



2020

# LAPORAN

HASIL PENILAIAN CYBER SECURITY MATURITY  
DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK  
PROVINSI NUSA TENGGARA BARAT



# DAFTAR ISI

DAFTAR ISI .....	2
PENDAHULUAN .....	3
I. Tujuan Kegiatan .....	3
II. Ruang Lingkup Kegiatan.....	3
III. Metodologi Kegiatan .....	4
IV. Pelaksanaan Kegiatan .....	6
HASIL KEGIATAN .....	7
I. Informasi Stakeholder .....	7
II. Deskripsi Ruang Lingkup Penilaian .....	7
III. Hasil Penilaian CSM .....	9
IV. Kekuatan/Kematangan.....	11
V. Kelemahan/Kekurangan.....	17
VI. Rekomendasi .....	21
PENUTUP .....	22



# PENDAHULUAN

## I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat kematangan keamanan siber di lingkungan Dinas Komunikasi, Informatika, dan Statistik Provinsi Nusa Tenggara Barat. Dengan adanya tingkat kematangan ini diharapkan dapat memberikan gambaran dan mempermudah organisasi untuk mengetahui kekuatan dan kelemahan yang perlu ditingkatkan pada setiap aspek keamanan siber sehingga Dinas Komunikasi, Informatika, dan Statistik Provinsi Nusa Tenggara Barat maupun Badan Siber dan Sandi Negara (BSSN) dapat menyusun strategi peningkatan kematangan keamanan siber (*Cyber Security Maturity*) dengan tepat sasaran.

## II. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek pengelolaan keamanan siber yang meliputi beberapa aspek sebagai berikut :

### 1. Tata Kelola

Aspek Tata Kelola terdiri dari sub aspek kesadaran, audit, kontrol, pemenuhan, kebijakan dan proses.

### 2. Identifikasi

Aspek Identifikasi terdiri dari sub aspek manajemen aset, inventaris, manajemen resiko, prioritas, pelaporan, dan klasifikasi.

### 3. Proteksi

Aspek Proteksi terdiri dari sub aspek jaringan, aplikasi, pengguna, manajemen identitas dan akses, cloud, dan data.

### 4. Deteksi

Aspek Deteksi terdiri dari sub aspek perubahan, monitor, peringatan, pemberitahuan, intelijen, dan pelaporan.



## 5. Respon

Aspek Respon terdiri dari sub aspek penahanan, penanggulangan, pemulihan, kegiatan paska insiden, dan pelaporan.

### III. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen pemetaan Cyber Security Maturity (CSM), wawancara/diskusi, dan melihat ketersediaan dokumen dan/atau data dukung pendukung pengisian instrumen. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas tiap aspek Keamanan Siber.

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

Nilai Level Kematangan dikategorikan menjadi :

- Level 1 (Implementasi Awal)

Rentang nilai yang dikategorikan pada level 1 yaitu mulai dari 0 sampai dengan 1.5. Pada level 1 (satu) ini menggambarkan bahwa dalam penerapan keamanan siber tidak ada proses yang terorganisir, bersifat informal, tidak dilakukan secara konsisten, dan tidak dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini tidak dapat terukur dengan baik dan organisasi memiliki tingkat risiko siber yang sangat tinggi.

- Level 2 (Implementasi Berulang)

Rentang nilai yang dikategorikan pada level 2 yaitu lebih dari 1.5 sampai dengan kurang dari 2.5. Pada level 2 (dua) ini menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir, bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini tidak dapat terukur dengan baik dan organisasi memiliki tingkat risiko siber yang tinggi



- Level 3 (Implementasi Terdefinisi)

Rentang nilai yang dikategorikan pada level 3 yaitu mulai dari 2.5 sampai dengan kurang dari 3.5. Pada level 3 (tiga) ini 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.

- Level 4 (Implementasi Terkelola)

Rentang nilai yang dikategorikan pada level 4 yaitu mulai dari 3.5 sampai dengan kurang dari 4.5. Pada level 4 (empat) ini 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.

- Level 5 (Implementasi Optimal)

Rentang nilai yang dikategorikan pada level 5 yaitu mulai dari 4.5 sampai dengan 5. Pada level 5 (lima) ini menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan baik, diterapkan proses otomatisasi, bersifat formal, dilakukan secara berulang secara konsisten, direviu berkala, serta penerapan perbaikan dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini dapat terukur dengan sangat baik dan keamanan siber telah menjadi bagian budaya secara menyeluruh di organisasi.



## IV. Pelaksanaan Kegiatan

1. Pengisian setiap pertanyaan dari *Tools CSM* oleh responden dari Dinas Komunikasi, Informatika, dan Statistik Provinsi Nusa Tenggara Barat dengan asistensi BSSN dilakukan pada tanggal 10 - 11 Desember 2020.
2. Validasi Pemetaan CSM

Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen keamanan siber. Kegiatan validasi dilaksanakan pada 10 - 11 Desember 2020.



# HASIL KEGIATAN

## I. Informasi Stakeholder

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

Provinsi Nusa Tenggara Barat

Alamat : Jl. Udayana No. 14 Kota Mataram, Nusa Tenggara Barat

Nomor Telp./Fax. : (0370) 644264

Email : kominfotik@ntbprov.go.id

Narasumber Instansi/Lembaga :

1. Widayati Tjatur Suryadi, SH, MM
2. Lalu Arief Gunawan, S.E, M.Si
3. Syamsul Bahri, S.Kom, M.T
4. Robert Silas Kabanga, S.Kom, M.Eng
5. Robi Ramadhan Syah, S.Kom
6. Dany Ilham Iswara

## II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

Organisasi Keseluruhan  Regional, Kanwil, Cabang  Unit Kerja  Lainnya

2. Unit Kerja : Diskominfo dan Statistik Provinsi Nusa Tenggara Barat

3. Fungsi Kerja

Dinas Komunikasi, Informatika, dan Statistik Pemerintah Provinsi Nusa Tenggara Barat memiliki tugas dan fungsi yang diatur dalam Peraturan Gubernur Nusa Tenggara Barat Nomor 46 Tahun 2018 tentang Perubahan Kedua Atas Peraturan Gubernur Nusa Tenggara Barat Nomor 50 Tahun 2016 tentang Kedudukan, Susunan



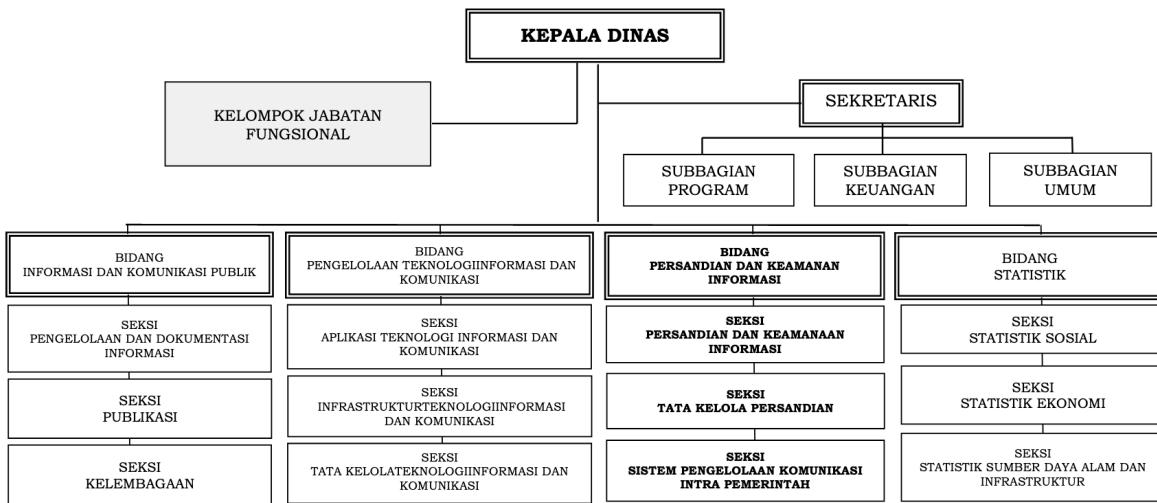
Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas - Dinas Daerah Provinsi Nusa Tenggara Barat Pasal.

Untuk menyelenggarakan tugas pokok Dinas Komunikasi, Informatika, dan Statistik Provinsi Nusa Tenggara Barat mempunyai fungsi sebagai berikut :

- a. Perumusan kebijakan teknis Bidang Informasi dan Komunikasi Publik, Bidang Pengelolaan Teknologi Informasi dan Komunikasi, Bidang Persandian dan Keamanan Informasi, dan Bidang Statistik;
- b. Pelaksanaan kebijakan teknis Bidang Informasi dan Komunikasi Publik, Bidang Pengelolaan Teknologi Informasi dan Komunikasi, Bidang Persandian dan Keamanan Informasi, dan Bidang Statistik;
- c. Pelaksanaan Evaluasi dan Pelaporan Bidang Komunikasi Publik, Bidang Pengelolaan Teknologi Informasi dan Komunikasi, Bidang Persandian dan Keamanan Informasi, dan Bidang Statistik;
- d. Pelaksanaan Administrasi Dinas Komunikasi Informatika dan Statistik Pemerintah Provinsi Nusa Tenggara Barat; dan
- e. Pelaksanaan fungsi lain yang diberikan oleh Gubernur yang berkaitan dengan tugas dan fungsinya.

Dalam melaksanakan tugas dan fungsinya, Dinas Komunikasi Informatika dan Statistik Provinsi Nusa Tenggara Barat memiliki susunan organisasi yang terdiri atas :

- a. Kepala Dinas;
- b. Sekretariat;
- c. Bidang Informasi dan Komunikasi Publik;
- d. Bidang Pengelolaan Teknologi Informasi dan Komunikasi;
- e. Persandian dan Keamanan Informasi;
- f. Bidang Statistik dan
- g. Kelompok Jabatan Fungsional.



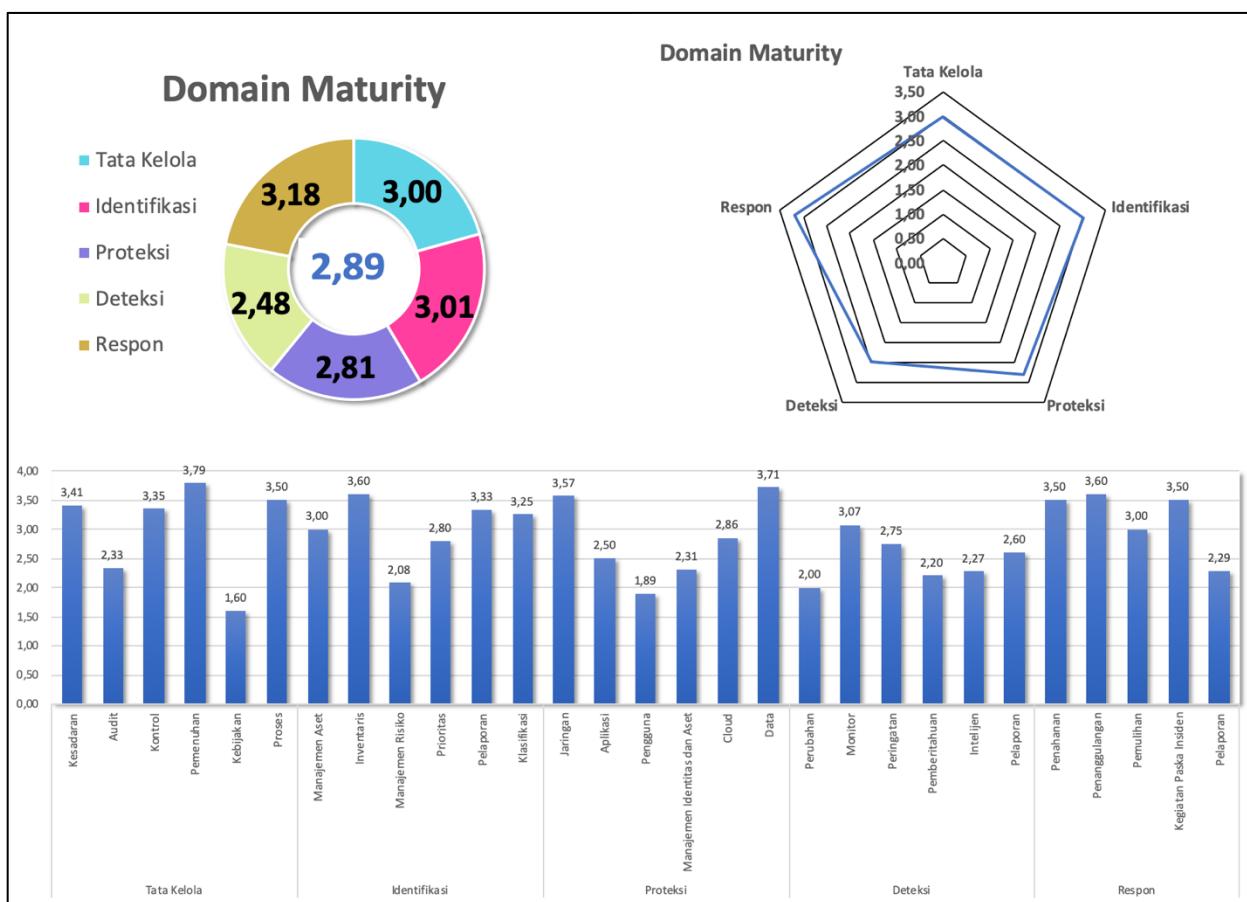
Gambar 1 Struktur Organisasi Dinas Komunikasi, Informatika, dan Statistik Provinsi NTB

### III. Hasil Penilaian CSM

Berdasarkan wawancara dan diskusi dalam rangka validasi pengisian *Cyber Security Maturity* diperoleh hasil sebagai berikut:

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
3,00		3,01		2,81		2,48		3,18	
Kesadaran	3,41	Manajemen Aset	3,00	Jaringan	3,57	Perubahan	2,00	Penahanan	3,50
	2,33		3,60	Aplikasi	2,50	Monitor	3,07	Penanggulangan	3,60
Audit	2,33	Inventaris	2,08	Pengguna	1,89	Peringatan	2,75	Pemulihan	3,00
	3,35		2,80	Manajemen Identitas dan Aset	2,31	Pemberitahuan	2,20	Kegiatan Paska Insiden	3,50
Kontrol	3,79	Prioritas	3,33	Cloud	2,86	Intelijen	2,27	Pelaporan	2,29
	1,60		3,25	Data	3,71	Pelaporan	2,60		
Proses	3,50	Klasifikasi							

Gambar 2 Hasil Penilaian Provinsi NTB per Aspek pada Cyber Security Maturity



Gambar 3 Grafik Hasil Penilaian CSM pada Pemerintah Provinsi NTB

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

**Total Score Indeks Kematangan : 2,89**

Sehingga perhitungan penentuan Level Kematangan didapatkan tingkat level kematangan sebagai berikut :

**Tingkat Kematangan Level 3**



## IV. Kekuatan/Kematangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kekuatan keamanan siber pada Dinas Komunikasi, Informatika & Statistik Provinsi Nusa Tenggara Barat sebagai berikut:

### a. Aspek Tata Kelola

1. Program pemahaman kesadaran keamanan informasi telah dilakukan secara berkelanjutan setidaknya setahun sekali untuk semua karyawan dan diperbaharui secara berkala dengan menyesuaikan terhadap teknologi baru, standar, dan persyaratan bisnis serta mengatasi adanya ancaman.
2. Semua karyawan mengetahui dan menerapkan kebijakan keamanan informasi.
3. Setiap karyawan baru di Organisasi mendapatkan pengarahan mengenai keamanan informasi.
4. Dinas Kominfo dan Statistik telah memberitahukan kepada OPD tentang teknik atau kerentanan siber yang berkembang saat ini yang dapat digunakan dalam peningkatan risiko fraud/penipuan.
5. Memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi dan dilakukan proses reviu secara berkala serta telah dipastikan sesuai dengan persyaratan dalam undang-undang dan peraturan terkait lainnya yang berlaku.
6. Melakukan reviu security risk assessment secara berkala minimal 1 tahun sekali
7. Pelaksanaan internal audit telah dilakukan setiap setahun sekali.
8. Diagram yang menggambarkan Aliran data di seluruh sistem jaringan telah didokumentasikan dan dilakukan pembaruan setiap ada perubahan.
9. Standar konfigurasi (port, protokol, service) telah diterapkan dan didokumentasikan.
10. Sistem manajemen keamanan informasi telah dipastikan dapat mencapai hasil yang diharapkan.
11. Semua tanggungjawab keamanan informasi telah ditentukan dan dialokasikan secara menyeluruh.



12. Organisasi telah mewajibkan semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan yang ditetapkan dan prosedur organisasi.
13. Program untuk vulnerability assessment atau penetrating testing pada aplikasi web, aplikasi client-based, aplikasi mobile, wireless, server dan perangkat, jaringan telah dilaksanakan secara berkala.
14. Dilakukan pemisahan environment antara sistem production dan development dan tidak mengizinkan akses kepada pengembang tanpa pengawasan dari bagian keamanan organisasi
15. Aplikasi web organisasi telah dilindungi menggunakan firewall aplikasi web (WAFs).
16. Alamat IP internal di organisasi telah dilindungi oleh NAT (Network Address Translation)
17. Penggunaan IDS/IPS telah diterapkan jaringan internal dan jaringan perimeter, serta diperbarui secara regular dengan threat intelligence.
18. Risk register terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
19. Dilakukan filterisasi terhadap seluruh jenis file lampiran email
20. Peraturan, persyaratan kontrak, dan peraturan lainnya telah diidentifikasi, didokumentasi dan diperbarui untuk setiap sitem informasi.
21. Kontrol kriptografi telah diterapkan sesuai dengan peraturan yang berlaku.
22. Prosedur untuk memastikan kepatuhan terhadap peraturan perundangan dan persyaratan kontrak yang berhubungan dengan hak kekayaan intelektual serta penggunaan produk perangkat lunak proprietary telah diterapkan.
23. Dokumentasi yang dimiliki organisasi dilindungi dan dijaga agar tidak hilang, hancur, dipalsukan, diakses oleh pihak yang tidak sah sesuai dengan persyaratan dan peraturan.



24. Kebijakan Perlindungan Data stakeholder / klien / konsumen / pelanggan secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi yaitu referensi untuk pedoman pemrosesan dan persyaratan data pribadi.
25. Menyampaikan kebijakan data privasi kepada OPD segera setelah terjalin kerjasama dan telah berkomunikasi dengan OPD terkait data pribadi yang digunakan dan dikelola oleh masing-masing OPD.
26. 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.
27. Memiliki kebijakan yang menetapkan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber
28. Kebijakan keamanan informasi mengatur mengenai single ID yang unik untuk melakukan semua otentikasi
29. Kebijakan terminasi diterapkan dengan masa tenggang yang diizinkan terkait hak akses karyawan ke dalam sistem informasi berupa hak akses segera dinonaktifkan
30. Kebijakan dan prosedur keamanan informasi telah dikembangkan sesuai dengan kerangka kerja dan standar yang diakui yaitu menggunakan ISO 270001.
31. Menerapkan praktik secure coding yang sesuai dengan bahasa pemrograman dan development environment yang digunakan
32. Source code yang dibuat secara mandiri dilakukan reviu kerentanannya terlebih dahulu oleh pihak ketiga menggunakan teknis otomatis dan manual sebelum masuk ke production
33. Menghimpun dan menjaga informasi dari pihak ketiga yang akan digunakan untuk melaporkan insiden keamanan, seperti penegakan hukum, departemen pemerintah terkait, vendor, dan mitra ISAC
34. Melakukan penetrating testing menggunakan pihak eksternal dan internal secara berkala



35. Prosedur Otorisasi/persetujuan untuk menambah / mengubah / menghapus hak akses ketika terjadi perpindahan karyawan.

**b. Aspek Identifikasi**

1. Melakukan perencanaan kapasitas secara berkelanjutan untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan
2. Seluruh aset yang diidentifikasi telah disusun berdasarkan klasifikasi kritikalitas (berdasarkan analisis risiko operasional, analisis bisnis, dan analisis strategis organisasi) serta telah ditetapkan penanggung jawab untuk setiap aset tersebut
3. Melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi
4. Kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi
5. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
6. Melakukan segmentasi jaringan berdasarkan fungsionalitas (segmen bagian development, keuangan, SDM, dll) dengan kontrol keamanan antar segmen

**c. Aspek Proteksi**

1. Memiliki IPS yang terkonfigurasi dan diupdate
2. Koneksi ke perangkat server dan jaringan di organisasi Anda menggunakan protokol terenkripsi seperti SSH, secure RDP, dll
3. Penggunaan firewall telah di konfigurasi dengan baik seperti implicit atau explicit deny any/any rule, inbound dan outbound network traffic;
4. Menerapkan port access control pada perangkat yang terhubung;
5. Menerapkan DNS Filtering;
6. Email system di organisasi (termasuk yang ada di cloud) memiliki pengecekan otomatis terhadap spam / phishing / malware
7. Menerapkan semua metode otentikasi melalui saluran terenkripsi
8. Akses ke data OPD diatur dengan hak akses



9. Dapat melacak dan dapat mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun stakeholder / klien / konsumen / pelanggan
10. Pengguna selain admin database hanya memiliki akses read-only pada akses ke database
11. Hanya mengizinkan traffic pada layanan cloud untuk kebutuhan bisnis organisasi
12. Semua data OPD dienkripsi saat dikirim
13. Semua critical system clocks telah disinkronkan dengan metode otomatis seperti Network Time Protocol

**d. Aspek Deteksi**

1. Perubahan konfigurasi pada peralatan jaringan terdeteksi secara otomatis
2. Melakukan deteksi akses Wireless Access Point pada Jaringan LAN
3. Aktivitas pihak ketiga di organisasi dipantau untuk mendeteksi adanya potensi kejadian keamanan siber
4. Memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber
5. Melakukan monitoring log dari perangkat security control, jaringan dan aplikasi
6. Monitoring akses pengguna, koneksi jaringan, perangkat lunak dan keras;
7. Dapat mendeteksi kegagalan login pada akun admin pada perangkat jaringan, server, dan aplikasi
8. Log hasil deteksi malware terhubung dengan perangkat anti-malware administrations dan event log servers sehingga dapat digunakan untuk analisis
9. Memiliki ticketing system yang digunakan untuk melacak progres dari events post-notification
10. Mendeteksi aktivitas anomali login seperti waktu, lokasi, durasi
11. Memiliki contact tree untuk melakukan eskalasi dalam melakukan respon kejadian;
12. Mendapatkan isu keamanan siber terkini
13. Memiliki sistem untuk mendeteksi adanya Malicious Code



14. Mendeteksi Indicator of Compromise (IoC), artefak jaringan, malware, prosedur dan teknik yang digunakan dalam serangan siber

**e. Aspek Respon**

1. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait
2. Melakukan perencanaan skenario penanganan insiden secara rutin kepada karyawan pengelola TI
3. Melakukan backup data yang ada di pc/laptop karyawan ke cloud organisasi
4. Tim respon insiden siber di organisasi Anda memiliki peralatan sumber daya analisis insiden (misalnya daftar host, packet snifer, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar asset penting, alat digital forensic, dan sebagainya)
5. Jika organisasi mengalami insiden siber, 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)
6. 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
7. 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. Laporan insiden di organisasi dilaporkan ke top management dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi



## V. Kelemahan/Kekurangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kelemahan/kekurangan keamanan siber pada Dinas Komunikasi, Informatika & Statistik Provinsi Nusa Tenggara Barat sebagai berikut:

### a. Aspek Tata Kelola

1. Belum melakukan simulasi phising setidaknya setiap tahun
2. Belum memiliki tools untuk melakukan Vulnerability Scanning dan belum menggunakan akun khusus dalam proses Vulnerability Scanning
3. Belum memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi dan dilakukan proses reviu secara berkala
4. Belum melakukan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
5. 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.
6. Belum menerapkan kebijakan pengelolaan anti-virus secara terpusat;
7. Belum menerapkan metode sandbox pada lampiran email yang dikomunikasikan.
8. Belum ada kegiatan penelusuran yang memastikan bahwa data OPD yang disimpan adalah data yang akurat
9. Belum melakukan kegiatan pengukuran tingkat kepatuhan pengguna dalam implementasi kebijakan keamanan informasi.
10. Belum terdapat dokumen BCP dan DRP
11. Belum mempunyai kebijakan yang menetapkan sanksi yang dijatuhan saat terdapat pelanggaran dalam hal keamanan siber
12. Belum mengatur mengenai Single ID



### b. Aspek Identifikasi

1. Belum terdapat kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi
2. Belum terdapat dokumentasi alur informasi pada stakeholder atau konstituen
3. Belum dilakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman
4. Belum memiliki Business Impact Analysis
5. Belum dilakukannya review dalam melakukan klasifikasi aset TI

### c. Aspek Proteksi

1. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint
2. Belum dilakukan pembatasan penggunaan scripting tools (seperti: Microsoft PowerShell dan Python) di organisasi
3. Belum menerapkan pengaturan akses (read/write) terhadap perangkat USB/media penyimpanan eksternal
4. Belum penerapan Multi-Factor Authentication (MFA) yang digunakan untuk mengakses data sensitif (misal data pribadi, data keuangan, dll)
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 OPD dienkripsi saat disimpan
9. Penyimpanan data backup belum dilindungi secara tepat, baik secara fisik maupun non fisik (seperti: enkripsi, dsb)

### d. Aspek Deteksi



1. Semua perubahan konfigurasi belum melalui proses Change Management System dan tidak dilakukan reviu secara berkelanjutan
2. Belum terdapat mekanisme monitoring terhadap akses dan perubahan pada data sensitif? (seperti File Integrity Monitoring atau Event Monitoring)
3. Belum memiliki mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah
4. Belum melakukan monitoring terhadap log dari perangkat security control, jaringan, dan aplikasi
5. Belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data OPD contohnya penggunaan DLP (Data Loss Prevention)
6. Belum menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi, dan analisis log
7. Escalation profile belum dibuat untuk setiap security event yang ditemukan, dan tidak disimpan sebagai panduan untuk digunakan di masa mendatang
8. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal
9. Belum memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber
10. Threat intelligence feeds belum dikonfigurasi secara otomatis untuk memperbarui kontrol pencegahan, seperti pembaruan signature IPS, update rules, dan konfigurasi lainnya
11. Belum menjalankan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber menggunakan agent/aplikasi yang diinstal pada endpoint.
12. Belum memiliki sistem yang untuk mendeteksi ancaman siber sehingga dapat memberikan input/feed bagi threat intelligence seperti penggunaan deception technology
13. Belum memiliki sistem untuk melakukan Malicious Code Detection untuk mendeteksi, menghapus, dan melindungi dari malicious code



14. Belum memiliki unit yang melakukan Cyber Threat Intelligence (CTI)
15. Metrik security event belum reviu untuk tujuan operasional

**e. Aspek Respon**

1. Belum membuat skema penilaian insiden dan prioritas berdasarkan potensial dampak (aspek kerugian operasional, bisnis, reputasi, dan hukum) bagi organisasi
2. Belum memberikan pelatihan untuk karyawan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi
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. Belum melakukan reviu terhadap root cause dari suatu insiden siber untuk mencegah kejadian serupa berulang
7. Belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan
8. Belum memiliki metrik perhitungan biaya untuk mencegah insiden siber yang menggunakan metode perhitungan ROI (Return of Investment) pada program keamanan siber di organisasi menggunakan sumber referensi terpercaya dalam menentukan skala prioritas tindakan mitigasi risiko dan meminimalisir kerugian biaya akibat terjadinya insiden siber.



## 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. Secara umum diperlukan peningkatan terhadap faktor-faktor yang menjadi kelemahan/kekurangan pada aspek tata kelola, aspek identifikasi, aspek proteksi, aspek deteksi, dan aspek respon.
2. Melaksanaan peningkatan kapasitas SDM terutama terkait dengan pengujian keamanan, mekanisme proteksi dan penanganan insiden
3. Menyusun Pedoman dan Kebijakan Penerapan Keamanan Informasi mengacu pada Standar ISO 27001 khususnya terkait dengan Penerapan kriptografi, Mekanisme Penghapusan Data, dan Pengendalian terhadap Aset Informasi.
4. Menyusun Risk Register berdasarkan kriteria ISO 31000 terkait dengan manajemen risiko yang diantaranya memetakan terkait Aset, Kerentanan, Ancaman, Kemungkinan, Dampak, Level Risiko, Proses Mitigasi, dan Penanggungjawab
5. Menyusun Dokumen Bussiness Continuity Plan, Disaster Recovery Plan, Business Impact Analysis untuk melihat proses bisnis dan aset kritikal berdasarkan aspek Kerahasiaan, keutuhan, ketersediaan, otentikasi dan Anti penyangkalan sehingga dapat dirumuskan prioritas penanganan risiko.
6. Menetapkan format baku dalam melakukan dokumentasi penanganan insiden keamanan siber.



# PENUTUP

Demikian disampaikan laporan kegiatan penilaian CSM pada Dinas Komunikasi, Informatika, dan Statistik Pemerintah Provinsi Nusa Tenggara Barat, sebagai bahan masukan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Mataram, 11 Desember 2020

Kabid Persandian dan Keamanan Informasi

(Widajati Tjatur Surjadi, S.H., M.M.)

Tim BSSN

(Marcelina Tri N. W., S.Sos., M.Si(han).)