2022

# LAPORAN

## HASIL PENILAIAN

## *CYBER SECURITY MATURITY* (CSM)

## DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK PROVINSI DKI JAKARTA

# 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 DKI Jakarta 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:

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

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 Juli 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 25 – 27 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfo dan Statistik Provinsi DKI Jakarta. Tim BSSN yang terlibat:

   1) Marcelina Tri Nasiti Widayatmi, S.Sos., M.Si (han)
   2) Irma Nurfitri Handayani, S.ST.
   3) Aprita Danang Permana, S.ST., M.Kom.
   4) Carissa Mega Yulianingrum, S.Tr.TP.

# HASIL KEGIATAN

## I. Deskripsi Ruang Lingkup Penilaian

Nama Instansi/Lembaga : Diskominfo dan Statistik Provinsi DKI Jakarta
Alamat : Jl. Medan Merdeka Selatan no 8-9 Blok H Lantai 13, Jakarta Pusat 10110
Nomor Telp./Fax. : (021) 3822357
Email : diskominfotik@jakarta.go.id
Pimpinan Instansi/Lembaga : Atika Nur Rahmania, S.IP., M.Si.
Narasumber Instansi/Lembaga :

1) R. Boedi Setiawan
2) Andrie Yuswanto
3) Tony Yudianto
4) Reihan Adinata
5) Tanti Widyaningrum
6) Lamria Simatupang
7) Andy Susanto
8) Rycan Fahmi
9) M. Taufik Hidayat
10) Iman Pribadi
11) Venny Yulianty
12) Arif Buchari Marpaung
13) Novaldo Caesar
14) Rina Yuliani Fadila

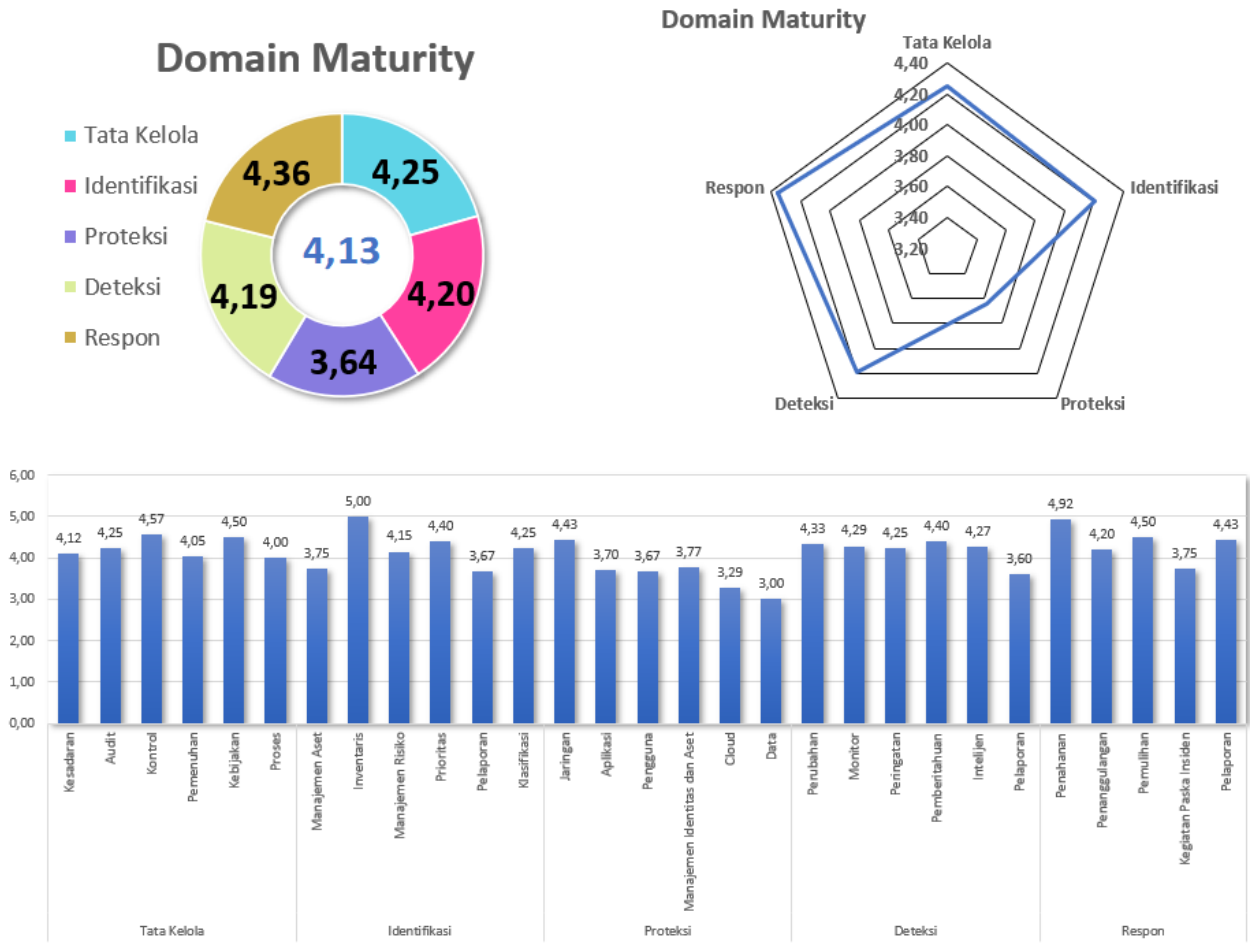
## II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja* : Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta

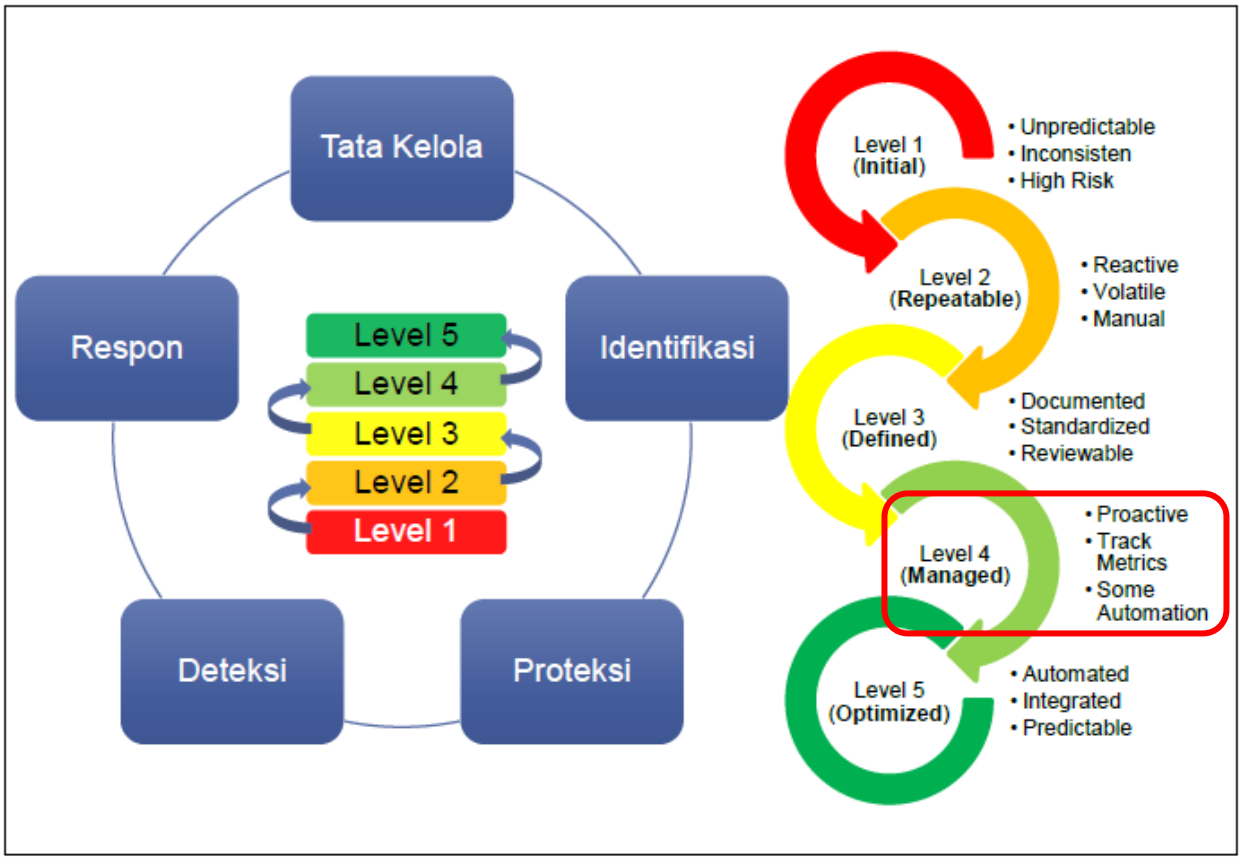
# III. Hasil Penilaian CSM




Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 4,13**, 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 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat formal, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan.

**Catatan:**

Berdasarkan penilaian CSM yang telah dilakukan pada tahun 2020 dengan total skor indeks kematangan adalah 4,06, terdapat kenaikan 0,07 poin menjadi 4,13 dengan kategori level yaitu level 4.

# IV. Kekuatan/Kematangan

**Tata Kelola**

1. Organisasi secara berkala dan berkelanjutan telah menerapkan program kesadaran keamanan informasi pada sebagian besar pegawai.
2. Organisasi telah melaksanakan audit dan kontrol keamanan siber dengan melakukan kegiatan *vulnerability scanning* dan *risk assessment* oleh tim yang sudah dibentuk.
3. Organisasi telah melakukan pelatihan keamanan informasi secara terjadwal untuk pegawai berdasarkan *roadmap baseline* pendidikan dan pelatihan.
4. Organisasi secara formal membuat dan menyampaikan kebijakan/prosedur keamanan informasi.
5. Organisasi telah mewajibkan pegawai dan kontraktor menerapkan kebijakan/prosedur keamanan informasi.
6. Organisasi telah memastikan dalam pengembangan perangkat lunak/sistem informasi/aplikasi dilakukan analisis statis dan dinamis, dan memastikan versi yang dipakai masih memiliki dukungan pengembang.
7. Organisasi secara berkala melakukan analisis risiko keamanan fisik dan sistem elektronik.
8. Organisasi telah memperhatikan dasar-dasar keamanan informasi, seperti pemisahan lingkungan *production* dan *development*, melakukan pengujian komponen penting dari aplikasi, menerapkan praktik secure coding dan memastikan dilakukan pengecekan kesalahan pada semua input pada aplikasi, menerapkan NAT secara menyeluruh, filterisasi lampiran *email*, pengaturan *Single* ID / *Single Sign On* untuk melakukan akses kepada aplikasi milik organisasi, penggunaan NAC, WAF, AV, IDS/IPS.
9. Organisasi telah memiliki dokumen BCP, DRP, penilaian risiko keamanan dan pengendaliannya, serta diriview secara berkala.
10. Kegiatan *threat hunting* sudah dilakukan secara berkala/rutin.

**Identifikasi**

1. Organisasi telah melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan.
2. Organisasi telah melakukan inventaris terhadap aset perangkat lunak dan perangkat keras secara berkala dan setiap ada perubahan.
3. Organisasi telah mengidentifikasi dan mebatasi akses perangkat yang tidak diizinkan oleh organisasi.
4. Organisasi telah melakukan klasifikasi informasi dan melakukan inventarisasi.
5. Organisasi telah memiliki kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
6. Organisasi telah memiliki kebijakan dan implementasi mengenai retensi data sensitif.
7. Organisasi secara berkala telah melakukan *vulnerability scanning/penetration testing* terhadap smeua aset perangkat dan aplikasi organisasi.
8. Organisasi telak melakukan klasifikasi secara terorganisir dan berkelanjutan dalam klasifikasi TI dan *cyber threat*.
9. Organisai telah melakukan segmentasi jaringan berdasarkan fungsionalitas.
10. Organisasi telah konsisten menjadikan aspek keamanan menjadi pertimbangan dan diprioritaskan dalam beberapa pengambilan keputusan TI. Upaya remedasi telah didasarkan pada level risiko serta dilakukan langkah proteksi untuk memprioritaskan data dan aset kritis.
11. Organisasi telah konsisten melakukan manajemen risiko dengan menerapkan *screening* terhadap pihak ketiga ketika menggunakan aset mereka pada jaringan organisasi. Selain itu, terdapat *risk register* yang didukumentasikan untuk semua aplikasi.
12. Organisasi sudah mengidentifikasi seluruh aset berdasarkan klasifikasi kritikalitas serta telah ditetapkan penanggung jawab untuk setiap aset.
13. Organisasi menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi (seperti *port*, akses *smartphone*, dll).

**Proteksi**

1. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan *firewall* dan IPS beserta pengaturannya, mengkonfigurasikan sistem dan protokol terenkripsi, serta melakukan *filtering* pada *inbound /outbond network traffic* serta *filtering* terhadap layanan DNS.
2. Organisasi telah melakukan manajemen aplikasi yang dimiliki dengan konsisten, berupa *patching* aplikasi, memastikan aplikasi masih memiliki *update support* dan memastikan *master images server* tersimpan dengan aman.
3. Organisasi telah menerapkan pembatasan akun pengguna dan perlindungan *user* dengan menggunakan URL *filtering*, *device control*, dan *application control*.
4. Organisasi telah melakukan manajemen identitas dan akses dengan menggunakan identitas dan akses kengguna untuk pembatasan hak akses pada jaringan, database, transaksi dan data lain.
5. Organisasi telah membatasi aplikasi yang dapat diunduh, diinstal dan dioperasikan dan telah menggunakan *anti virus* pada semua perangkat *endpoints*, termasuk *server*.
6. Organisasi telah menggunakan *server* terpisah untuk semua aplikasi yang dipakai organisasi.
7. Email system di organisasi telah memiliki pengecekan otomatis terhadap *spam/phishing/malware*.

**Deteksi**

1. Organisasi telah menerapkan *monitoring* (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan, *log* dari perangkat *security control*, jaringan dan aplikasi.
2. Organisasi telah melakukan *record* terhadap perubahan dengan deteksi perubahan konfigurasi perangkat jaringan.

3. Organisasi telah memiliki sistem *monitoring* yang aktif terhadap akses fisik dan logic dan mempersiapkan peningkatan keterampilan bagi tim *monitoring*.
4. Dalam hal peringatan, organisasi sudah dapat mendeteksi kegagalan login pada akun, adanya alert jika terdapat port yang tidak sah terdeteksi pada suatu sistem.
5. Organisasi telah memiliki perangkat *anti-malware* yang secara otomatis melakukan *scanning* terhadap *removable media* yang terhubung ke perangkat.
6. *System ticketing* sudah diberlakukan berdasarkan dampak dan event notification berbeda-beda untuk setiap jenis eskalasi.
7. Organisasi telah memiliki sistem untuk mendeteksi ancaman siber.

**Respon**

1. Organisasi telah memiliki SOP dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Organisasi telah melakukan latihan respon insiden secara rutin dan memberikan pelatihan kepada para personil TI dan Sebagian besar pegawai mengenai tentang cara identifikasi, penanganan dan pelaporan suatu insiden.
3. Organisasi memastikan desain jaringan yang aman dengan pemisahan server DMZ ketika terjadi compromise.
4. Organisasi memiliki sumber daya redundan yang cukup (75%-95%) untuk kondisi sistem kritikal yang terganggu karena insiden siber.
5. Organisasi memiliki format baku untuk pencatatan respon insiden, dan tim respon dipastikan dapat menlakukan pencatatan setiap langkah dalam penanggulangan insiden
6. Dalam kegiatan pasca insiden, organisasi dapat memastikan pencapaian SLA dalam penganganan insiden.
7. Laporan insiden di organisasi sudah dilaporkan ke *middle* dan *top management* serta ke pihak eksternal yang berkepentingan.

# V. Kelemahan/Kekurangan

**Tata Kelola**

1. Organisasi belum melakukan dan mendokumentasikan simulasi serangan *phising* secara berkala, namun telah menyusun skenario simulasinya.
2. Belum adanya kontrol untuk mengukur kepatuhan pengguna terhadap kebijakan keamanan informasi organisasi, misalnya seperti survey atau yang lainnya, tetapi sudah menyusun kuesioner survey.
3. Organisasi belum memiliki BCP dan DRP yang mencakup *backup* dan *restoration* dari data pribadi.
4. Organisasi belum memiliki kebijakan atau prosedur mengenai pemberitahuan jika terjadi pelanggaran terhadap data pribadi.
5. Organisasi belum melakukan reviu terhadap kebijakan yang mengharuskan penerapan perlindungan data pribadi.

**Identifikasi**

1. Metode atau standar untuk klasifikasi data organisasi belum dikontrol dengan DRM (*Digital Right Management*) dan belum didukung dengan DLP (*Data Lost Prevention*).
2. *Roadmap* keamanan TI organisasi diperbarui masih berdasarkan adanya permintaan kebutuhan dari regulator.

**Proteksi**

1. Karyawan di organisasi belum mengaktifkan fitur *wireless* pada perangkatnya hanya sesuai kebutuhan organisasi.
2. Organisasi belum melakukan pembatasan penggunaan *scripting tools*.

3. Organisasi belum memastikan penggunaan *add-on* dan *plugin* aplikasi sudah sesuai dengan ketentuan organisasi.
4. Organisasi belum menggunakan *Next Generation Endpoint Protection*.
5. Organisasi belum secara optimal memanfaatkan *Multi-Factor Authentication* untuk semua akses jaringan dan mengakses data sensitif serta menambahkan verifikasi *One Time Password* (OTP) melalui SMS, WhatsApp Messenger, Telepon, Elektronil Mail, Google Authenticator, atau media lainnya untuk transaksi yang berisiko tinggi.
6. Organisasi belum menerapkan *single sign-on* dan *multi-factor authentication* pada *cloud* serta belum membatasi akses *traffic* ke *cloud* hanya dari alamat IP yang dikenal.

**Deteksi**

1. Organisasi belum memiliki sistem untuk me*monitoring* dan mencegah kehilangan data sensitif (belum menggunakan DLP).
2. Belum ada notifikasi secara otomatis kepada admin saat terjadi kegagalan login pada akun admin pada perangkat jaringan, *server* dan aplikasi.
3. Organisasi belum mengaktifkan DNS *query logging* dalam mendeteksi *hostname lookups* untuk mengetahui adanya *malicious domain*.
4. Mekanisme *sharing* informasi hasil deteksi baru untuk internal saja.

**Respon**

1. Pelatihan tentang cara identifikasi, penanganan dan pelaporan suatu insiden hanya dilaksanakan untuk personil IT dan sebagian pegawai.
2. Belum memiliki metode yang terdokumentasi dan diinformasikan kepada *stakeholder* untuk melaporkan penyalahgunaan informasi *stakeholder*.

# VI. Rekomendasi

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
    a. Melakukan dan mendokumentasikan simulasi serangan *phising* secara berkala dengan menerapkan skenario simulasi yang telah dibuat.
    b. Menyediakan kontrol untuk mengukur kepatuhan pengguna terhadap kebijakan keamanan informasi organisasi, misalnya seperti survey/kuesioner, yang kemudian didistribusikan ke karyawan.
    c. Menambahkan cakupan *backup* dan *restoration* data pribadi pada dokumen BCP dan DRP yang telah dimiliki.
    d. Menyusun kebijakan atau prosedur mengenai pemberitahuan jika terjadi pelanggaran terhadap data pribadi yang bisa dimasukkan dalam kebijakan perlindungan data pribadi.
    e. Melakukan reviu terhadap kebijakan yang mengharuskan penerapan perlindungan data pribadi.
    f. Melakukan perubahan terhadap kebijakan izin akses pengguna misalnya dengan dari yang sebelumnya mengganti *password* 3 bulan sekali menjadi kompleksitas *password*nya harus yang baik.
    g. Menyusun kebijakan metode penghapusan data yang di dalamnya termasuk terhadap *mobile devices*.
    h. Menerapkan keamanan informasi di semua proyek TI termasuk fase perencanaan, pembangunan, dan pengembangannya.

2. Aspek ldentifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
    a. Metode atau standar untuk klasifikasi data organisasi sebaiknya dikontrol dengan DRM (*Digital Right Management*) dan DLP (*Data Lost Prevention*).
    b. Sebaiknya memperbaharui *roadmap* keamanan TI organisasi dalam jangka waktu tertentu berdasarkan perubahan kondisi lingkungan eksternal maupun internal organisasi.

c. Perlu mendokumentasikan proses dan prosedur manajemen *patch* untuk semua aset perangkat dan aplikasi.
d. Perlu pertimbangan untuk pengelolaan data *log* keamanan informasi setiap hari secara otomatis dilaporkan kepada manajemen.

3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
   a. Diharapkan karyawan di organisasi mengaktifkan fitur *wireless* pada perangkatnya hanya sesuai kebutuhan organisasi
   b. Diperlukan pembatasan penggunaan *scripting tools*.
   c. Memastikan penggunaan *add-on* dan *plugin* aplikasi sudah sesuai dengan ketentuan organisasi, seperti Microsoft PowerShell dan Python.
   d. Diperlukan pertimbangan untuk penggunaan *Next Generation Endpoint Protection*.
   e. Pertimbangan untuk menggunakan *Multi-Factor Authentication* dan Verifikasi *One Time Password* untuk sistem informasi dengan transaksi berisiko tinggi.
   f. Menerapkan *single sign-on* dan *multi-factor authentication* pada *cloud* serta membatasi akses *traffic* ke *cloud* hanya dari alamat IP yang dikenal.
   g. Pertimbangan penggunaan *cloud resources* dan *services form* untuk dijadikan dasar dalam menentukan RTO dan RPO di dokumen *Business Continuity Plan* (BCP).
   h. Pertimbangan melakukan enkripsi pada semua perangkat *mobile* (laptop, handphone) karyawan di organisasi.
   i. Semua media penyimpanan eksternal di organisasi sebaiknya dilakukan enkripsi.
   j. Memastikan penggunaan *password* yang kompleks untuk semua akses *login* dan penggantian *password* secara berkala secara otomatis.
   k. Semua data penting di organisasi di-*backup* secara berkala dan otomatis.
   l. Semua data *stakeholder* dienkripsi saat disimpan maupun saat dikirim.

4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
    a. Memiliki sistem untuk me*monitoring* dan mencegah kehilangan data sensitif (belum menggunakan DLP).
    b. Sebaiknya ada notifikasi secara otomatis kepada admin saat terjadi kegagalan login pada akun admin pada perangkat jaringan, *server* dan aplikasi.
    c. Mengaktifkan DNS *query logging* dalam mendeteksi *hostname lookups* untuk mengetahui adanya *malicious domain*.
    d. Mekanisme *sharing* informasi hasil deteksi sebaiknya dilakukan untuk internal dan eksternal.
    e. Pertimbangan menyusun *Change Advisory Board* (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.
    f. Diperlukan penambahan perangkat yang mampu mendeteksi *malware*, perilaku anomali pengguna atau serangan secara otomatis.
    g. Sistem atau perangkat yang mendeteksi aktivitas anomali *login* seperti waktu, lokasi, durasi, dan sebagainya sebaiknya dapat ternotifikasi secara otomatis.
    h. *Top Level Management* pada organisasi sebaiknya menerima *briefing* tentang kondisi keamanan siber terkini minimal satu kali setiap bulan.

5. Aspek Respon ditingkatkan dengan cara:
    a. Organisasi dapat menyelenggarakan simulasi penanganan insiden siber, meliputi insiden *malware*, *web defacement*, DDOS, *ransomware*, dan sejenisnya.
    b. Membuat metode yang terdokumentasi dan diinformasikan kepada stakeholder untuk melaporkan penyalahgunaan informasi stakeholder.
    c. Melakukan tindakan pencegahan terhadap *root cause* dari suatu insiden siber untuk mencegah kejadian serupa berulang.
    d. Melakukan reviu setiap bulan terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan.

6. Penilaian CSM diharapkan mencakup ruang lingkup Diskominfotik Provinsi DKI Jakarta dan tidak hanya menilai satu bidang saja, tetapi setiap bidang yang ada pada Diskominfotik Provinsi DKI Jakarta. Jadi, setiap bidang dapat bekerja sama dalam penilaian yang mungkin membutuhkan data dukung dari setiap bidang tersebut dengan tujuan untuk mengetahui tingkat kematangan keamanan siber di ruang lingkup Diskominfotik Provinsi DKI Jakarta sehingga dapat dijadikan acuan dalam menyusun strategi peningkatan kematangan *cyber security* dan pengelolaan keamanan siber dengan tepat sasaran.

# PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi DKI Jakarta. Agar Pemerintah Daerah Provinsi DKI Jakarta 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 untuk disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi DKI Jakarta; dan
3. Sekretaris Daerah Provinsi DKI Jakarta.

Jakarta, 27 Juli 2022

| Kepala Bidang Siber dan Sandi | Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemda |
|---|---|
| | Ditandatangani secara elektronik oleh:<br>SANDIMAN AHLI MADYA PADA DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAH DAERAH<br>**Marcelina Tri Nasiti Widayatmi, S.Sos., M.Si (han)**<br>Pembina (IV/a) |
| R. Boedi Setiawan, S.H. | Marcelina Tri N. W., S.Sos., M.Si (han) |
| 19700917 199803 1 006 | 19750717 199412 2 001 |

Mengetahui,
Kepala Diskominfo dan Statistik
Provinsi DKI Jakarta

Atika Nur Rahmania, S.IP., M.Si.
19720406 199803 2 006