2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI KALIMANTAN 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 dan Informatika Provinsi Kalimantan 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 23 Juli 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 26 s.d. 28 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Kalimantan Selatan. Tim BSSN yang terlibat:

   1) Firman Maulana, S.E.
   2) Diah Sulistyowati, S.Kom., M.T.
   3) Mochamad Jazuly, S.S.T.TP.
   4) Faizal Wahyu Romadhon, S.Tr.TP.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Kalimantan Selatan

Alamat : Jl. Dharma Praja II - Kawasan Perkantoran Pemerintah Provinsi Kalimantan Selatan, Banjarbaru

Nomor Telp./Fax. : (0511) 6749844 / (0511) 6749842

Email : diskominfo@kalselprov.go.id

Narasumber Instansi/Lembaga :

1. M. Noor Ikhwanadi, S.H.
2. Satyawirawan
3. Abdul Hafizh
4. H. Joko Santoso
5. Dian Arifia
6. Agustini Q.
7. Febri K.
8. Novi Rahmawati
9. M. Ahmadi

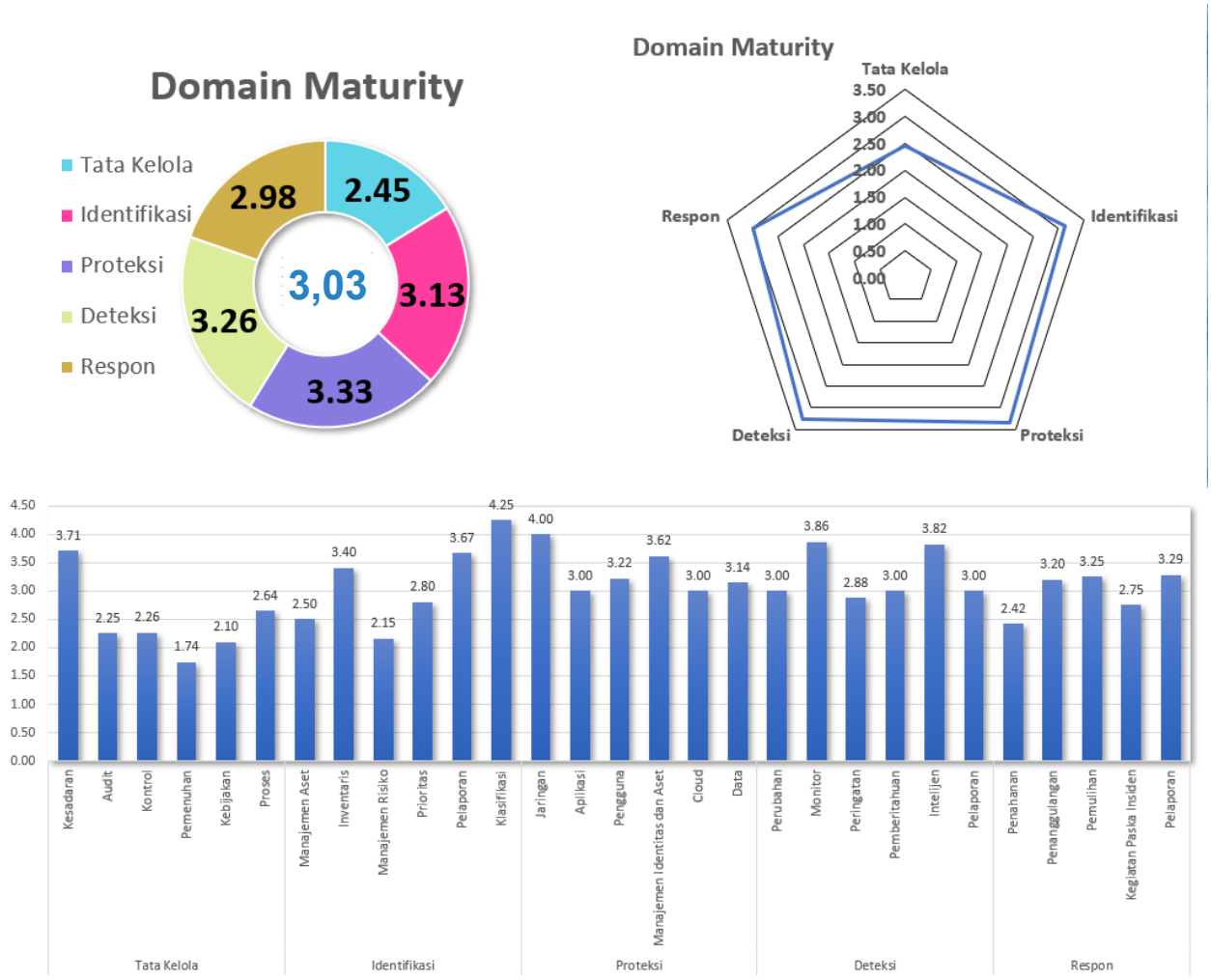
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja : Dinas Komunikasi dan Informatika Provinsi Kalimantan Selatan

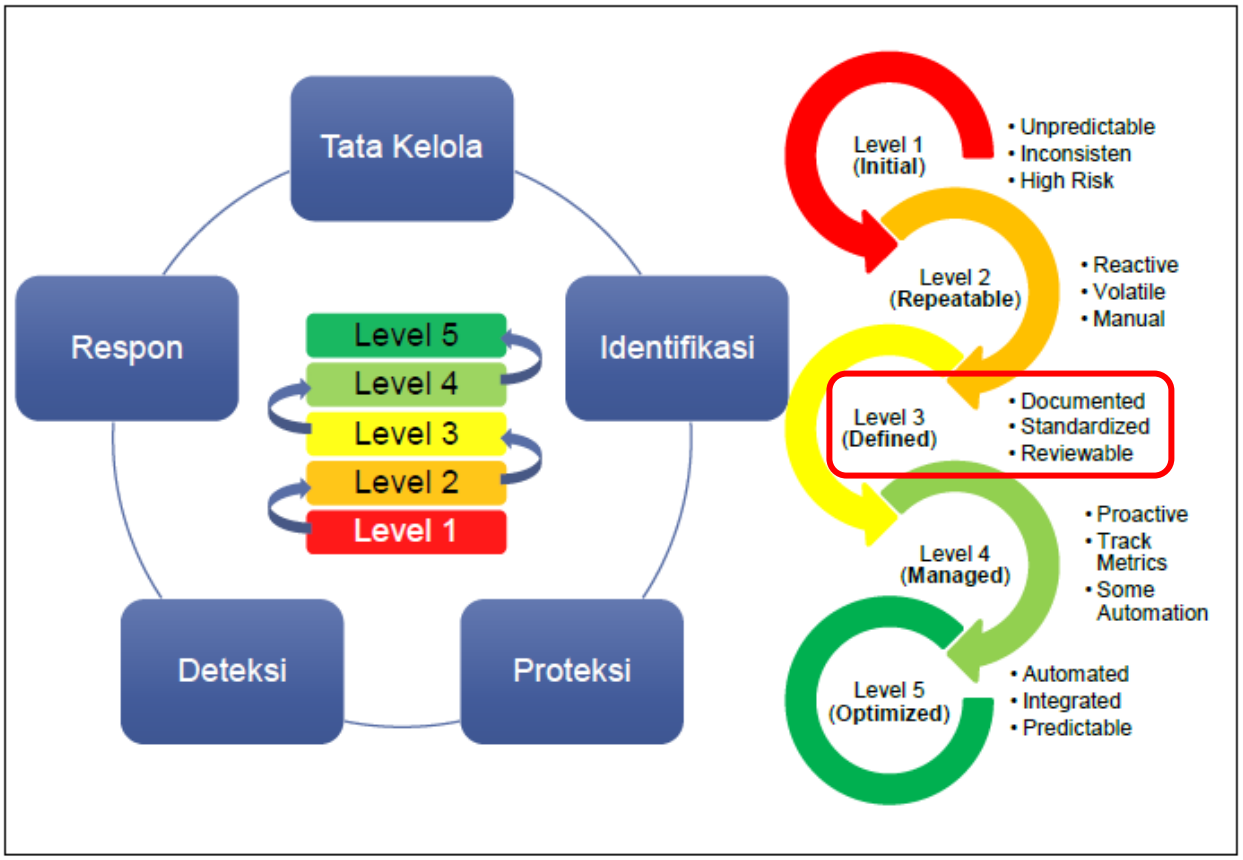
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 3,03,** 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 menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini mulai dapat terukur.

IV. Kekuatan/Kematangan

Tata Kelola

1. Organisasi telah memiliki program kesadaran keamanan informasi yang telah dilakukan dan di*review* secara berkala kepada sebagian pegawai.
2. Setiap pegawai baru mendapatkan pengarahan mengenai keamanan informasi.
3. Telah melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan.
4. Telah melakukan internal audit keamanan informasi secara berkala, namun masih menggunakan SDM internal Diskominfo.
5. Dapat memastikan sistem manajemen keamanan informasi dapat mencapai hasil yang diharapkan.
6. Semua tanggungjawab keamanan informasi telah ditentukan dan dialokasi oleh organisasi sehingga terkoordinir dengan baik
7. Organisasi mewajibkan semua pegawai dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan yang ditetapkan dan prosedur organisasi.
8. Alamat IP internal telah dilindungi oleh NAT (Network Addresss Translation).
9. Dokumentasi yang dimiliki organisasi dilindungi dan dijaga agar tidak hilang, hancur, dipalsukan, diakses oleh pihak yang tidak sah.
10. Memiliki prosedur/ kebijakan untuk menambah / mengubah / menghapus hak akses ketika terjadi perpindahan pegawai.

Identifikasi

1. Dapat mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan oleh organisasi.
2. Pihak ketiga tidak diizinkan untuk menggunakan aset mereka pada jaringan organisasi dan dikontrol dengan menggunakan NAC (network access control).
3. Telah melakukan prioritasi terkait langkah proteksi keamanan siber termasuk strategi untuk memprioritaskan perlindungan data dan aset kritis.

4. Aspek keamanan telah mempertimbangkan kapasitas server dan perangkat jaringan.
5. Memiliki metode / standar untuk klasifikasi aset TI dan dilakukan reviu secara berkala setahun sekali atau setiap terdapat perubahan.
6. Organisasi telah melakukan segmentasi jaringan berdasarkan fungsionalitas.

Proteksi

1. Penggunaan IPS yang terkonfigurasi dan selalu di update.
2. koneksi ke perangkat server dan jaringan di organisasi Anda menggunakan protokol terenkripsi.
3. Firewall telah dikonfigurasi dengan seoptimal mungkin sebagai gerbang keluar masuknya data di organisasi.
4. Seluruh aplikasi yang dikelola menggunakan server yang terpisah baik fisik maupun virtual.
5. Email system yang digunakan dapat melakukan pengecekan otomatis terhadap spam / phishing / malware.
6. Telah mengimplementasikan Next Gen Protection pada produk Fortinet.
7. Semua perangkat *endpoints* termasuk server telah menggunakan *antivirus* meskipun *default*.
8. Informasi identitas dan akses pengguna digunakan untuk membatasi hak akses dari dalam dan luar jaringan, serta data yang dikelola dalam aplikasi.
9. Melakukan identifikasi perangkat pada setiap transaksi yang dilakukan oleh pegawai.
10. Selain admin database hanya memiliki akses read-only pada akses ke database.
11. Semua critical system clocks telah disinkronkan dengan metode otomatis seperti Network Time Protocol.

Deteksi

1. Setiap perubahan konfigurasi pada peralatan jaringan terdeteksi secara otomatis.

2. Telah melakukan pengelolaan log sesuai dengan kebutuhan dan kemampuan organisasi.
3. Telah melakukan deteksi terhadap anomali pada jaringan untuk melihat potensi kejadian keamanan siber.
4. Telah memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
5. Memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
6. Memiliki ticketing system yang digunakan untuk melacak progres dari events post-notification.
7. Memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
8. *Threat intelligence feeds* dikonfigurasi secara otomatis untuk memperbarui kontrol pencegahan, seperti pembaruan signature IPS, update rules, dan konfigurasi lainnya.
9. Memiliki sistem yang untuk mendeteksi ancaman siber sehingga dapat memberikan input/feed bagi threat intelligence seperti penggunaan deception technology.
10. Memiliki sistem untuk melakukan Malicious Code Detection untuk mendeteksi, menghapus, dan melindungi dari malicious code.
11. Memiliki unit yang berfungsi untuk melakukan Cyber Threat Intelligence (CTI)

Respon

1. Memiliki standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Dengan cepat dapat melakukan diskoneksi segmen jaringan ketika terdapat laporan terjadinya infeksi malware di organisasi.
3. Tim respon insiden siber memiliki peralatan sumber daya analisis insiden dan kompetensi mendeteksi insiden, melakukan analisis dan memberikan solusi.

4. Hasil reviu terhadap rekap laporan insiden siber dilaporkan ke top management serta digunakan dalam rangka mereviu kontrol yang ada untuk perbaikan respon penanganan insiden siber selanjutnya.
5. Semua rekaman insiden dan pelanggaran di organisasi Anda disimpan dan dilaporkan berdasarkan trends insiden setiap bulan, triwulan dan tahunan.

V. Kelemahan/Kekurangan

Tata Kelola

1. Pelaksanaan *vulnerability scanning* secara mandiri tanpa menggunakan bantuan menggunakan tool *vulnerability scanning*, yang hasilnya dapat digunakan sebagai titik awal dalam melakukan *penetrating testing*.
2. Belum melakukan reviu *risk assessment*, *security risk assessment* dan *security risk treatment*.
3. Belum mereviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
4. Belum membuat persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi.
5. Belum menetapkan program untuk *vulnerability assessment* atau penetrating testing secara berkala kepada aplikasi web, aplikasi client-based, aplikasi mobile, wireless, server dan perangkat jaringan.
6. 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.
7. Belum menggunakan standar *hardening configuration template* dalam penggunaan *database*.
8. Belum melakukan reviu secara berkala terhadap penerapan kontrol keamanan untuk meminimalisir risiko.
9. Belum melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi organisasi.

10. Belum memastikan privasi dan perlindungan informasi pribadi sesuai dengan persyaratan dalam undang-undang dan peraturan terkait lainnya yang berlaku.
11. Belum menyusun *Business Continuity Plan* dan *Disaster Recovery Plan*.
12. Belum ada batasan berapa lama data dan akses stakeholder/ pengguna aktif dan disimpan.
13. Belum menerapkan *Secure Software Development Life Cycle* (*Secure* SDLC) dalam pembangunan dan pengembangan aplikasi.
14. Belum melalukan reviu terhadap konfigurasi firewall, router dan switch secara berkala.

Identifikasi

1. Belum mendokumentasikan proses dan prosedur untuk manajemen patch semua aset perangkat dan aplikasi.
2. Pegawai diiizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi.
3. Belum ada implementasi mengenai retensi data sensitif termasuk data stakeholder / klien / konsumen / pelanggan di organisasi Anda sesuai dengan kebijakan regulasi dan kebutuhan proses bisnis.
4. Belum mengidentifikasi dan menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi.
5. Terdapat data otentikasi yang disimpan diperangkat browser end user.
6. Belum melakukan prioritasi upaya remediasi dengan memanfaatkan level risiko dari hasil penilaian risiko.

Proteksi

1. Belum membatasi aplikasi yang diunduh, diinstal, dan dioperasikan oleh pegawai.
2. Belum dapat memastikan web browser, email client yang digunakan pada perangkat milik organisasi masih mendapatkan update support.

3. Web URL filtering, device control, dan application control belum diimplementasikan pada semua perangkat endpoint pengguna.
4. Belum melakukan enkripsi pada semua media penyimpanan eksternal.
5. Belum menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu seperti: browsing internet, email, akses ke sosial media, transfer file via media eksternal, dan sebagainya.
6. Multi-Factor Authentication (MFA) belum digunakan untuk semua akses jaringan dan akses data sensitif.
7. Belum melakukan pengujian data integrity secara berkala terhadap data yang di backup dengan melakukan restore data.

Deteksi

1. Belum menerapkan *Change Management System* dan melakukan reviu terhadapnya.
2. Belum dapat menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
3. Log hasil deteksi malware belum terhubung dengan perangkat anti-malware administrations dan event log servers sehingga dapat digunakan untuk analisis.
4. Escalation profile belum disusun untuk setiap *security event* yang ditemukan, kemudian disimpan sebagai panduan untuk digunakan di masa mendatang.
5. Metrik security event belum dilakukan reviu untuk tujuan operasional.

Respon

1. Belum menyusun skema penilaian insiden dan prioritas berdasarkan potensial dampak (aspek kerugian operasional, bisnis, reputasi, dan hukum) bagi organisasi.
2. Belum merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai atau tim yang terlibat dalam respon insiden.

3. Belum memberikan pelatihan untuk pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
4. Belum dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
5. Ketika sistem penting/kritikal yang down karena insiden siber, terdapat sumber daya redundan (internaet) yang dapat langsung digunakan, namun tidak untuk layanan aplikasi.
6. Belum menetapkan SLA dalam penanganan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
    a. Melakukan reviu *risk assessment*, *security risk assessment* dan *security risk treatment*.
    b. Melakukan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
    c. Menetapkan program untuk *vulnerability assessment* atau penetrating testing secara berkala kepada aset yang dimiliki.
    d. 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.
    e. Melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi organisasi.
    f. Memastikan privasi dan perlindungan informasi pribadi sesuai dengan persyaratan dalam undang-undang dan peraturan terkait lainnya yang berlaku.
    g. Menyusun *Business Continuity Plan* dan *Disaster Recovery Plan*.
    h. Melakukan pembatasan lama data dan akses stakeholder/ pengguna aktif dan disimpan.

i. Menerapkan *Secure Software Development Life Cycle* (*Secure* SDLC) dalam pembangunan dan pengembangan aplikasi.
j. Melalukan reviu terhadap konfigurasi firewall, router dan switch secara berkala.

2. Aspek ldentifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
   a. Mendokumentasikan proses dan prosedur untuk manajemen patch semua aset perangkat dan aplikasi.
   b. Membatasi akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi.
   c. Mengidentifikasi dan menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi.
   d. Memastikan data otentikasi tidak disimpan diperangkat browser end user.
   e. Melakukan prioritasi upaya remediasi dengan memanfaatkan level risiko dari hasil penilaian risiko.

3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
   a. Membatasi aplikasi yang diunduh, diinstal, dan dioperasikan oleh pegawai.
   b. Melakukan enkripsi pada semua media penyimpanan eksternal.
   c. Menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu seperti: browsing internet, email, akses ke sosial media, transfer file via media eksternal, dan sebagainya.
   d. Mengunakan Multi-Factor Authentication (MFA) untuk semua akses jaringan dan akses data sensitif.
   e. Melakukan pengujian data integrity secara berkala terhadap data yang di backup dengan melakukan restore data.

4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
   a. Menerapkan *Change Management System* dan melakukan reviu terhadapnya.

b. Menghubungkan log hasil deteksi dengan perangkat anti-malware administrations dan event log servers sehingga dapat digunakan untuk analisis.
c. Escalation profile disusun untuk setiap *security event* yang ditemukan, kemudian disimpan sebagai panduan untuk digunakan di masa mendatang.
d. Melakukan reviu terhadap Metrik security event untuk tujuan operasional.

5. Aspek Respon ditingkatkan dengan cara:
   a. Menyusun skema penilaian insiden dan prioritas berdasarkan potensial dampak (aspek kerugian operasional, bisnis, reputasi, dan hukum) bagi organisasi.
   b. Menyusun skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai atau tim yang terlibat dalam respon insiden.
   c. Memberikan pelatihan untuk pegawai (terutama pegawai di lingkungan Diskominfo) tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
   d. Memastikan ketika server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
   e. Memastikan adanya redundan ketika terjadi insiden siber yang mengakibatkan tidak berjalannya layanan, seperti listrik dan layanan aplikasi.
   f. Menetapkan SLA dalam penanganan insiden.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi dan Informatika Provinsi Kalimantan Selatan ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Kalimantan Selatan. Agar Pemerintah Daerah Provinsi Kalimantan 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 3 (tiga) untuk disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Kalimantan Selatan; dan
3. Sekretaris Daerah Provinsi Kalimantan Selatan.

Banjarbaru, 28 Juli 2022

Plt. Kepala Bidang Persandian dan Keamanan Informasi Diskominfo Provinsi Kalimantan Selatan	Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Telah ditandatangani secara elektronik oleh M NOOR IKHWANADI, SH., MM NIP. 19740721 200903 1 004	Ditandatangani Secara Elektronik Oleh: Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III Firman Maulana S.E. Pembina (IV/a)
M. Noor Ikhwanadi, S.H. 19740721 200903 1 004	Firman Maulana, S.E. 19740503 199312 1 001

Mengetahui,

Kepala Komunikasi dan Informatika
Provinsi Kalimantan Selatan

Telah ditandatangani secara elektronik oleh
Dr. H. MUHAMAD MUSLIM, S.Pd., M.Kes
NIP. 19680311 198903 1 003

Dr. H. Muhamad Muslim, S.Pd., M.Kes.
19680311 198903 1 003