



2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK
PROVINSI NUSA TENGGARA BARAT



PENDAHULUAN

I. Umum

Tingkat kesiapan keamanan siber di setiap organisasi berbeda-beda, sehingga masing-masing organisasi juga membutuhkan strategi yang berbeda-beda pula dalam menghadapi ancaman, serangan, maupun ancaman siber. Dalam implementasi keamanan siber, beberapa organisasi baru fokus terhadap perbaikan penerapan kontrol keamanan yang lebih proaktif, penyusunan peraturan dan kebijakan keamanan siber, dan penyusunan strategi keamanan berdasarkan hasil deteksi insiden. Selain itu, sebagian organisasi telah mendorong investasi teknologi sebagai kebutuhan keamanan serta telah memberikan dukungan personel di bidang keamanan siber yang kompeten, serta mempertimbangkan risiko siber serta mendorong budaya keamanan siber secara menyeluruh untuk keberlangsungan organisasinya.

Setiap organisasi harus memahami kelemahan dari proses keamanan siber yang dimiliki. Sehingga dapat menentukan target tingkat keamanan siber yang akan dicapai dan memastikan bahwa organisasi tersebut telah siap dalam menghadapi ancaman siber dalam bentuk apa pun. Oleh karena itu diperlukan suatu metode pengukuran kematangan keamanan siber agar organisasi dapat melakukan peningkatan dalam pengelolaan proses keamanan siber dan memastikan bahwa telah dioptimalkan sepenuhnya dan berfungsi secara menyeluruh. Untuk itu, Badan Siber dan Sandi Negara (BSSN) telah membentuk suatu *framework* untuk mengukur *cyber security maturity* yang dapat digunakan sebagai metode untuk mengukur tingkat kematangan keamanan siber suatu organisasi.

Tools Cyber Security Maturity merupakan alat bantu yang digunakan untuk mengukur kematangan keamanan siber di organisasi. Sektor pemerintahan sebagai salah satu domain yang memanfaatkan ruang siber diharapkan turut melakukan peningkatan pengelolaan keamanan siber serta memastikan pengelolaan tersebut berjalan dengan optimal dan berfungsi secara menyeluruh.



II. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi Informatika dan Statistik Provinsi Nusa Tenggara Barat pada tahun 2022. Dengan adanya perbaikan pada tingkat maturitas ini diharapkan dapat memberikan gambaran mengenai apa yang harus menjadi tindak lanjut baik oleh *stakeholder* maupun Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan maturitas keamanan siber.

III. Ruang Lingkup Kegiatan

Kegiatan hasil evaluasi tindak lanjut rekomendasi yang dilaksanakan meliputi ruang lingkup pemetaan kematangan keamanan siber yang meliputi :

1. Aspek Tata Kelola
2. Aspek Identifikasi
3. Aspek Proteksi
4. Aspek Deteksi
5. Aspek Respon

IV. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen *Cyber Security Maturity* (CSM), wawancara/diskusi, dan melihat ketersediaan dokumen keamanan siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas setiap aspek keamanan siber.

Penentuan Level Kematangan diukur berdasarkan Indeks Kematangan yang didapat. Konversi Indeks Kematangan menjadi Level Kematangan menggunakan formula:

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



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* pada bulan Juli 2022.

2. Validasi Penilaian CSM

BSSN melakukan validasi pengisian instrumen CSM pada tanggal 11 - 15 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfotik Provinsi Nusa Tenggara Barat. Tim BSSN yang terlibat:

- 1) Lukman Nul Hakim, S.E.,M.M.
- 2) Irma Nurfitri Handayani, S.ST.
- 3) Arif Fachru Rozi, S.ST.
- 4) Carissa Mega Yulianingrum, S.Tr.TP.



HASIL KEGIATAN

I. Deskripsi Ruang Lingkup Penilaian

Nama Instansi/Lembaga : Dinas Komunikasi, Informatika, dan Statistik Provinsi Nusa Tenggara Barat

Alamat : Jalan Udayana No. 14 Mataram - NTB

Nomor Telp./Fax. : (0370) 644264 / (0370) 7509831

Email : sandikami@ntbprov.go.id

Narasumber Instansi/Lembaga :

- 1) Lalu Amjad, S.H., M.H.
- 2) Yasrul, S.Kom., M.Eng.
- 3) Lalu Arief Gunawan, S.E., M.Si.
- 4) Ni Made Febrie Arisandi Ak, SE., ST.
- 5) Yosafat Parulian D.
- 6) Robert Silas Kabanga, S.Kom., M.Eng.
- 7) R. Ronald Ommy Y., S.T., M.T.

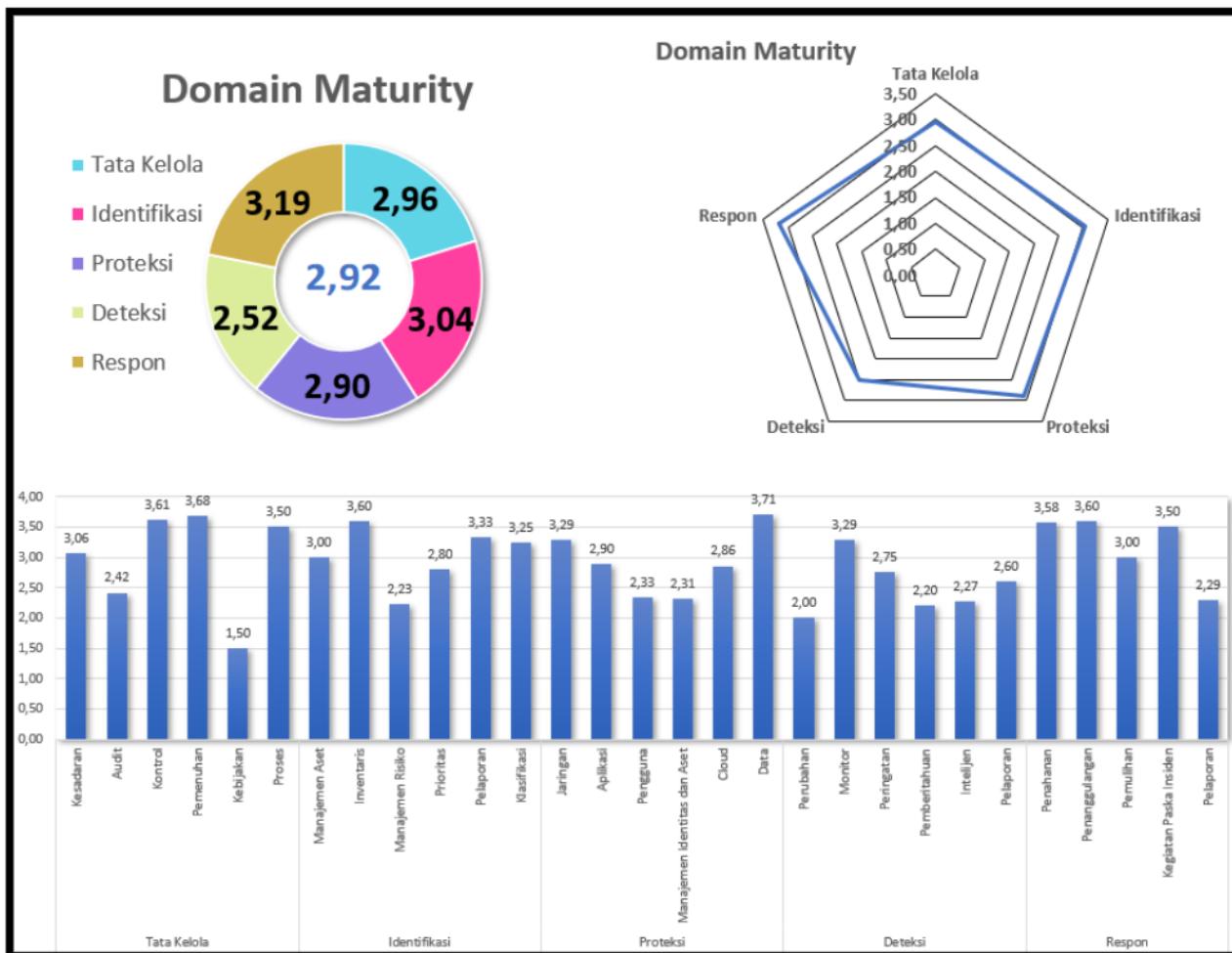
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

Organisasi Keseluruhan Regional, Kanwil, Cabang Unit Kerja Lainnya

2. Instansi/Unit Kerja^{*} : Dinas Komunikasi Informatika dan Statistik
Provinsi Nusa Tenggara Barat

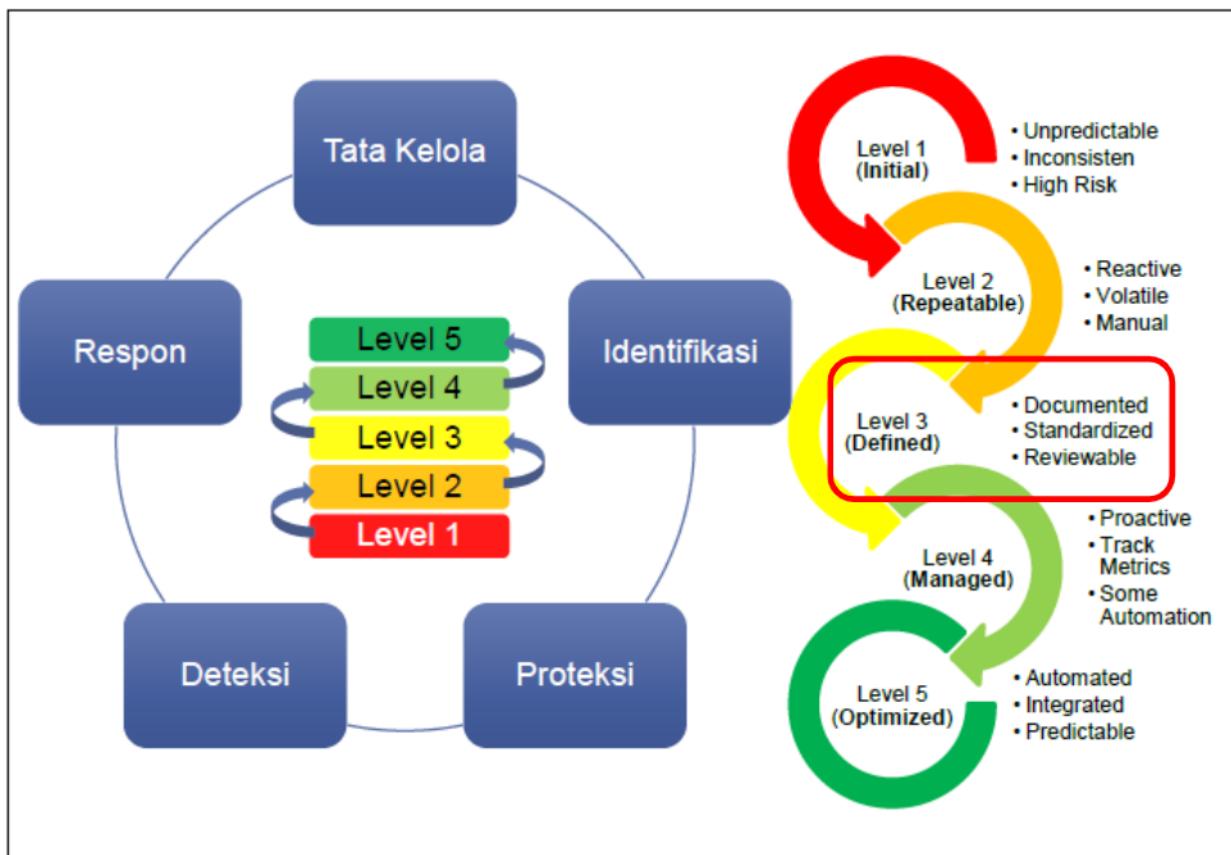
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,92**, sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :





Gambar 2. Capaian Level Kematangan

Level Kematangan 3:

Level kematangan 3 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi, Informatika, dan Statistik Provinsi Nusa Tenggara Barat sudah sudah terorganisir dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan.

Catatan:

Berdasarkan hasil penilaian CSM yang telah dilakukan pada tahun 2020 dengan total skor indeks kematangan adalah 2,89, terdapat kenaikan 0,03 poin menjadi 2.92 dengan kategori level yaitu level 3.



IV. Kekuatan/Kematangan

Tata Kelola

1. Sudah mengimplementasikan *software anti virus* dan *anti malware* secara terpusat dan selalu *update*.
2. Sudah melakukan reviu *security risk assessment* dan *treatment*, namun belum secara berkala.
3. Diagram yang menggambarkan aliran data di seluruh sistem jaringan telah didokumentasikan dan dilakukan pembaruan setiap ada perubahan.
4. Standar konfigurasi (*port*, *protokol*, *service*) telah diterapkan dan didokumentasikan.
5. Program untuk *vulnerability assessment* atau *penetrating testing* pada aplikasi web, aplikasi *client-based*, aplikasi *mobile*, *wireless*, *server* dan perangkat, jaringan telah dilaksanakan setidaknya 1 tahun sekali.
6. Dilakukan pemisahan environment antara sistem *production* dan *development* dan tidak mengizinkan akses kepada pengembang tanpa pengawasan dari bagian keamanan organisasi.
7. Aplikasi web organisasi telah dilindungi menggunakan *firewall* aplikasi web (WAFs).
8. Alamat IP internal di organisasi telah dilindungi oleh NAT (Network Address Translation).
9. Penggunaan IDS/IPS telah diterapkan untuk jaringan perimeter.
10. Dilakukan filterisasi terhadap seluruh jenis *file* lampiran *email*.
11. Peraturan, persyaratan kontrak, dan peraturan lainnya telah diidentifikasi dan didokumentasi.
12. Kontrol kriptografi telah diterapkan sesuai dengan peraturan yang berlaku.
13. Dalam pengembangan *software*, organisasi telah melakukan verifikasi bahwa versi semua *software* yang diperoleh dari luar organisasi masih didukung oleh pengembang atau dipertegas berdasarkan rekomendasi keamanan pengembang.



14. Organisasi telah menerapkan praktik *secure coding* yang sesuai dengan bahasa pemrograman dan *development environment* yang digunakan.
15. *Source code* yang dibuat secara mandiri dilakukan reviu kerentanannya terlebih dahulu oleh *developer* internal menggunakan teknis otomatis dan manual sebelum masuk ke *production*.
16. Terdapat prosedur otorisasi/ persetujuan untuk menambah/ mengubah/ menghapus hak akses ketika terjadi perpindahan karyawan.

Identifikasi

1. Melakukan perencanaan kapasitas secara berkelanjutan untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan.
2. Telah melakukan inventarisasi data yang ada pada semua perangkat keras, tetapi masih belum semua pada perangkat lunak.
3. Melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi.
4. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
5. Melakukan segmentasi jaringan berdasarkan fungsionalitas dengan kontrol keamanan antar segmen.

Proteksi

1. Koneksi ke perangkat *server* dan jaringan di organisasi menggunakan protokol terenkripsi.
2. Penggunaan *firewall* telah di konfigurasi dengan baik seperti *implicit* atau *explicit deny any/any rule, inbound* dan *outbound network traffic*.
3. Menerapkan DNS *Filtering*.
4. Email system di organisasi (termasuk yang ada di cloud) memiliki pengecekan otomatis terhadap *spam/ phishing/ malware*.



5. Semua perangkat *endpoints* termasuk server menggunakan *anti virus*.
6. Akses ke data *stakeholder* diatur dengan hak akses.
7. *Critical system clocks* telah disinkronkan dengan metode otomatis seperti *Network Time Protocol*.

Deteksi

1. Sudah menerapkan monitoring (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan.
2. Menerapkan SIEM atau *Log Analytic Tools* untuk keperluan dokumentasi, korelasi, dan analisis *log*.
3. Setiap orang yang tergabung dalam tim monitoring pada organisasi mendapatkan peningkatan keterampilan, akan tetapi tidak setiap tahun.
4. Memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
5. Memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
6. Dapat mendeteksi kegagalan *login* pada akun admin pada perangkat jaringan, server, dan aplikasi.
7. Organisasi dapat mendeteksi aktivitas anomali *login* seperti waktu, lokasi, durasi.
8. Memiliki sistem untuk mendeteksi adanya *malicious code*.

Respon

1. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden.
2. Melakukan perencanaan skenario penanganan insiden secara rutin kepada karyawan pengelola TI.



3. Mempunyai daftar kontak tim penanganan insiden internal dan eksternal (misalnya penegak hukum, ambulance, pemadam kebakaran, dll) yang dapat dihubungi pada saat terjadi insiden.
4. Melakukan *backup data* yang ada di pc/laptop karyawan ke *cloud* organisasi.
5. Tim respon insiden siber di organisasi memiliki peralatan sumber daya analisis insiden (misalnya daftar *host*, *packet sniffer*, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat *digital forensic*, dan sebagainya).
6. Tim respon insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis (contoh: spesialis keamanan teknis, tim bisnis, spesialis hukum, tim SDM, dan tim komunikasi eksternal) dan dapat dengan cepat mengakses informasi (dari penyedia pihak ketiga, dan informasi pendukung yang penting lainnya) saat organisasi mengalami insiden siber.
7. Hasil reviu terhadap rekap laporan insiden siber dilaporkan ke top management dan didistribusikan kepada para pemangku kepentingan serta digunakan dalam rangka mereviu kontrol yang ada untuk perbaikan respon penanganan insiden siber selanjutnya.
8. Laporan insiden di organisasi dilaporkan ke top management dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Program pemahaman kesadaran keamanan informasi telah dilakukan namun belum secara berkelanjutan untuk diketahui oleh seluruh karyawan.
2. Belum melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan secara berkelanjutan.
3. Belum melakukan simulasi phising setidaknya setiap tahun.



4. Belum menggunakan *tools vulnerability scanning* sebagai titik awal dalam melakukan *penetrating testing* secara rutin.
5. Belum memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi dan dilakukan proses reviu secara berkala.
6. Belum melakukan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
7. Belum membentuk *Red Team* dan *Blue Team* serta belum melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.
8. Belum ada kegiatan penelusuran yang memastikan bahwa data stakeholder yang disimpan adalah data yang akurat.
9. Belum memiliki *risk register* terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
10. Belum melakukan kegiatan pengukuran tingkat kepatuhan pengguna dalam implementasi kebijakan keamanan informasi.
11. Belum terdapat dokumen BCP dan DRP.
12. Belum mempunyai kebijakan yang menetapkan sanksi yang dijatuhkan saat terdapat pelanggaran dalam hal keamanan siber.
13. Belum memiliki kebijakan keamanan informasi mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.

Identifikasi

1. Aset yang diidentifikasi belum disusun berdasarkan klasifikasi kritikalitas (berdasarkan analisis risiko operasional, analisis bisnis, dan analisis strategis organisasi) serta belum ditetapkan penanggung jawab untuk setiap aset tersebut.
2. Belum terdapat kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.



3. Belum terdapat dokumentasi alur informasi yang memproses data *stakeholder* termasuk yang dikelola pihak ketiga.
4. Belum memiliki kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
5. Belum memiliki *risk register* yang terdokumentasi untuk semua aplikasi yang memproses data stakeholder.
6. Belum memiliki *Bussines Impact Analysis* terhadap perangkat dan aplikasi TI dan direviu secara berkala.
7. Organisasi tidak memiliki standar untuk klasifikasi aset TI.

Proteksi

1. Belum memiliki IPS.
2. Organisasi tidak membatasi aplikasi yang diunduh, diinstal, dan dioperasikan.
3. Belum menerapkan pengaturan akses (*read/write*) terhadap perangkat USB/media penyimpanan eksternal.
4. Belum penerapan *Multi-Factor Authentication* (MFA) yang digunakan untuk semua akses jaringan dan mengakses data sensitif.
5. Belum memastikan penggunaan password yang kompleks untuk semua akses login.
6. Belum menambahkan verifikasi *On Time Password* (OTP) melalui SMS, WhatsApp Messenger, Telepon, Elektronik Mail, Google Authenticator, atau media lainnya untuk transaksi yang berisiko tinggi.
7. Belum menerapkan Single Sign-On pada layanan cloud.
8. Belum semua data stakeholder dienkripsi saat disimpan.

Deteksi

1. Semua perubahan konfigurasi belum melalui proses Change Management System dan tidak dilakukan reviu secara berkelanjutan.



2. Melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi namun ketika diketahui ada masalah.
3. Belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data *stakeholder*.
4. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritis.
5. Belum menjalankan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber menggunakan *agent*/aplikasi yang diinstal pada endpoint.

Respon

1. Belum melakukan review secara berkala terhadap dokumen rencana respon insiden atau *disaster recovery plan* (DRP).
2. Belum memberikan pelatihan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi untuk seluruh karyawan.
3. Belum mendesain jaringan yang dapat memastikan apabila *server* DMZ terkena serangan siber, penyerang tidak dapat mengakses *server* yang lain.
4. Belum memiliki sumber daya redundan yang dapat langsung digunakan pada sistem penting/kritis yang down karena insiden siber.
5. Setelah ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*, belum dilakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup.
6. Tim respon insiden di organisasi belum melakukan pencatatan setiap langkah yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku (telah ditetapkan oleh organisasi).
7. Belum merancang standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim



penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.

8. Belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan.

VI. Rekomendasi

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), disampaikan beberapa rekomendasi yang dapat dilakukan dalam rangka peningkatan kematangan siber pada Dinas Komunikasi, Informatika & Statistik Provinsi Nusa Tenggara Barat sebagai berikut:

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
 - a. Menyusun program pemahaman kesadaran keamanan informasi yang dilakukan secara berkelanjutan.
 - b. Menerapkan manajemen risiko terhadap seluruh aset milik organisasi.
 - c. Menyusun dokumen BCP dan DRP.
 - d. Menyusun kebijakan untuk penerapan perlindungan data pribadi dan direviu secara berkala.
 - e. Menyusun kebijakan keamanan informasi yang telah disetujui manajemen serta dikomunikasikan kepada karyawan dan pihak eksternal terkait dan dikembangkan sesuai dengan kerangka kerja dan standar yang diakui khususnya terkait dengan penerapan kriptografi, mekanisme penghapusan data, dan pengendalian terhadap aset informasi.
 - f. Menyusun kebijakan keamanan informasi mengatur mengenai *single ID* yang unik untuk melakukan semua otentikasi.
2. Aspek Identifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:



- a. Menyusun *Business Impact Analysis* terhadap perangkat dan aplikasi TI berdasarkan aspek kerahasiaan, keutuhan, ketersediaan, otentikasi dan anti penyangkalan sehingga dapat dirumuskan prioritas penanganan risiko.
 - b. Menyusun dokumen *risk register* untuk seluruh aset milik organisasi dan semua aplikasi yang memproses data *stakeholder* sesuai dengan kerangka kerja dan standar yang diakui dengan memetakan terkait aset, kerentanan, ancaman, kemungkinan, dampak, level risiko, proses mitigasi, dan penanggungjawab.
 - c. Menyusun kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
 - d. Menyusun metode/standar untuk klasifikasi aset TI dan direviu secara berkala.
3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
- a. Menerapkan penggunaan *multi factor authentication*.
 - b. Menerapkan otentikasi terpusat pada semua perangkat jaringan.
 - c. Menerapkan *single sign-on* pada *cloud* organisasi.
 - d. Menerapkan enkripsi pada semua data *stakeholder* saat disimpan.
4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
- a. Menerapkan *change management system* Semua untuk semua perubahan konfigurasi dan dilakukan reviu secara berkelanjutan.
 - b. Melakukan monitoring terhadap log dari perangkat *security control*, jaringan, dan aplikasi selama 24 jam sehari.
 - c. Menerapkan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber menggunakan agent/aplikasi yang diinstal pada *endpoint*.



5. Aspek Respon ditingkatkan dengan cara:

- a. Melakukan peningkatan kapasitas SDM terutama terkait dengan pengujian keamanan, mekanisme proteksi dan penanganan suatu insiden.
- b. Menetapkan format baku dalam melakukan dokumentasi penanganan insiden keamanan siber.
- c. Menyusun standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.
- d. Melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi.



PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi Informatika dan Statistik Provinsi Nusa Tenggara Barat ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Nusa Tenggara Barat. Agar Pemerintah Daerah Provinsi Nusa Tenggara Barat melaksanakan tindak lanjut atas hasil observasi dan rekomendasi yang disampaikan pada Laporan Penilaian CSM ini dan melaporkan tindak lanjutnya kepada BSSN.

Laporan Penilaian CSM ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Nusa Tenggara Barat; dan
3. Sekretaris Daerah Provinsi Nusa Tenggara Barat.

Mataram, 14 Juli 2022

Kepala Bidang Persandian
dan Keamanan Informasi

Lalu Amjad, S.H., M.H.
19691231 199203 1 099

Sandiman Madya pada Direktorat
Keamanan Siber dan Sandi Pemerintah
Daerah

Lukman Nul Hakim, S.E., M.M.
19701116 199110 1 001

Mengetahui,
Plt. Kepala Dinas Komunikasi Informatika dan Statistik
Provinsi Nusa Tenggara Barat

Baiq Nelly Yuniarti, AP., M.Si.
19750615 199412 2 001