



2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI KALIMANTAN TIMUR



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 Kaltim. 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:

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



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* atau Bidang TIK dan Persandian, Diskominfo Pemprov Kaltim pada tanggal 14 s.d. 15 Juli 2022.

2. Validasi Penilaian CSM

BSSN melakukan validasi pengisian instrumen CSM pada tanggal 19 dan 20 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Kaltim. Tim BSSN yang terlibat:

- 1) Firman Maulana, S.E.
- 2) Diah Sulistyowati, S.Kom, M.T.
- 3) Jehan Bilhaq, S.ST, M.AP.
- 4) Aris Munandar, S.S.T.MP.



HASIL KEGIATAN

I. Informasi Stakeholder

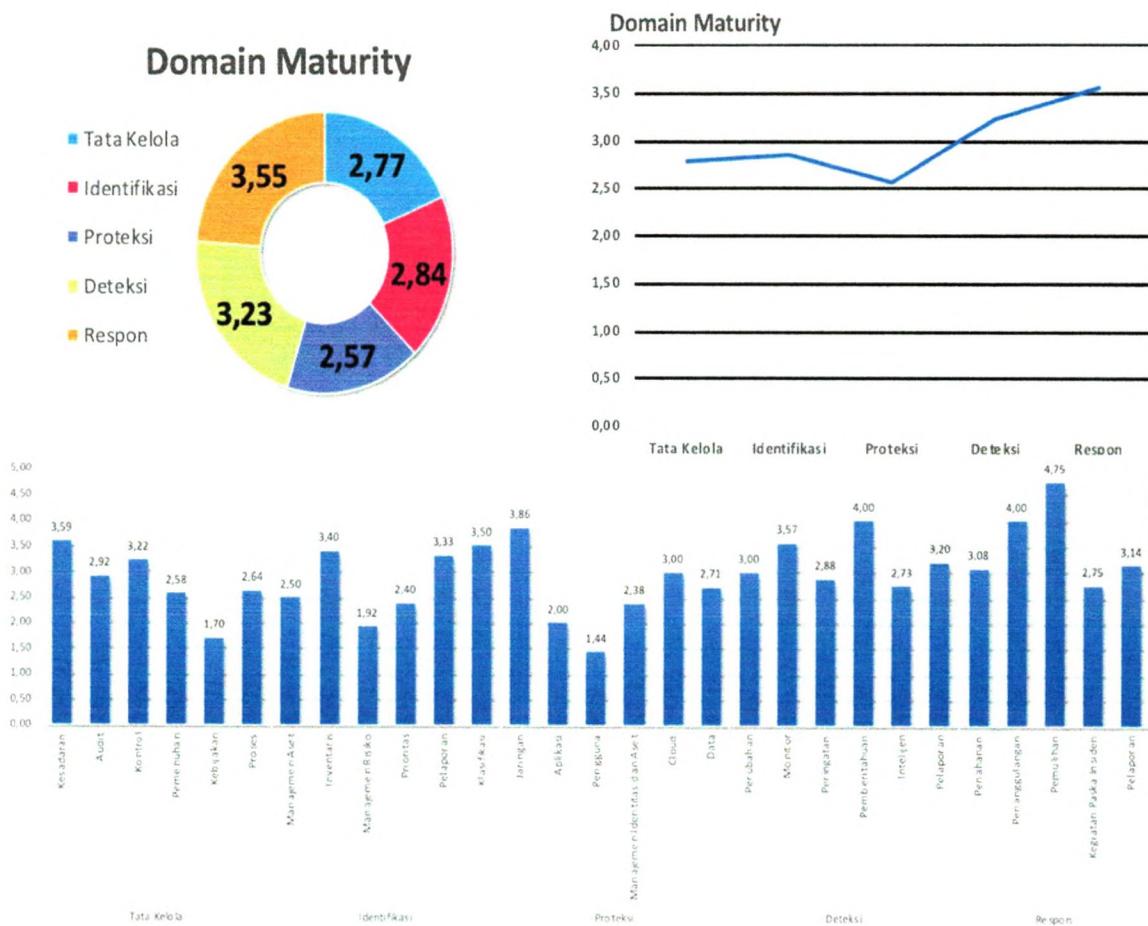
Nama Instansi/Lembaga	:	Dinas Komunikasi dan Informatika Provinsi Kaltim
Alamat	:	Jl. Basuki Rahmat No. 41 Kota Samarinda, 75242
Nomor Telp./Fax.	:	(0541) 731963
Email	:	tik.sandi@kaltimprov.go.id
Narasumber Instansi/Lembaga	:	
1. Drs. Dianto, M.Si		Kabid TIK dan Persandian
2. Dra. Hj. Normalina, M.Si		Kabid Aptika
3. Bambang Kukiloargo Suryo, S.Kom., MMSI		Kasi Pengelolaan E-Goverment
4. Agus Eko Santoso, S.Sos., M.M.		Kasi Keamanan Informasi dan Persandian
5. Fahmy Asa, S.IP, M.Eng		Kasi Pengelolaan Data Dan Integrasi SI
6. Eva Yusefa, ST, MM		Kasi Infrastruktur Teknologi Inforamasi Komunikasi
7. Edo Santradijaya, ST		Analis Sistem Informasi dan Jaringan
8. Fery, S.Kom., M.Si		Pranata Komputer Ahli Muda
9. Riko Aji Prabowo, S.Sn		Pengendali Teknologi Informasi

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 Kaltim



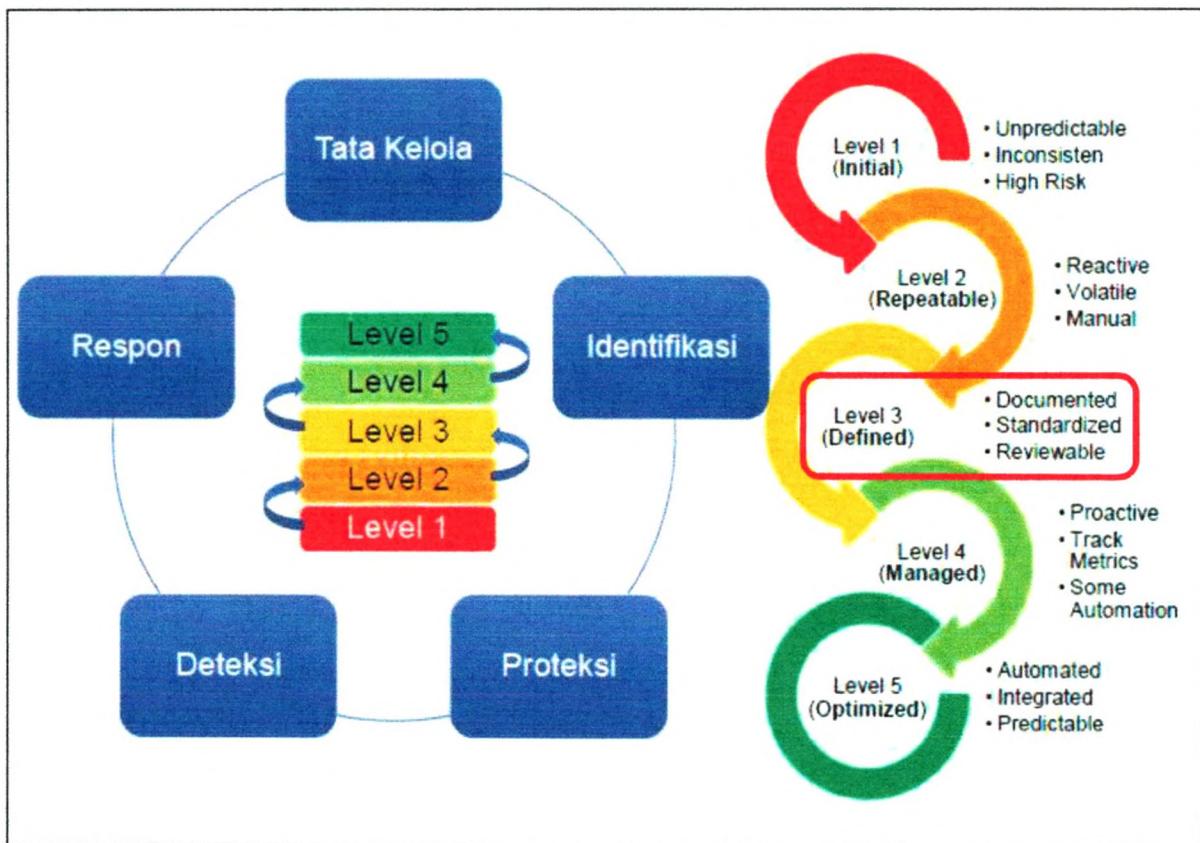
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan: 2,99**, 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 Kaltim 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. Organisasi sudah membuat program pemahaman kesadaran keamanan informasi untuk semua karyawan namun belum berkelanjutan.
2. Organisasi memastikan bahwa terdapat program kesadaran keamanan informasi diperbarui secara berkala minimal 1 tahun sekali.
3. Karyawan dalam organisasi sebagian besar mengetahui dan menerapkan kebijakan keamanan informasi di lingkungan kerja.
4. Setiap karyawan sudah mendapatkan pengarahan mengenai Keamanan Informasi namun sebagian kecil pegawai telah mengetahui dan menerapkan kebijakan keamanan informasi, namun belum semuanya berkontribusi terhadap efektivitas sistem manajemen keamanan informasi.
5. Organisasi sudah melatih staf secara khusus tentang kewajiban menjaga data privasi namun organisasi jarang melakukan manajemen kerentanan siber dan mitigasi kerentanan serta belum melakukan simulasi secara rutin.
6. Organisasi telah memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi, namun tidak direview secara berkala.
7. Telah melakukan review security risk assessment, dan dilakukan secara berkala minimal 1 tahun sekali namun organisasi belum melaksanakan risk treatment.
8. Organisasi memiliki kebijakan keamanan informasi salah satunya Dokumen daftar SOP SMKI, namun belum dipublikasikan dan tidak dikomunikasikan.

Identifikasi

1. Organisasi telah melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa semua asset perangkat dan aplikasi sesuai dengan kebutuhan.
2. Organisasi menerapkan patch keamanan pada sebagian perangkat keras dan perangkat lunak saat ada update patch yang sudah dirilis, namun belum seluruhnya tergantung pada risiko hasil pengujian.



3. Organisasi mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan.
4. Organisasi sudah melakukan klasifikasi informasi, namun belum terinventarisasi.
5. Aspek keamanan menjadi pertimbangan dan diprioritaskan dalam semua pengambilan keputusan TI, kapasitas server dan perangkat jaringan.
6. Organisasi melakukan klasifikasi terhadap cyber threats yang ditemukan.

Proteksi

1. Telah memiliki IPS dan telah dilakukan konfigurasi dan update secara rutin.
2. Koneksi ke perangkat server dan jaringan di Organisasi menggunakan protokol terenkripsi seperti SSH dan secure RDP.
3. Semua perangkat jaringan menggunakan otentikasi terpusat.
4. Firewall atau ACL menerapkan implicit or explicit deny any/any rule.
5. Inbound dan outbound network traffic hanya mengizinkan traffic yang dibutuhkan oleh organisasi.
6. Inbound network traffic di filter untuk memeriksa malware dan mencegah eksploitasi terhadap kerentanan, namun masih terkendala pembaharuan lisensi untuk implementasinya.
7. Organisasi menggunakan server terpisah baik fisik maupun virtual, namun hanya pada sebagian aplikasi.
8. Master images tersimpan pada server yang dikonfigurasi secara aman.
9. Organisasi memastikan penggunaan password yang kompleks namun masih secara manual.
10. Organisasi dapat melacak dan dapat mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun stakeholder.
11. Organisasi melakukan identifikasi perangkat pada setiap transaksi yang dilakukan oleh karyawan maupun stakeholder.
12. Sebagian perangkat dilakukan enkripsi dan time-based authentication.



13. Telah menggunakan informasi identitas dan akses pengguna digunakan untuk membatasi hak akses dari dalam jaringan.
14. Semua data penting di organisasi Anda di-backup secara berkala dan disimpan di tempat yang aman, meskipun dilakukan secara manual, belum dilakukan pengujian integritas data dan tidak diamankan dengan enkripsi.
15. Log telah disimpan sehingga mempermudah untuk dilakukan audit dan forensik dan disimpan dalam kurun waktu kurang dari 1 tahun.
16. Penyimpanan backup telah dilindungi secara tepat, baik secara fisik maupun non fisik namun belum dilakukan enkripsi.
17. Semua critical system clocks telah disinkronkan dengan metode otomatis seperti Network Time Protocol.

Deteksi

1. Terdapat Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi, namun belum dilakukan dengan jadwal tertentu hanya sesuai dengan kebutuhan.
2. Sudah menerapkan monitoring (pemantauan dan notifikasi) terhadap aktivitas lalulintas jaringan.
3. Telah melakukan monitoring terhadap log dari perangkat security control, jaringan, dan aplikasi pada saat diketahui masalah.
4. Organisasi melakukan monitoring terhadap akses pengguna, koneksi jaringan, perangkat keras, dan perangkat lunak.
5. Organisasi menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi dan analisis log.
6. Memonitor aktivitas fisik dan juga pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.



7. Organisasi memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
8. Organisasi memiliki ticketing system yang digunakan untuk melacak progres dari event post-notification.
9. Memiliki SOC bayangan atau manajemen teknis yang dapat dihubungi setiap saat untuk menangani kejadian dengan prioritas tinggi dan kritikal sesuai dengan tupoksi yang ada.
10. Memiliki contact tree untuk mengeskalasi dalam merespon suatu kejadian.
11. Memiliki mekanisme sharing informasi hasil deteksi meskipun hanya lingkup internal.
12. Organisasi melakukan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.
13. Organisasi melakukan vulnerability scanning secara otomatis menggunakan agent/aplikasi yang di instal pada endpoint.
14. Top Level Management telah menerima briefing tentang kondisi keamanan siber terkini, minimal setiap 3 bulan sekali dan perlu ditingkatkan.
15. Terdapat mekanisme sharing informasi hasil deteksi.

Respon

1. Memiliki kebijakan penanganan insiden namun tidak selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Memiliki standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
3. Memiliki Rencana Respon insiden atau Disaster Recovery plan (DRP) dan Standart Operasional Prosedur (SOP) penanganan insiden namun belum di review secara berkala
4. Telah memiliki kontak tip penanganan insiden internal dan eksternal dan selalu di perbaharui.



5. Telah mendokumentasikan, mendefinisikan peran personel serta memastikan bahwa rencana respon insiden terdokumentasi dan dapat mendefinisikan peran personal pada fase penanganan / managemen insiden serta pembagian peran kepada pihak eksternal dalam eskalasi permasalahan.
6. Desain jaringan dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain, karena secara fisik server terpisah.
7. Tim respons insiden memiliki kemampuan mendeteksi insiden, melakukan analisis, dan rekomendasi solusi.
8. Tim melakukan scanning ulang untuk memastikan bahwa pada suatu kerentanan yang ditangani sudah ditutup.
9. Ketika mengalami insiden siber apakah tim respons insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis namun sulit mendapatkan informasi dari pihak ketiga.
10. Tim respons insiden di organisasi Anda mencatat setiap langkah yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku.
11. Mempublikasikan informasi untuk semua pegawai dan stakeholder / klien / konsumen / pelanggan mengenai mekanisme pelaporan anomali dan insiden siber kepada tim penanganan insiden siber organisasi namun tidak dimasukkan dalam kegiatan rutin.
12. Laporan insiden di organisasi Anda dilaporkan ke middle management dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum dilakukan secara berkelanjutan kegiatan program pemahaman kesadaran keamanan informasi dengan fokus/isu baik terkait dengan kebijakan yang telah ditetapkan maupun permasalahan keamanan informasi.
2. Belum melakukan internal audit keamanan informasi secara berkala.



3. Organisasi belum melakukan gap analisis untuk memahami skill dan behavior yang tidak dimiliki oleh karyawan untuk membuat roadmap terkait baseline Pendidikan dan pelatihan terkait keamanan informasi dan belum nya melakukan simulasi secara rutin.
4. Personel yang terlibat dalam pengembangan software/aplikasi belum mendapatkan pelatihan secure coding.
5. Belum melakukan reviu izin akses dari akun pengguna secara berkala.
6. Konfigurasi firewall belum terdokumentasi dengan baik dan dilakukan reviu terhadap konfigurasi router dan switch bila dianggap perlu saja.
7. Belum membentuk Red Team dan Blue Team serta 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 melakukan pemisahan environment antara sistem production dan development dan mengizinkan akses kepada pengembang tanpa pengawasan dari bagian keamanan organisasi.
9. Belum menggunakan standar hardening configuration template pada database dan belum dilakukan pengujian pada semua sistem (software) yang menjadi bagian penting dari proses bisnis organisasi.
10. Belum mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.
11. Belum melakukan filterisasi terhadap seluruh jenis file lampiran email dan penerapan sandbox.
12. Belum memiliki Business Continuity Plan dan Disaster Recovery Plan yang mencakup backup dan restoration dari data pribadi.
13. Belum memiliki kebijakan metode penghapusan data.
14. Belum memiliki kebijakan terkait perlindungan data pribadi.



15. Belum melakukan analisis statis dan/atau dinamis untuk memverifikasi bahwa praktik secure coding benar-benar diterapkan pada software yang dikembangkan secara internal.
16. Belum ada kebijakan yang mengatur single ID untuk otentikasi.
17. Dalam pengembangan software belum menggunakan Praktik secure coding, algoritma enkripsi dan direviu secara berkala, serta belum menerapkan kontrol kriptografi.
18. Belum ada prosedur untuk menambah / mengubah / menghapus hak akses ketika terjadi perpindahan karyawan.

Identifikasi

1. Organisasi belum membuat/memperbarui roadmap keamanan TI organisasi dalam jangka waktu tertentu.
2. Belum memiliki system configuration management tools untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
3. Belum memiliki metode / standar untuk klasifikasi asset TI.
4. Belum dilakukan inventaris data yang ada pada asset perangkat lunak secara rutin.
5. Organisasi belum melakukan Analisa Keterkaitan antara keamanan dan kenyamanan dari pengguna asset dalam rangka penyusunan standar keamanan informasi.
6. Belum ada nya dokumentasi mengenai alur informasi yang memproses data stakeholder yang sesuai dengan kebijakan regulasi dan kebutuhan bisnis.
7. Belum ada nya review yang berkaitan dengan pemerosesan data sensitive termasuk data stakeholder sesuai dengan kebijakan dan regulasi.
8. Belum adanya kebijakan dan implementasi mengenai retensi data.
9. Belum dilakukan pemeringkatan pada kerentanan yang ditemukan berdasarkan pedoman / standart organisasi.
10. Belum memiliki Bisnis Impact Analysis terhadap pertangkat dan aplikasi TI.



11. Belum menjadikan prioritas terkait dengan langkah proteksi keamanan siber termasuk memprioritaskan perlindungan data dan asset kritis.
12. Belum tercantum pada risk register untuk semua aplikasi yang memproses data stakeholder/klien/konsumen/pelanggan.
13. Belum memiliki system configuration management tools otomatisasi konfigurasi perangkat keras dan perangkat lunak.
14. Belum memiliki metode / standar untuk klasifikasi asset IT.
15. Belum melakukan klasifikasi terhadap cyber threats yang ditemukan.
16. Belum melakukan vulnerability scanning dan/atau penetration testing terhadap semua aset perangkat dan aplikasi.

Proteksi

1. Belum memiliki perangkat jaringan menggunakan otentikasi terpusat.
2. Belum menerapkan firewall filtering antar segmen pada jaringan local.
3. Belum menonaktifkan komunikasi antar workstation.
4. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint.
5. Belum memiliki pengaturan terkait pembatasan aplikasi yang dapat diunduh, diinstall dan dioperasikan pada perangkat milik organisasi.
6. Belum menerapkannya DNS Filtering Services.
7. Belum ada nya pembatasan dalam penggunaan scripting tools.
8. Organisasi belum memastikan web browser, email client yang digunakan pada perangkat milik organisasi masih mendapatkan update support dan juga dalam penggunaan add-on dan plugin.
9. Belum mmelakukan implementasi URL filtering, device control dan application control pada semua perangkat end-point
10. Belum ada nya pengaturan akses terhadap perangakt USB/ penyimpanan eksternal.
11. Belum menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan.



12. Belum menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
13. Belum dapat melacak dan mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun stakeholder / klien / konsumen / pelanggan beserta mengidentifikasi perangkat yang digunakannya.
14. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint.
15. Tidak ada data stakeholder / klien / konsumen / pelanggan dienkripsi saat disimpan, namun di enkripsi saat proses transmisi.
16. Belum melakukan pengujian data integrity secara berkala terhadap data yang dibackup.
17. Belum menerapkan enkripsi untuk data stakeholder/pengguna yang disimpan oleh organisasi dan enkripsi pada media penyimpanan eksternal.

Deteksi

1. Belum dilakukan review terhadap semua perubahan konfigurasi melalui Change Management system.
2. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
3. Belum melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center.
4. Belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data stakeholder / klien / konsumen / pelanggan.
5. Belum dapat mendeteksi Wireless Access Point yang terhubung ke jaringan LAN (ethernet) karena masih menggunakan ISP secara langsung.
6. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
7. Belum mengimplementasikan SIEM untuk monitoring secara maksimal untuk monitoring anomali pada jaringan, server dan aplikasi.



8. Belum menerapkan automated port scan secara berkala terhadap semua sistem dan memberikan alert jika terdapat port yang tidak sah terdeteksi pada suatu sistem.
9. Belum memiliki sistem yang untuk mendeteksi ancaman siber sehingga dapat memberikan input/feed bagi threat intelligence seperti penggunaan deception technology.
10. Belum memiliki sistem untuk melakukan Malicious Code Detection untuk mendeteksi, menghapus, dan melindungi dari malicious code.
11. Tidak menyimpan semua log terhadap URL yang diakses oleh pegawai.
12. Belum secara aktif melakukan threat hunting untuk mengetahui secara dini apakah sistem telah disusupi malicious file.
13. Belum mengimplementasikan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.
14. Belum secara aktif melakukan threat hunting untuk mengetahui secara dini apakah sistem telah disusupi malicious file.
15. Belum mengimplementasikan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.

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 melaksanakan pelatihan untuk pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
4. Belum memiliki sumber daya redundan yang dapat langsung digunakan ketika sistem penting/kritis yang down karena insiden siber.



5. Waktu yang dibutuhkan untuk melakukan diskoneksi segmen jaringan untuk mencegah penyebaran malware masih terlalu lama (lebih dari 3 jam).
6. Tim respon insiden memiliki sedikit peralatan sumber daya analisis insiden.
7. Hasil review terhadap rekap laporan insiden siber belum dilaporkan ke top management dan didistribusikan kepada para pemangku kepentingan serta digunakan dalam rangka mereview kontrol yang ada untuk perbaikan respon penanganan insiden siber selanjutnya.
8. Rekaman insiden dan pelanggaran tidak disimpan dan dilaporkan berdasarkan trends insiden dalam jangka waktu tertentu.
9. Belum menerapkan mekanisme backup data karyawan ke cloud organisasi.
10. Belum memiliki SLA (Service Level Agreement) dalam penanganan insiden.
11. Belum melakukan review rekap laporan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfo Pemprov Kaltim maka dapat dilakukan hal-hal sebagai berikut:
 - a. Menetapkan kebijakan Manajemen Keamanan Informasi SPBE atau Kebijakan Sistem Manajemen Keamanan Informasi.
 - b. Mengimplementasikan SOP Sistem Manajemen Keamanan Informasi.
 - c. Mengevaluasi secara berkala terkait SOP Sistem Manajemen Keamanan Informasi.
 - d. Perlu meningkatkan pelatihan teknis seperti Secure Coding untuk personel yang terlibat dalam pengembangan software/aplikasi dan Pelatihan Keamanan jaringan untuk personil yang menangani jaringan organisasi.
 - e. Melakukan pelatihan keamanan informasi secara terjadwal untuk semua pegawai. Setidaknya untuk sharing secara menyeluruh terkait keamanan informasi kepada seluruh pegawai.
 - f. Perlu menyelenggarakan 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.

- g. Mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.
- h. Menyusun dan melaksanakan secara konsisten dan berkelanjutan program pemahaman kesadaran keamanan informasi untuk semua pegawai.
- i. Melakukan threat hunting secara berkala.
- j. Mengatur setiap akun pengguna atau sistem yang digunakan dalam melakukan penetrating testing dikontrol dan dipantau untuk memastikan bahwa akun tersebut hanya digunakan untuk tujuan yang sah, dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan.
- k. Membuat dokumentasi seluruh sistem dan jaringan.

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:

- a. Melakukan pembaharuan secara berkala dalam inventarisasi data asset (perangkat keras maupun lunak), disusun berdasarkan klasifikasi kritikalitas, memiliki penanggung jawab aset.
- b. Melakukan secara berkala dalam perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan.
- c. Menerapkan patch keamanan pada semua perangkat keras dan perangkat lunak saat ada update patch yang sudah dirilis.
- d. Membuat/ memperbaharui roadmap keamanan TI organisasi dalam jangka waktu tertentu
- e. Membuat Bisnis Impact Analysis terhadap perangkat dan aplikasi TI
- f. Memastikan pegawai tidak menyimpan credentials di browser.
- g. Melakukan vulnerability scanning dan/atau penetration testing terhadap semua aset perangkat dan aplikasi secara berkala.



3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
 - a. Menerapkan authorized cloud storage, dengan kriteria minimal menerapkan SSL pada cloud yang digunakan.
 - b. Menyimpan data backup telah dilindungi secara tepat, baik secara fisik maupun non fisik pada lokasi yang aman dan terenkripsi.
 - c. Log disimpan minimal 1 tahun sehingga akan mempermudah ketika dilakukan audit dan forensik.
 - d. Seluruh perangkat endpoints menggunakan antivirus, menerapkan web URL filtering, device control, application control, enkripsi dan membatasi fitur autorun content.
 - e. Menyusun kebijakan untuk memastikan penggunaan password yang kompleks untuk semua akses login, pergantian password secara berkala dan menggunakan/menambahkan verifikasi OTP.
 - f. Menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
 - g. Menerapkan enkripsi pada media penyimpanan eksternal, dapat menggunakan software open source atau menggunakan aplikasi dari BSSN.
 - h. Melakukan enkripsi data pada saat disimpan.
 - i. Membatasi aplikasi yang diunduh, diinstal, dan dioperasikan oleh pegawai serta membatasi penggunaan scripting tools pada aplikasi.
4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
 - a. Melakukan perubahan konfigurasi pada peralatan jaringan terdeteksi secara otomatis.
 - b. Menetapkan mekanisme monitoring terhadap akses dan perubahan pada data sensitif.
 - c. Menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
 - d. Menyusun escalation profile untuk setiap security event yang ditemukan.



- e. Memastikan log hasil deteksi malware terhubung dengan perangkat anti-malware administrations dan event log servers.
- f. Menyusun Metrik Security Event.
- g. Menerapkan ticketing system melacak kejadian berdasarkan tingkat keparahan / prioritas / dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian.
- h. Mengadakan atau menganggarkan pelatihan terkait Cyber Threat Intelligence kepada personil untuk menjalankan fungsi CTI.
- i. Menggunakan aplikasi maupun OS dengan lisensi yang original (tidak bajakan) dalam rangka menghindari kerentanan yang timbul pada aplikasi tidak berlisensi.

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. Memberikan pelatihan untuk pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
- e. Mengadakan sumber daya redundan yang dapat langsung digunakan saat sistem penting/kritis mengalami down karena insiden siber.
- f. Melakukan scanning ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup ketika ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan patching.
- g. Memastikan pencapaian SLA dalam penanganan insiden.



PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan siber pada Pemprov Kaltim. Agar Pemprov Kaltim 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 4 (empat) untuk disampaikan kepada :

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Kalimantan Timur;
3. Kepala Dinas Komunikasi dan Informatika, Pemprov Kaltim.
4. Direktur Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III, BSSN

Kaltim, 21 Juli 2022

Sandiman Madya pada Direktorat Keamanan
Siber dan Sandi Pemerintah Daerah

Kepala Bidang
TIK dan Persandian

Drs. Dianto, M.Si
NIP. 19660413 199703 1 004

Firman Maulana, S.E.
NIP. 19740503 199312 1 001