2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI BALI

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 dan Statistik Provinsi Bali. 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 7 Juli 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 11 s.d. 14 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfos Provinsi Bali. Tim BSSN yang terlibat:

   1) Dwi Kardono, S.Sos., M.A.
   2) Guruh Prasetyo Putro, S.ST., M.Si (Han)
   3) Mochamad Jazuly, S.S.T.TP.
   4) Rey Citra Kesuma, S.Tr.TP.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi, Informatika dan Statistik Provinsi Bali

Alamat : Jl. DI Panjahitan No.7 Renon Denpasar - 80235

Nomor Telp./Fax. : (0361) 225859

Email : diskominfos@baliprov.go.id

Narasumber Instansi/Lembaga :

1. I Putu Sundika, ST., MT
2. I Made Widiartha, ST., M.A.P
3. Ida Bagus Gede Darma Kusuma, SE
4. I Putu Riska Desthara, S.IP.
5. I Kadek Ari Cahyadi
6. I Dewa Ketut Agung Purbayana, S.Kom

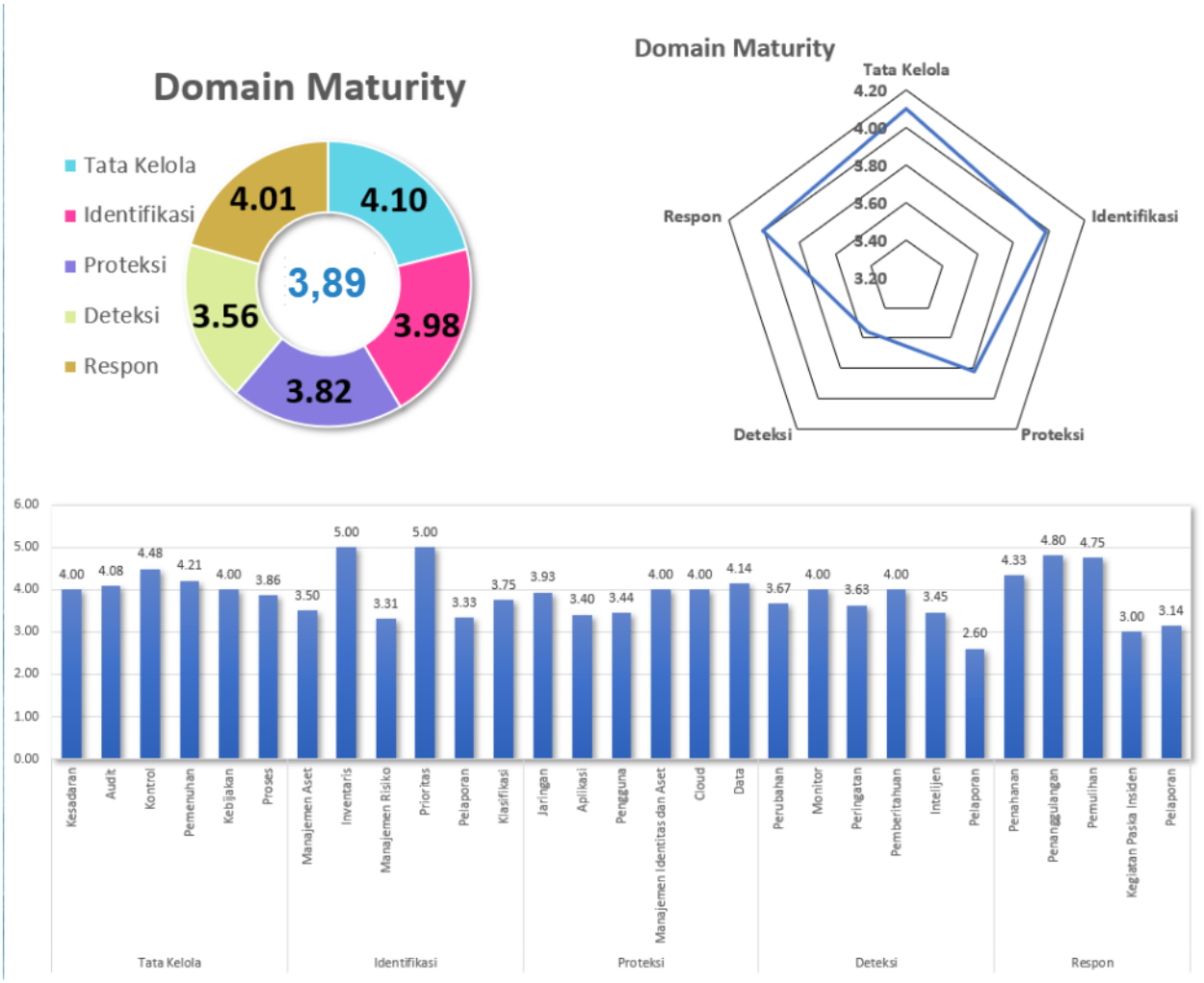
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja : Dinas Komunikasi, Informatika dan Statistik Provinsi Bali

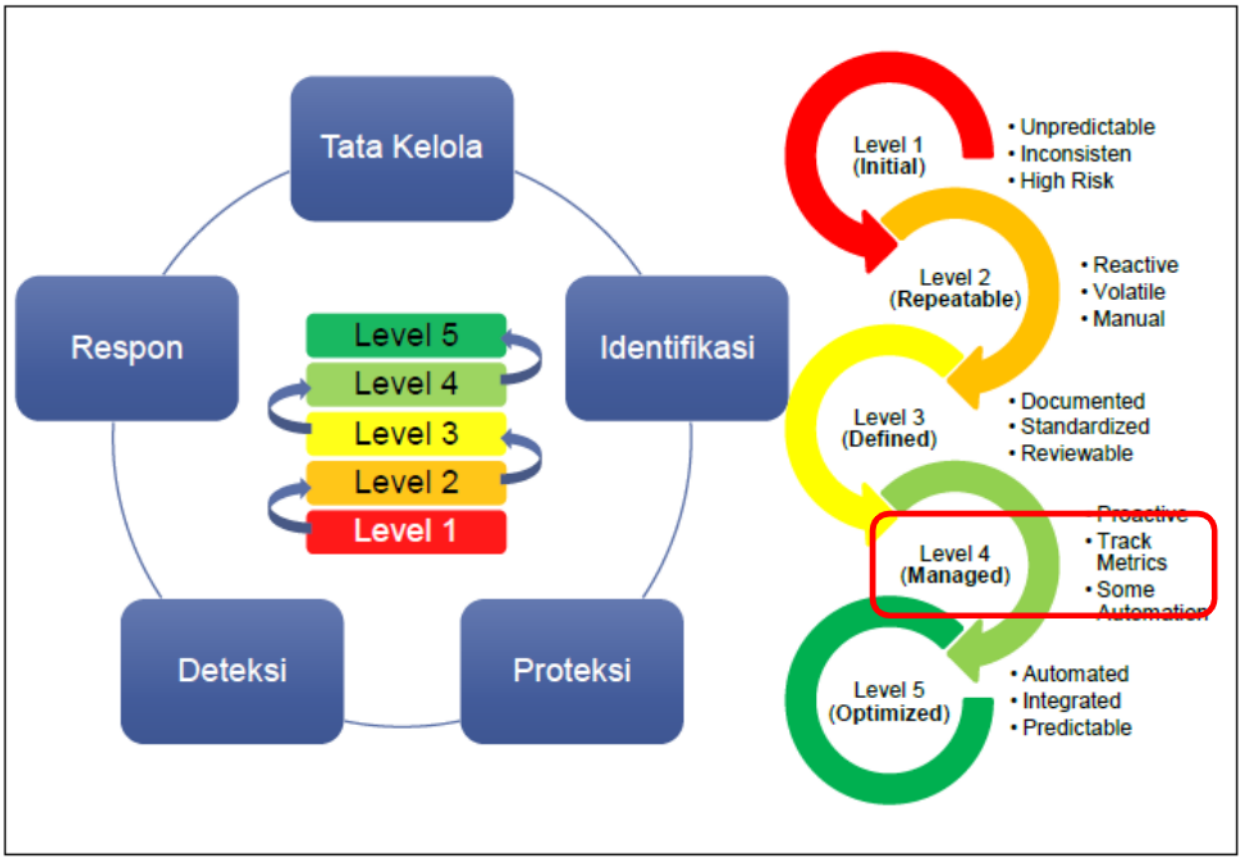
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 3,89,** sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat 4



Gambar 2. Capaian Level Kematangan

Level Kematangan 4:

Level kematangan 4 menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat formal, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini dapat terukur dengan baik.

IV. Kekuatan/Kematangan

Tata Kelola

1. Organisasi telah memiliki program kesadaran keamanan informasi yang telah dilakukan dan di*review* secara berkala kepada sebagian pegawai, hal ini didukung dengan adanya survey yang dilakukan oleh Bidang Persandian untuk memastikan bahwa Pedoman Manajemen Keamanan Informasi dan Manajemen Keamanan Siber dipahami serta diimplementasikan oleh setiap pegawai di lingkungan Diskominfos Provinsi Bali, hal ini menjadi tolok ukur bahwa kedua pedoman tersebut didistribusikan dengan baik.
2. Lentera Siber merupakan program strategis untuk meningkatkan *security awareness* pegawai.
3. Telah memiliki personil yang memiliki kompetensi *Software Quality Control*, khususnya dalam melakukan pengujian keamanan perangkat lunak.
4. Telah melakukan manajemen kerentanan siber secara aktif dengan bekerjsama dengan pihak eksternal (BSSN dan konstituen).
5. Telah melakukan pemeriksaan *background* pada pegawai baru.
6. Secara aktif melakukan *sharing* informasi terkait teknik atau kerentanan keamanan informasi pada Tim BaliProv-CSIRT.
7. Telah memiliki kebijakan penerapan perlindungan data pribadi yang dituangkan dalam Pedoman Manajemen Keamanan Siber dan telah dilakukan reviu setiap tahunnya.
8. Telah memiliki *tool vulnerability scanning* dan melakukan *vulnerability assessment* secara mandiri serta terjadwal.
9. Organisasi menggunakan akun khusus untuk melakukan *vulnerability scanning*, dan akan dihapus jika sudah tidak terpakai.
10. Telah memiliki *risk assessment*, *risk treatment*, internal audit keamanan informasi dan direviu secara berkala.
11. Telah memiliki gambaran secara global topologi infrastruktur dan jaringan di lingkungan Diskominfos Provinsi Bali.

12. Tanggungjawab keamanan informasi telah ditentukan dan dialokasi oleh organisasi sehingga ter koordinir dengan baik yang tertuang dalam Pergub Bali Nomor 56 Tahun 2021 Tentang SOTK Provinsi Bali dan SK Gub tentang CSIRT.
13. Telah memiliki Red Team dan Blue Team.
14. Dalam pengembangan aplikasi telah dilakukan dengan mempertimbangkan aspek keamanan, baik dalam proses *development* maupun *production*.
15. Telah mengimplementasikan WAFs, *firewall* pada *end user*, NAT, IPS, DMARC, dan perangkat keamanan lainnya untuk memastikan aset yang dikelola dan *end user* aman dan dapat dimitigasi ketika terjadi insiden.
16. Telah menerapkan kontrol kriptografi sesuai dengan semua perjanjian, undang-undang, dan peraturan yang berlaku.
17. Telah menerapkan metode *sandbox* terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap *malicious behaviour*.
18. *Vulnerability assessment* dan *penestration testing* telah dilakukan dengan melibatkan pihak internal dan eksternal.
19. Keamanan informasi menjadi salah satu pertimbangan pimpinan dalam pengambilan keputusan.
20. Telah mengimplementasikan *single id* untuk berbagai akses aplikasi.
21. Telah memiliki mekanisme pelaporan insiden siber dan penanggulangan insiden siber.

Identifikasi

1. Telah melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan setiap tahunnya.
2. Telah menerapkan *patch* keamanan pada semua perangkat keras dan perangkat lunak saat ada *update patch* yang sudah dirilis, namun tanpa pengujian internal.
3. Telah melakukan pendataan seluruh aset yang dikelola baik perangkat keras maupun lunak.

4. Dapat mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan oleh organisasi.
5. Memiliki kebijakan terkait pembatasan penggunaan aset organisasi untuk kepentingan pribadi, namun belum termonitor.
6. Pihak ketiga tidak diizinkan untuk menggunakan aset mereka pada jaringan organisasi.
7. Segala sesuatu yang berkaitan dengan pemrosesan data *stakeholder* / klien / konsumen / pelanggan dicatat, dimonitoring, dan dilaporkan secara berkala.
8. Organisasi memperbaharui *roadmap* keamanan Tl organisasi dalam jangka waktu tertentu dengan diprioritaskan berdasarkan perubahan kondisi lingkungan eksternal maupun internal organisasi.
9. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
10. Organisasi telah melakukan klasifikasi *cyber threat* dengan bantuan aplikasi wazuh, Fortinet dan honeypot.
11. Organisasi telah melakukan segmentasi jaringan berdasarkan fungsionalitas.

Proteksi

1. Penggunaan IPS dengan menggunakan Fortinet.
2. Akses nirkabel telah dilindungi dengan enkripsi.
3. Koneksi ke perangkat server dan jaringan telah menggunakan protokol terenkripsi.
4. Seluruh perangkat jaringan menggunakan otentikasi terpusat.
5. Firewall telah dikonfigurasi dengan seoptimal mungkin sebagai gerbang keluar masuknya data di organisasi.
6. Seluruh aplikasi yang dikelola menggunakan server yang terpisah baik fisik maupun virtual.
7. Semua perangkat *endpoints* termasuk server telah menggunakan *antivirus* meskipun *default*.

8. Master images tersimpan dengan aman.
9. Penggunaan add-on dan plugin aplikasi sudah sesuai dengan ketentuan organisasi.
10. Telah mengimplementasikan Next Gen Protection pada produk Fortinet.
11. Informasi identitas dan akses pengguna tidak digunakan untuk membatasi hak akses dari dalam jaringan.
12. Pada *email system* dilakukan pengecekan secara otomatis terhadap spam/ *phishing*/*malware* menggunakan *magic spam* dan mail server.
13. Sudah ada *whitelist* aplikasi dalam memastikan *authorized software library* dan *signed script*.
14. Sistem manajemen identitas dan akses telah digunakan untuk seluruh sistem operasi.
15. Penggunaan *password* kompleks telah diimplementasikan, namun belum dilakukan dapat memastikan penggantian berkala.
16. Penggunaan akses data telah diatur hak akses dan penerapan *whitelist* untuk memverifikasi alamat IP yang mempunyai hak akses.
17. Anomali transaksi oleh pegawai/ *stakeholder*/ klien dapat diidentifikasi dan dilakukan pelacakan/ pendeteksian.
18. Organisasi sudah memiliki *cloud storage* yang memiliki proses otorisasi, menerapkan MFA, Single Sign-On, dapat diakses melalui VPN dan memiliki DCR.
19. Data penting telah dilakukan *backup* secara berkala dan dilakukan pengujian data integrity dalam kondisi tertentu.
20. Penyimpanan log sudah dilakukan dalam rangka penanggulangan insiden siber.
21. Lalu lintas data dilindungi dengan enkripsi.

Deteksi

1. *Update* atau perubahan aplikasi telah terekam dalam aplikasi.
2. Organisasi memiliki aplikasi *monitoring* terhadap akses dan perubahan pada data sensitif (seperti *File Integrity Monitoring* atau *Event Monitoringi*).

3. Organisasi melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi.
4. Organisasi Anda mengaktifkan *Enable Detailed Logging* yang mencakup informasi terperinci seperti *event source*, tanggal, *user*, *timestamp*, *source addresses*, *destination addresses*, dan komponen lainnya.
5. Organisasi menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
6. Sebagian personil yang tergabung dalam tim *monitoring* pada organisasi mendapatkan peningkatan keterampilan.
7. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam ruangan *data center* untuk mendeteksi potensi kejadian keamanan siber.
8. Organisasi memiliki perangkat *anti-malware* yang secara otomatis melakukan *scanning* terhadap *removable media* yang terhubung ke perangkat.
9. Memiliki ticketing system untuk aduan siber.
10. Organisasi memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
11. Organisasi memiliki *contact tree* untuk mengeskalasi dalam merespons suatu kejadian.
12. Telah memperoleh informasi dari *multiple threat intelligence feeds* untuk mendeteksi serangan siber.
13. *Vulnerability scanning tools* yang digunakan secara otomatis untuk mendeteksi kerentanan siber.
14. Organisasi memiliki sistem untuk melakukan *Malicious Code Detection* untuk mendeteksi, namun untuk menghapus dan melindungi dari *Malicious Code* baru akan dilakukan pengadaan tahun ini.
15. *Midle Level Management* pada organisasi telah menerima *briefing* tentang kondisi keamanan siber terkini.
16. Organisasi telah memiliki mekanisme *sharing* informasi hanya untuk internal.

Respon

1. Organisasi memiliki kebijakan penanganan insiden, namun belum selaras dengan kebijakan pengaturan kesinambungan organisasi atau *Business Continuity Planning* (BCP).
2. Organisasi memiliki panduan pelaporan insiden dan SOP penanganan insiden, namun belum dilakukan reviu berkala.
3. Organisasi merencanakan skenario dan latihan respons insiden secara rutin dengan bekerja sama dengan BSSN.
4. Telah memberikan pelatihan pada sebagian pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
5. Organisasi memiliki daftar kontak tim penanganan insiden internal dan eksternal.
6. Organisasi mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
7. Tim respons insiden telah memiliki peralatan sumber daya analisis insiden dan memiliki kemampuan mendeteksi insiden, melakukan analisis, dan memberikan rekomendasi.
8. Ketika organisasi mengalami insiden, tim respons insiden dengan mudah mendapat bantuan dari tim manajemen kritis.
9. Sumber daya redundan telah siap dijalankan secepat mungkin untuk mengantisipasi ketika aset mengalami insiden siber.
10. Melakukan pemantauan atas rekomendasi pada kerentanan yang ditemukan.
11. Hasil *review* dan rekap laporan penanganan insiden telah dilaporkan ke *top management*.
12. Laporan insiden yang disusun dengan format baku di organisasi dilaporkan ke *top management* dan ke pihak eksternal yang berkepentingan.
13. Telah memiliki prosedur Tindakan ketika terindikasi adanya kehilangan data pribadi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum memiliki gap analisis kemampuan sehingga organisasi belum dapat membuat *baseline* pelatihan keamanan informasi.
2. Sebagian pegawai Diskominfos Provinsi Bali belum dilakukan peningkatan kompetensi (minimal dasar keamanan informasi dan siber) untuk meningkatkan *security awareness*.
3. Belum melalukan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
4. Belum mengimplementasikan *software* anti virus dan anti *malware* secara terpusat dan selalu *update* terhadap perangkat *endpoint*.
5. Belum memiliki *Business Continuity Plan* dan *Disaster Recovery Plan* secara khusus, masih dalam dokumen terpisah-pisah.
6. Belum ada kebijakan dan prosedur yang terdokumentasi terkait pemberitahuan dan keputusan *stakeholder* untuk memilih tidak membagikan data.
7. Belum memiliki kebijakan yang menetapkan sanksi yang dijatuhkan terhadap pegawai yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
8. Belum memiliki proses formal untuk manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi router, switch, dan firewall.
9. Melakukan reviu terhadap konfigurasi pada infrastruktur pada saat diperlukan.

Identifikasi

1. Organisasi belum memiliki *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
2. Pegawai diizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal komputer, dll) milik organisasi dan belum dapat mengontrol penggunaan perangkat tersebut.

3. Belum ada kebijakan dan implementasi mengenai retensi data sensitif termasuk data *stakeholder* / klien / konsumen / pelanggan sesuai dengan kebijakan regulasi dan kebutuhan organisasi serta publik.
4. Masih ditemukan data otentikasi yang disimpan di perangkat browser *end user*.
5. Risk Register belum didokumentasikan untuk semua aplikasi.

Proteksi

1. Belum menonaktifkan komunikasi antar *worskstation* untuk mencegah potensi terjadinya serangan siber (*compromise neighboring systems*) dalam satu jaringan yang sama.
2. Organisasi belum melakukan *disable peer-to-peer* pada *wireless client* di perangkat *endpoint*.
3. Belum ada pembatasan aplikasi yang diunduh, diinstal, dan dioperasikan.
4. Belum dilakukan pembatasan penggunaan *scripting tools*.
5. Belum dapat memastikan enkripsi pada semua media penyimpanan eksternal.
6. Belum ada batasan fitur *auto-run content* dan pengaturan akses *read/write* pada perangkat USB.
7. Multi-Factor Authentication (MFA) belum digunakan untuk semua akses jaringan.
8. 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.

Deteksi

1. Organisasi belum memiliki sistem untuk me*monitoring* dan mencegah kehilangan data sensitif.
2. Organisasi tidak memantau aktivitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.

3. Organisasi tidak menerapkan *event notification* yang berbeda-beda untuk setiap jenis eskalasi.
4. Belum memiliki tim khusus Cyber Threat Intelligence (CTI).
5. *Metrik security event* digunakan untuk evaluasi dalam rangka menghitung efisiensi operasional pengelolaan TI.
6. *Sharing* informasi hasil deteksi belum menyasar pihak eksternal.

Respon

1. Belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respons sudah sesuai dengan standar yang ditetapkan.
2. Belum memiliki SLA penanganan insiden.
3. Organisasi belum merancang standar terkait waktu yang diperlukan bagi administrator sistem dan pegawai lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
    a. Melakukan gap analisis untuk memahami *skill* dan *behaviour* yang tidak dimiliki pegawai dan menggunakan informasi tersebut untuk membuat *roadmap* terkait *baseline* pendidikan dan pelatihan terkait keamanan informasi.
    b. Lentera Siber agar dapat dilakukan di internal Diskominfos untuk memperkuat *security awareness* internal organisasi secara menyeluruh.
    c. Melalukan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
    d. Menyusun *Business Continuity Plan* dan *Disaster Recovery Plan*.

e. Menyusun kebijakan dan prosedur terkait pemberitahuan dan keputusan *stakeholder* maupun pengguna untuk memilih tidak membagikan data.
f. Belum memiliki proses formal untuk manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi router, switch, dan firewall.
g. Melakukan reviu terhadap konfigurasi pada infrastruktur secara berkala dan terdokumentasi.

2. Aspek Identifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
   a. Menggunakan *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
   b. Membatasi akses pegawai sebagai administrator pada perangkat (laptop, personal komputer, dll) milik organisasi dan belum dapat mengontrol penggunaan perangkat tersebut.
   c. Menyusun kebijakan dan implementasi mengenai retensi data sensitif termasuk data *stakeholder* / klien / konsumen / pelanggan sesuai dengan kebijakan regulasi dan kebutuhan organisasi serta publik.
   d. Memberikan peringatan ketika ditemukan data otentikasi yang disimpan diperangkat browser *end user*.
   e. Mendokumentasikan seluruh sistem elektronik yang dikelola dalam Risk Register.

3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
   a. Menonaktifkan komunikasi antar *worskstation* untuk mencegah potensi terjadinya serangan siber (*compromise neighboring systems*) dalam satu jaringan yang sama.
   b. Melakukan *disable peer-to-peer* pada *wireless client* di perangkat *endpoint*.
   c. Memonitoring atau membatasi aplikasi yang diunduh, diinstal, dan dioperasikan.
   d. Melakukan enkripsi pada semua media penyimpanan eksternal.

e. Belum ada batasan fitur *auto-run content* dan pengaturan akses read/write pada perangkat USB.
f. Menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu.

4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
   a. Mengimplementasikan *Data Loss Prevention* untuk memonitoring dan mencegah kehilangan data yang sensitif.
   b. Melakukan pendampingan dengan pihak ketika melakukan aktivitas di lingkungan Diskominfos.
   c. Menerapkan *event notification* yang berbeda-beda untuk setiap jenis eskalasi yaitu notifikasi menyesuaikan kritikalitas kejadian (bisa dimasukkan dalam kebijakan atau prosedur penanganan insiden.
   d. Membentuk tim Cyber Threat Intelligence (CTI).
   e. *Sharing* informasi hasil deteksi didistribusi kepada pihak eksternal maupun internal.

5. Aspek Respon ditingkatkan dengan cara:
   a. Melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respons sudah sesuai dengan standar yang ditetapkan.
   b. Menyusun standar terkait waktu yang diperlukan bagi administrator sistem dan pegawai lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi, Informatika dan Statistik Provinsi Bali ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Bali. Agar Pemerintah Daerah Provinsi Bali 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;
2. Gubernur Provinsi Bali; dan
3. Sekretaris Daerah Provinsi Bali.

Denpasar, 15 Juli 2022

Kepala Bidang Persandian Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali	Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Ditandatangani secara elektronik oleh Kepala Bidang Persandian **I Putu Sundika** NIP. 19761226 200604 1 003	Ditandatangani secara elektronik oleh: SANDIMAN AHLI MADYA **Dwi Kardono, S.Sos., M.A.**
I Putu Sundika, ST., MT 19761226 200604 1 003	Dwi Kardono, S.Sos., M.A. 19710218 199110 1 001

Mengetahui,

Kepala Komunikasi, Informatika, dan Statistik
Provinsi Bali

Ditandatangani secara elektronik oleh :
KEPALA DINAS
Gede Pramana
NIP. 19680531 199703 1 002

Gede Pramana, ST., MT.
19680531 199703 1 002