



2020

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA TENGAH



PENDAHULUAN

I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Jawa Tengah. 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.

II. 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

III. 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*) : Penerapan keamanan siber tidak ada proses yang terorganisir, bersifat informal, tidak dilakukan secara konsisten, dan tidak dilakukan secara berkelanjutan.
- Level 2(*Repeatable*): Penerapan keamanan siber proses yang dilakukan sudah terorganisir, bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan.
- Level 3 (*Defined*) : 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.
- Level 4 (*Managed*) : 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.
- Level 5 (*Optimized*): 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.

IV. Pelaksanaan Kegiatan

1. Pengisian Instrumen CSM oleh internal stakeholder (*self assessment*)

Pengisian Instrumen oleh internal stakeholder dilakukan pada 01 Desember 2020.



2. Validasi Pemetaan CSM

Validasi Pemetaan CSM dilaksanakan untuk pengecekan hasil *self assessment* isian instrumen. Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen keamanan siber. Kegiatan validasi dilaksanakan pada 01 Desember 2020.



HASIL KEGIATAN

I. Informasi Stakeholder

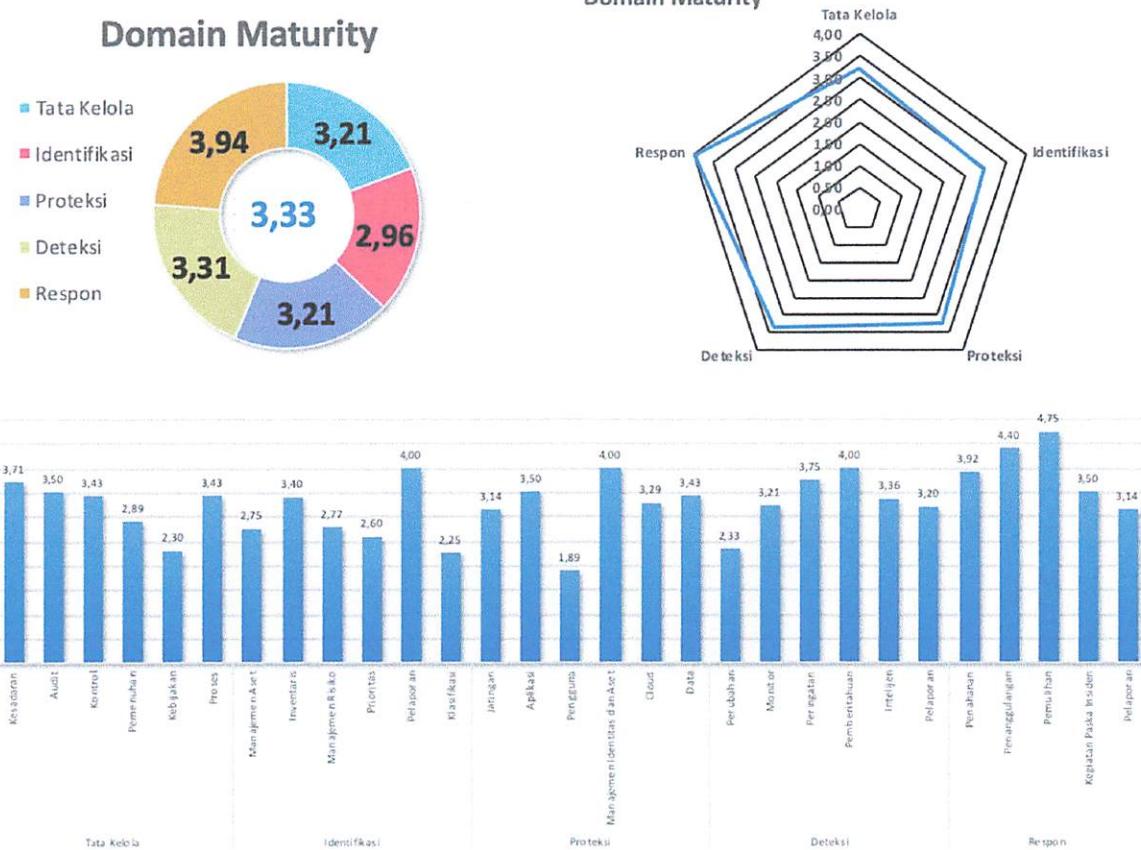
Nama Instansi/Lembaga : Diskominfo Provinsi Jawa Tengah
Alamat : Jl. Menteri Supeno 1/2 - Semarang, 50243
Nomor Telp./Fax. : (024) 8319140
Email : diskominfo@jatengprov.go.id
Narasumber Instansi/Lembaga :
1. Eny Soelastri, S.H.
 Kepala Bidang Persandian dan Keamanan Informasi
2. Subroto Budhi Utomo, S.Kom., M.T.
 Kepala Seksi Pengamanan Persandian dan Informasi
3. Widi Nugroho, M.Kom.
 Kepala Seksi Tata Kelola Persandian
4. Agus Aminudin
 Staff
5. Aminudin
 Staff
6. Mizan
 Staff

II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :
 Organisasi Keseluruhan Regional, Kanwil, Cabang Unit Kerja Lainnya
2. Instansi/Unit Kerja* : Dinas Komunikasi dan Informatika Provinsi Jawa Tengah



III. Hasil Penilaian CSM

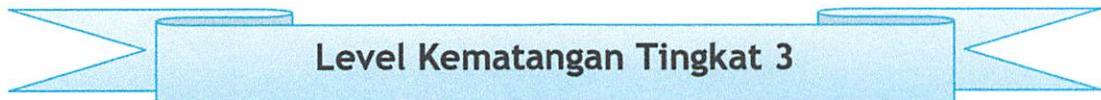




Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

Total Score Kematangan: 3,33

Sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :



IV. Kekuatan/Kematangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kekuatan keamanan siber pada Dinas Komunikasi dan Informatika Provinsi Jawa Tengah sebagai berikut:

Aspek Tata Kelola

1. Organisasi telah memiliki program kesadaran keamanan informasi yang telah dilakukan dan direview secara berkala.
2. Peningkatan kompetensi keamanan informasi telah terjadwal.
3. Organisasi telah memberikan pelatihan kepada karyawan tentang *secure authentication, social engineering, pengelolaan data sensitive*.
4. Organisasi telah melakukan manajemen kerentanan siber.
5. Organisasi telah melakukan pemeriksaan background pada karyawan baru.
6. Organisasi telah memiliki *tool vulnerability scanning* secara mandiri .
7. Organisasi menggunakan akun khusus untuk melakukan *vulnerability scanning*, dan akan dihapus jika sudah tidak terpakai.
8. Organisasi telah memiliki *risk assessment, risk treatment, internal audit* keamanan informasi.
9. Organisasi telah memiliki WAFs, *firewall* pada *end user*, NAT, DMARC, *filter* terhadap seluruh jenis file lampiran *email*.



10. Organisasi telah melakukan konfigurasi *firewall* secara berkala dan telah didokumentasikan.
11. *Vulnerability assessment* dan *penetration testing* telah dilakukan dengan melibatkan pihak internal dan eksternal.

Aspek Identifikasi

1. Organisasi telah melakukan manajemen aset secara optimal, dengan menerapkan update perencanaan kapasitas dan *update patch* terhadap semua aset.
2. Organisasi telah melakukan inventarisasi data yang ada pada semua aset perangkat keras maupun perangkat lunak. Dan aset yang diidentifikasi telah disusun berdasarkan klasifikasi kritisitas.
3. Organisasi telah melakukan manajemen resiko berupa retensi data sensitif.
4. Aspek keamanan mempertimbangkan kapasitas *server* dan perangkat jaringan secara menyeluruh.
5. Organisasi telah memiliki standar untuk melakukan klasifikasi *cyber threat*.

Aspek Proteksi

1. Penggunaan IDS dan IPS dengan menggunakan Sophos dan Fortiget.
2. Memanfaatkan sistem enkripsi dalam akses nirkabel.
3. Koneksi ke *server* dan jaringan sudah menggunakan protocol enkripsi.
4. Penggunaan *firewall* telah di konfigurasi dengan baik seperti *implicit* atau *explicit deny any/any rule, inbound network traffic* dan *outbound network traffic*.
5. Sudah menggunakan DNS *Filtering*.
6. Beberapa aplikasi sudah mulai dilakukan pemisahan sebagian besar *server* fisik maupun virtual.
7. Pengelolaan *patching* sudah dilakukan dan dilakukan secara otomatis.



8. Pada *email system* dilakukan pengecekan secara otomatis terhadap *spam/phishing/malware* menggunakan *magic spam* dan *mail server*
9. Sudah ada *white list* aplikasi dalam memastikan *authorized software library* dan *signed script*.
10. Sudah dilakukan *updating* secara berkala dalam penggunaan *web browser*, dan *email client* dalam organisasi;
11. Sistem manajemen identitas dan akses telah digunakan untuk seluruh sistem operasi.
12. *Multi-Factor Authentication (MFA)* telah digunakan pada akses LAN dan VPN serta untuk mengakses data sensitive (dengan menggunakan otentikasi dan captcha).
13. Penggunaan *password* telah digunakan pada semua akses login dan dilakukan penggantian berkala secara manual.
14. Penggunaan akses data telah diatur hak akses dan penerapan *white list* untuk memverifikasi alamat IP yang mempunyai hak akses.
15. Anomali transaksi oleh karyawan/stakeholder/klien dapat diidentifikasi dan dilakukan pelacakan/pendeteksian.
16. Organisasi sudah memiliki *cloud* internal yang memiliki proses otorisasi.
17. Data penting telah dilakukan *backup* secara berkala.
18. Penyimpanan log sudah dilakukan dalam rangka audit dan forensik.
19. Penyimpanan data *backup* sudah dilindungi baik secara fisik dan non fisik.

Aspek Deteksi

1. Organisasi melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi selama 24 jam.
2. Organisasi Anda mengaktifkan *Enable Detailed Logging* yang mencakup informasi terperinci seperti *event source*, tanggal, *user*, *timestamp*, *source addresses*, *destination addresses*, dan komponen lainnya.
3. Setiap orang yang tergabung dalam tim *monitoring* pada organisasi mendapatkan peningkatan keterampilan.



4. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
5. Organisasi memiliki perangkat *anti-malware* yang secara otomatis melakukan *scanning* terhadap *removable media* yang terhubung ke perangkat.
6. Organisasi memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
7. Organisasi memiliki *contact tree* untuk mengeskalasi dalam merespon suatu kejadian.
8. Organisasi telah memiliki mekanisme *sharing* informasi baik internal maupun eksternal.
9. Organisasi telah memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat untuk menangani kejadian prioritas tinggi dan mampu mendeteksi anomali.

Aspek Respon

1. Organisasi memiliki SOP pelaporan insiden, SOP penanganan insiden, dan *disaster recovery plan* yang telah direview secara berkala.
2. Organisasi melakukan simulasi penanganan insiden kepada karyawan secara rutin.
3. Organisasi memiliki rencana respon insiden dan daftar kontak tim penanganan insiden internal dan eksternal.
4. Organisasi mendesain jaringan yang dapat memastikan apabila *server DMZ* terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
5. Tim respon insiden telah memiliki peralatan sumber daya analisis insiden (misalkan *packet sniffer*, diagram jaringan, alat digital forensik, dll).
6. Ketika organisasi mengalami insiden, tim respon insiden dengan mudah mendapat bantuan dari tim manajemen kritis.
7. Hasil review dan rekap laporan pengangan insiden telah dilaporkan ke *top management*.



8. Laporan insiden di organisasi Anda 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 dan Informatika Provinsi Jawa Tengah sebagai berikut:

Aspek Tata Kelola

1. Organisasi belum memiliki gap analisis kemampuan sehingga organisasi tidak dapat membuat baseline pelatihan keamanan informasi.
2. Organisasi belum memiliki pelatihan *secure code* untuk personel yang terlibat dalam pengembangangan aplikasi.
3. Organisasi belum memiliki kebijakan terkait perlindungan data pribadi.
4. Organisasi tidak mereview izin akses dari akun pengguna.
5. Organisasi belum memiliki *red team* dan *blue team*.
6. Organisasi belum memiliki pemisahan *environment* antara sistem *production* dan *development*.
7. Organisasi belum menggunakan DLP (*Data Loss Prevention*) atau NAC (*Network Access Control*).
8. Organisasi belum menerapkan metode *sandbox* terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap *malicious behaviour*.
9. Organisasi Anda belum memiliki kebijakan yang menetapkan sanksi yang dijatuhan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
10. Organisasi belum memiliki kebijakan terkait SSO dan tenggat waktu kadaluarsa sebuah akun.



Aspek Identifikasi

1. Organisasi belum memiliki *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
2. Aset yang diidentifikasi belum dilakukan klasifikasi kritisitas dan belum ditetapkan penanggungjawabnya.
3. Belum dilakukan identifikasi maupun pembatasan akses perangkat yang tidak diizinkan.
4. Analisis keterkaitan antara keamanan dan kenyamanan dari pengguna aset perangkat dan aplikasi belum dilakukan dalam rangka penyusunan standar keamanan informasi.
5. Belum ada kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
6. Karyawan diizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi.
7. Pihak ketiga diizinkan untuk menggunakan aset mereka pada jaringan organisasi.
8. Tidak ada dokumentasi mengenai alur informasi yang memproses data *stakeholder* termasuk yang dikelola oleh pihak ketiga.
9. Pemrosesan data *stakeholder* (dicatat, dimonitoring, dilaporkan) tidak dilakukan review.
10. Organisasi belum menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan.
11. *Risk Register* belum didokumentasikan untuk semua aplikasi.
12. Organisasi tidak memperbarui roadmap keamanan TI organisasi dalam jangka waktu tertentu.
13. Organisasi belum memiliki *Business Impact Analysis* terhadap perangkat dan aplikasi TI.
14. Organisasi belum memiliki metode/standar klasifikasi aset TI dan *cyber threats* yang ditemukan.



15. Organisasi belum memprioritaskan Langkah proteksi keamanan siber dalam perlindungan data dan aset kritis.

Aspek Proteksi

1. Perangkat jaringan belum menggunakan otentifikasi terpusat.
2. *Inbound network traffic* belum di filter untuk memeriksa *malware* dan mencegah eksplotasi terhadap kerentanan.
3. Organisasi belum menerapkan *port access control* sebagai pengendalian terhadap otentifikasi perangkat yang terhubung ke jaringan.
4. Belum diterapkan *firewall filtering* antar segmen jaringan local.
5. Organisasi belum melakukan *disable peer-to-peer* pada *wireless client* di perangkat *endpoint*.
6. Belum ada pembatasan aplikasi yang diunduh, diinstal, dan dioperasikan.
7. Belum dilakukan pembatasan penggunaan *scripting tools*.
8. *Master image* belum dilakukan penyimpanan.
9. Belum ada batasan fitur *auto-run content* dan pengaturan akses *read/write* pada perangkat USB.
10. Semua perangkat *endpoints* termasuk *server* belum menggunakan antivirus.
11. Informasi identitas dan akses pengguna tidak digunakan untuk membatasi hak akses dari dalam jaringan.
12. Belum memanfaatkan metode otentifikasi pada saluran yang terenkripsi dan juga penambahan OTP.
13. Belum ada penerapan SSO, pembatasan IP dan MMA pada akses *cloud*.
14. Belum ada *Data Center Redudancy* terkait *cloud* yang ada di organisasi.



Aspek Deteksi

1. Organisasi belum memiliki *Change Advisory Board* (CAB).
2. Organisasi tidak memiliki mekanisme monitoring terhadap akses dan perubahan pada data sensitif (seperti *File Integrity Monitoring* atau *Event Monitoring*).
3. Organisasi tidak memiliki mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
4. Organisasi belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif.
5. Organisasi tidak menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi, dan analisis log
6. Organisasi tidak dapat mendeteksi *Wireless Access Point* yang terhubung ke jaringan LAN.
7. Organisasi belum menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
8. Organisasi tidak memantau aktifitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.
9. Organisasi belum memiliki *ticketing system* untuk melacak progress suatu kejadian.
10. Organisasi tidak menerapkan *event notification* yang berbeda-beda untuk setiap jenis eskalasi.
11. Organisasi belum memperoleh informasi dari *multiple threat intelligence feeds* untuk mendeteksi serangan siber.
12. Organisasi belum menjalankan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber.
13. Organisasi belum memiliki sistem untuk melakukan *Malicious Code Detection* untuk mendeteksi, menghapus, dan melindungi dari *Malicious Code*.
14. Organisasi belum memiliki *Metrik Security Event*.



Aspek Respon

1. Organisasi belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau *business continuity planning* (BCP).
2. Organisasi belum memiliki skema penilaian insiden dan prioritas berdasarkan potensial dampak.
3. Organisasi belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan.
4. Organisasi 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.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
 - a. Melakukan gap analisis untuk memahami *skill* dan *behaviour* yang tidak dimiliki karyawan dan menggunakan informasi tersebut untuk membuat *roadmap* terkait *baseline* Pendidikan dan pelatihan terkait keamanan informasi.
 - b. Meningkatkan kemampuan staf tentang kewajiban menjaga data privasi, termasuk hukuman terkait pengungkapan data yang salah.
 - c. Membuat kebijakan penerapan perlindungan data pribadi dan keamanan informasi.
 - d. Melakukan reviu izin akses dari akun pengguna setidaknya setiap 3 bulan sekali.
 - e. Menerapkan dan mendokumentasikan standar knfigurasi (*port*, *protocol*, *service*) untuk semua sistem.



- f. Membentuk *red team* dan *blue team* serta melakukan pengujian secara berkala dalam mengukur kesiapsiagaan dalam menangani insiden keamanan.
 - g. Melakukan pemisahan *environment* antara sistem *production* dan *development* serta melakukan *hardening* dan pengujian aplikasi yang menjadi kelolaan.
 - h. Melakukan penerapan antivirus dan antimalware secara terpusat dan selalu melakukan *update*.
 - i. Menggunakan Data Loss Prevention (DLP) atau Network Access Control (NAC).
 - j. Membuat *risk register*, *risk analysis*, metode *sandbox*, dan kontrol kriptografi.
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. Membuat klasifikasi kritikalitas aset serta menetapkan penanggungjawabnya.
 - c. Melakukan identifikasi dan pembatasan akses perangkat yang tidak diizinkan dan/atau yang tidak diperlukan oleh organisasi.
 - d. Membuat *Business Impact Analysis* (BIA) terhadap perangkat dan aplikasi TI.
 - e. Melakukan segmentasi jaringan berdasarkan fungsionalitas.
3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
- a. Melakukan *filtering Inbound network traffic* untuk memeriksa malware dan mencegah eksloitasi kerentanan.
 - b. Menerapkan *port access control* sebagai pengendali otentikasi perangkat yang terhubung ke jaringan.
 - c. Menerapkan *firewall filtering* antar segmen jaringan local.
 - d. Memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
 - e. Menerapkan SSO, pembatasan IP dan MMA pada akses *cloud*.



4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
 - a. Membentuk *Change Advisory Board* (CAB).
 - b. Membuat mekanisme monitoring terhadap akses dan perubahan pada data sensitive (*File Integrity Monitoring* atau *Event Monitoring*).
 - c. Membuat mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
 - d. Menerapkan SIEM atau *Log Analysis Tools* untuk keperluan dokumentasi korelasi dan analisis log.
 - e. Melakukan pendekripsi *Wireless Access Point* yang terhubung ke jaringan LAN.
 - f. Menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
 - g. Membuat *ticketing system* untuk melacak progress dari *event post-notification*.
 - h. Melakukan *vulnerability scanning* secara otomatis untuk mendekripsi kerentanan.
 - i. membuat *Metrik Security Event*.
5. Aspek Respon ditingkatkan dengan cara:
 - a. Membuat kebijakan penanganan insiden yang selaras dengan kebijakan *Business Continuity Planning* (BCP).
 - b. Membuat skema penilaian insiden dan prioritas berdasarkan potensial dampak (aspek kerugian operasional, bisnis, reputasi, dan hukum).
 - c. Melakukan reviu Laporan Insiden secara berkala.
 - d. Membuat SLA penanganan insiden siber.



PENUTUP

Demikian disampaikan laporan kegiatan penilaian maturitas keamanan siber pada Dinas Komunikasi dan Informatika Pemerintah Provinsi Jawa Tengah, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Semarang, 2 Desember 2020

Kepala Bidang Persandian dan Keamanan
Informasi

Eny Soelastri, S.H

Kepala Subdirektorat Penanggulangan dan
Pemulihan Pemerintah Daerah Wilayah I

Sriyanto, S.Sos., M.M