control sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.
6. 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.
7. Belum ada kebijakan terkait pembatasan penggunaan scripting tools.
8. Penggunaan Multi Factor Authentication belum diterapkan.
9. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
10. Belum menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
11. 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 pengguna, koneksi jaringan, perangkat keras dan perangkat lunak, akses dan perubahan pada data sensitive, monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
3. Belum memiliki sistem untuk monitoring dan mencegah kehilangan data sensitif.
4. Belum ada mekanisme monitoring aktivitas pihak ketiga yang dilakukan di organisasi.
5. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.



6. Organisasi belum menjalankan vulnerability scanning tools secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
7. Belum melaksanakan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
8. Belum melakukan *record* seperti Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.
9. Belum memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data *sensitive*.
10. Unit dalam organisasi belum menjalankan fungsi Cyber Threat Intelligence (CTI).
11. Organisasi belum memiliki Metrik Security Event.
12. Belum mengoperasionalkan SIEM atau Log Analytics Tools.
13. Belum memiliki perangkat anti malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
14. Belum membuat escalation profile untuk setiap security event yang ditemukan.
15. Belum memiliki sistem untuk melakukan Malicious Code Detection untuk melindungi dari malicious code.
16. Mekanisme sharing informasi hasil deteksi belum ada.
17. Top Level Management tidak pernah menerima laporan mengenai kondisi keamanan siber terkini.
18. Belum memiliki ticketing system.

Respon

1. Belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Belum memiliki dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar operasional prosedur (SOP) terkait pelaporan hingga paska penanganan insiden.
3. Belum merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.



4. Tim respon insiden belum melakukan pencatatan langkah-langkah penanggulangan insiden menggunakan format baku.
5. Belum mendesain jaringan terlindungi dari akses tidak sah penyerang apabila server DMZ terkena serangan.
6. Belum menerapkan mekanisme backup data karyawan ke cloud organisasi.
7. Belum memiliki sumber daya redundan yang dapat langsung digunakan dan menjadi cadangan apabila sumber daya utama sedang tidak dapat beroperasi atau terkena serangan.
8. Belum memiliki SLA (Service Level Agreement) dalam penanganan insiden.
9. Belum memiliki mekanisme pelaporan anomali atau insiden siber dari karyawan maupun stakeholder kepada tim penanganan insiden siber organisasi.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfo-SP Provinsi Sulsel 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 (kebijakan keamanan informasi atau kebijakan mengenai data pribadi) maupun permasalahan keamanan informasi yang perlu dilakukan secara berkelanjutan.
 - b. Mendokumentasikan standar konfigurasi (*port*, protokol, *service*) untuk semua sistem, seperti *operating system*, *software*/aplikasi.
 - c. Melakukan dan menyusun gap analisis terkait skill dan behavior karyawan yang nantinya dijadikan roadmap baseline pendidikan dan pelatihan terkait keamanan informasi.
 - d. Melakukan simulasi phishing.
 - e. Mengadakan atau mengalokasikan pelatihan secure coding untuk personil yang terlibat dalam pengembangan software.
 - f. Menyusun kebijakan perlindungan data pribadi.
 - g. Melakukan reviu security risk assessment secara berkala.



- h. Menyusun risk treatment dan melakukan reviu terhadap risk treatment secara berkelanjutan.
 - i. Menerapkan mekanisme reviu izin akses dari akun pengguna secara periodik (setiap tiga bulan).
 - j. Menyusun persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi.
 - k. Menetapkan program untuk vulnerability assessment secara berkala.
 - l. Membentuk Red Team dan Blue Team.
 - m. Menerapkan firewall aplikasi web (WAFs).
 - n. Menerapkan IDS/IPS pada jaringan.
 - o. Menerapkan metode sandbox terhadap seluruh lampiran email.
 - p. Menyusun BCP (Business Contonuity Plan) dan DRP (Disaster Recovery Plan).
 - q. Menyusun kebijakan terkait otentifikasi menggunakan single ID unik.
2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
- a. Melakukan identifikasi aset dan di inventaris yang disusun berdasarkan klasifikasi kritikalitas dan mencantumkan penanggungjawab untuk setiap aset yang diinventaris.
 - b. Menyusun proses dan prosedur untuk *manajemen patch* semua aset perangkat dan aplikasi.
 - c. Menerapkan system configuration management tools untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
 - d. Melakukan risk assessment secara berkala, mereviu dan memperbarui risk register untuk seluruh aset yang dikelola.
 - e. Menyusun Business Impact Analysis terhadap perangkat dan aplikasi TI.
 - f. Menyusun alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
 - g. Menyusun kebijakan mengenai retensi data sensitif termasuk data stakeholder dan menerapkan kebijakan tersebut.



- h. Menyusun standar terkait klasifikasi data, klasifikasi aset TI dan klasifikasi terhadap cyber threat.
 - i. Melakukan identifikasi dan membuat mekanisme atau kebijakan terkait pembatasan akses perangkat yang tidak diizinkan oleh organisasi.
 - j. Membuat analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.
 - k. Menyusun kebijakan terkait pembatasan penggunaan aset organisasi untuk kepentingan pribadi, retensi data sensitif termasuk data stakeholder sesuai dengan kebijakan regulasi dan kebutuhan bisnis.
 - l. Menyusun roadmap keamanan TI organisasi.
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. Mengatur dan membuat kebijakan terkait retensi log.
 - c. Menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan serta penambahan OTP untuk otentikasi.
 - d. Menerapkan otentikasi terpusat, menerapkan port access control sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.
 - e. Membuat pengaturan terkait pembatasan fitur wireless, penerapan disable peer-to-peer pada wireless client, penerapan DNS filtering services dan pembatasan terkait aplikasi yang diperbolehkan untuk diunduh, diinstal dan dioperasikan.
 - f. Menyusun kebijakan terkait pembatasan penggunaan scripting tools.
 - g. Menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
 - h. Mempertimbangkan faktor keamanan pada data stakeholder / klien / konsumen / pelanggan yang disimpan yaitu dengan menerapkan enkripsi saat disimpan.



4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
 - a. Melaksanakan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data *center*.
 - b. Menerapkan deteksi secara otomatis terhadap perubahan konfigurasi pada peralatan jaringan.
 - c. Menyusun mekanisme monitoring terhadap akses pengguna, koneksi jaringan, perangkat keras dan perangkat lunak, akses dan perubahan pada data sensitive, monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
 - d. Menerapkan sistem untuk monitoring dan mencegah kehilangan data sensitif.
 - e. Menyusun mekanisme monitoring aktivitas pihak ketiga yang dilakukan di organisasi.
 - f. Menerapkan SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
 - g. Menerapkan vulnerability scanning tools secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
 - h. Mengatur mekanisme dan melaksanakan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
 - i. Menerapkan *Change Management System* untuk melakukan perubahan konfigurasi.
 - j. Menyusun *escalation profile* untuk setiap *security event* yang ditemukan.
 - k. Menjalankan fungsi Cyber Threat Intelligence (CTI).
 - l. Menyusun metrik security event.
 - m. Mengoperasionalkan kembali SIEM atau Log Analytics Tools.
 - n. Menerapkan perangkat anti malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
 - o. Menerapkan sistem untuk melakukan Malicious Code Detection untuk melindungi dari malicious code.



- p. Menyusun mekanisme untuk sharing informasi hasil deteksi ke karyawan ataupun stakeholder.
 - q. Menyusun laporan periodik terkait kondisi keamanan siber terkini dan melaporkan atau menyampaikan ke top level management.
 - r. Mengimplementasikan ticketing system untuk memantau tahapan penanganan pengamanan informasi.
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 dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar standar operasional prosedur (SOP) penanganan insiden dan menjadwalkan reviu secara berkala.
 - c. Melakukan latihan respon insiden dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
 - d. Tim respon insiden selalu melakukan pencatatan langkah-langkah penanggulangan insiden menggunakan format baku.
 - e. Mendesain jaringan terlindungi dari akses tidak sah penyerang apabila server DMZ terkena serangan.
 - f. Menerapkan cloud organisasi dan karyawan melakukan backup data dari perangkat yang digunakan ke cloud organisasi.
 - g. Menerapkan sumber daya redundan yang dapat langsung digunakan dan menjadi cadangan apabila sumber daya utama sedang tidak dapat beroperasi atau terkena serangan.
 - h. Menyusun SLA (Service Level Agreement) dalam penanganan insiden.
 - i. Menyusun mekanisme pelaporan anomali atau insiden siber dari karyawan maupun stakeholder kepada tim penanganan insiden siber organisasi.



PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi Informatika Statistik dan Persandian Provinsi Sulawesi Selatan ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Sulawesi Selatan. Agar Pemerintah Daerah Provinsi Sulawesi Selatan 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 2 (dua) untuk disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara; dan
2. Gubernur Provinsi Sulawesi Selatan.

Makassar, 16 Juni 2022

Kepala Bidang Persandian

(Riswan, S.Sos.,M.M.)

Koordinator Tata Kelola Kamsibersan
Pemda selaku Ketua Tim PTKKSS

(Lukman Nul Hakim, S.E.,M.M.)

Mengetahui,
Kepala Diskominfo-SP Provinsi Sulawesi Selatan

(Amson Padolo, S.Sos.)