2021

LAPORAN

HASIL PENILAIAN TINDAK LANJUT REKOMENDASI *CYBER SECURITY MATURITY* (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TENGAH

PENDAHULUAN

I. Umum

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

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

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

II. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tindak lanjut hasil rekomendasi tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Jawa Tengah pada tahun 2020. Dengan adanya perbaikan pada tingkat maturitas ini diharapkan dapat memberikan gambaran peningkatan kegiatan pengamanan informasi pada lingkup *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.

V. Deskripsi Ruang Lingkup Penilaian

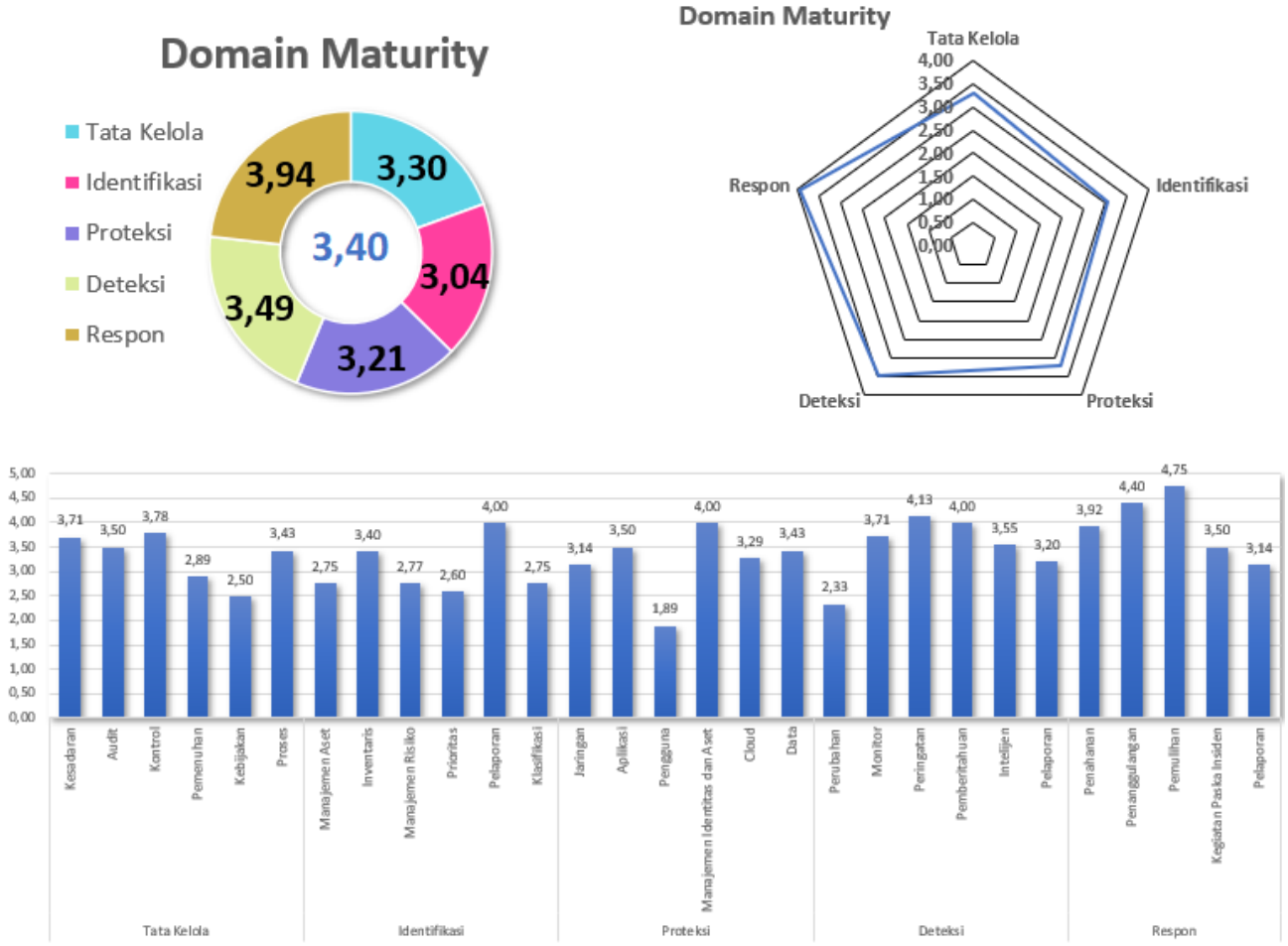
1. Ruang Lingkup Penilaian :

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

KLASIFIKASI: RAHASIA

2. Instansi/Unit Kerja* : Dinas Komunikasi dan Informatika Provinsi Jawa Tengah

VI. Hasil Penilaian CSM

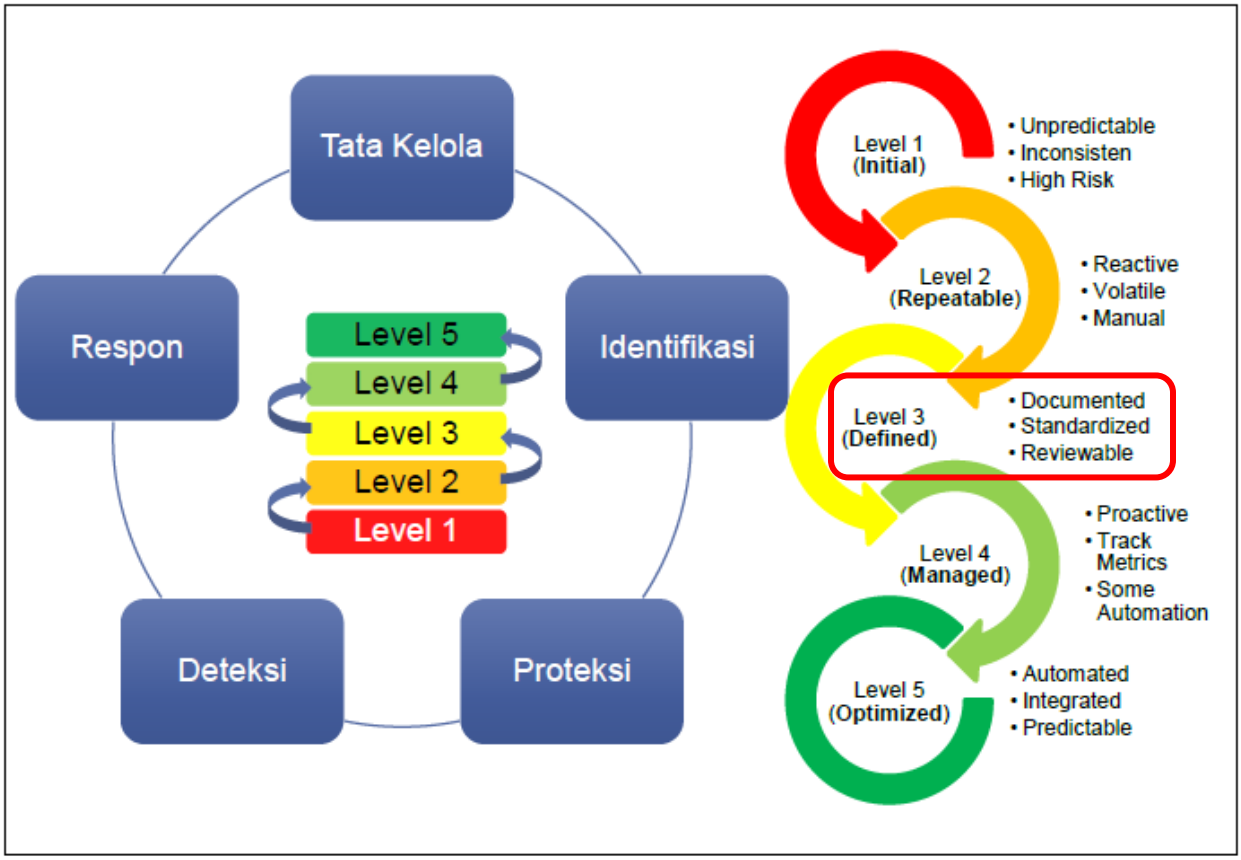


Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 3,40,** sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat 3

KLASIFIKASI: RAHASIA



Gambar 2. Capaian Level Kematangan

Level Kematangan 3:

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

Catatan:

Berdasarkan penilaian CSM tahun 2020 adalah 3,33, dengan merujuk pada hasil evaluasi tindak lanjut rekomendasi kegiatan keamanan siber yang telah dilakukan pada tahun 2021, terdapat kenaikan 0,07 poin menjadi 3,40 dengan kategori level masih berada pada level 3.

Tindak Lanjut Rekomendasi

No	Rekomendasi	Tindak Lanjut
AREA TATA KELOLA		
1	Meningkatkan kemampuan staf tentang kewajiban menjaga data privasi, termasuk hukuman terkait pengungkapan data yang salah	- Terkait kewajiban menjaga data privasi sudah tertuang dalam kebijakan dan operasional prosedur terkait keamanan informasi.
2	Membuat kebijakan penerapan perlindungan data pribadi dan keamanan informasi	- Diskominfo Prov Jateng sudah menyusun kebijakan terkait keamanan informasi dan beberapa operasional prosedur turunannya.
3	Melakukan reviu izin akses dari akun pengguna setidaknya setiap 3 bulan sekali	- Prosedur terkait reviu izin akses akun pengguna sudah ada, namun penerapannya belum optimal dikarenakan kendala SDM yang kesulitan mengingat password yang kompleks dan selalu berganti.
4	Membentuk red team dan blue team serta melakukan pengujian secara berkala dalam mengukur kesiapsiagaan dalam menangani insiden keamanan	- Diskominfo Prov Jateng sudah melakukan pengujian secara berkala dalam mengukur kesiapsiagaan dalam menangani insiden keamanan, kegiatan yang dilakukan berupa cyber security drill test. - Namun red team dan blue team belum dibentuk.
5	Melakukan pemisahan environment antara sistem production dan development serta melakukan hardening dan pengujian aplikasi yang menjadi kelolaan	- Sudah ada pemisahan *environment* antara sistem production dan development namun belum optimal karena kendala anggaran.
6	Membuat risk register, risk analysis, metode sandbox, dan kontrol kriptografi	- Diskominfo Prov Jateng sudah memiliki kebijakan dan operasional prosedur manajemen risiko SMKI
AREA IDENTIFIKASI		
1	Menggunakan *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak	- Belum ada *system configuration management tools*
2	Membuat klasifikasi kritikalitas aset serta menetapkan penanggungjawabnya	- Sudah ada penetapan penanggungjawab aset - Belum dilakukan pengklasifikasian kritikalitas aset. Klasifikasi kritikalitas aset dapat dituangkan dalam daftar inventaris aset
3	Melakukan identifikasi dan pembatasan akses perangkat yang tidak diizinkan dan/atau yang tidak diperlukan oleh organisasi	- Belum menerapkan dan belum ada pembatasan akses perangkat yang tidak diizinkan
4	Membuat Business Impact Analysis (BIA) terhadap perangkat dan aplikasi TI	- Sudah ada kebijakan dan operasional prosedur yang mendefinisikan terkait Business Impact Analysis namun belum dibuat kertas kerja Business Impact Analysis (BIA)
5	Melakukan segmentasi jaringan berdasakan fungsionalitas	- Sudah ada segmentasi jaringan
AREA PROTEKSI		
1	Melakukan *filtering inbound network traffic* untuk memeriksa malware dan mencegah eksploitasi kerentanan	- Sudah menerapkan firewall dan IDS/IPS
2	Menrapkan *port access control* sebagai pengendali otentikasi perangkat yang terhubung ke jaringan	- Sudah ada tindak lanjut yaitu sedang mencoba implementasi *port knocking*
3	Menerapkan *firewall filtering* antar segmen jaringan lokal	- Sudah menerapkan firewall dan segmentasi jaringan

No	Rekomendasi	Tindak Lanjut
4	Memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP	- Sudah menerapkan SSL
5	Menerapkan SSO, pembatasan IP dan MMA pada akses cloud	- Sudah ada SSO namun masih parsial. Penerapan SSO masih ada kendala karena banyaknya aplikasi yang didevelop
AREA DETEKSI		
1	Membuat mekanisme monitoring terhadap akses dan perubahan pada data sensitive (File Integrity Monitoring atau Event Monitoring)	- Masih belum ada mekanisme monitoring terhadap akses dan perubahan pada data sensitive
2	Membuat mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah	- Masih belum ada mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah
3	Menerapkan SIEM atau Log Analysis Tools untuk keperluan dokumentasi korelasi dan analisis log	- Diskominfo Prov Jateng sudah menerapkan SIEM
4	Menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan	- Alokasi kapasitas penyimpanan log sudah dikelola oleh bagian Infrastruktur
5	Membuat ticketing system untuk melacak progress dari event post-notification	- Diskominfo Prov Jateng sudah mengimplementasi OTRs
6	Melakukan vulnerability scanning secara otomatis untuk mendeteksi kerentanan	- Sudah melakukan vulnerability scanning
ASPEK RESPON		
1	Membuat kebijakan penanganan insiden yang selaras dengan kebijakan Business Continuity Planning (BCP)	- Kebijakan penanganan insiden yang selaras dengan kebijakan Business Continuity Planning (BCP) belum ada
2	Melakukan reviu Laporan Insiden secara berkala	- Diskominfo Prov Jateng sudah melakukan reviu terhadap laporan insiden
3	Membuat SLA penanganan insiden siber	- SLA sudah tertuang dalam operasional prosedur mengenai penanganan keamanan informasi

PENUTUP

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

Depok, Januari 2022

Koordinator Kelompok Manajemen Risiko dan Pengukuran Tingkat Kematangan Keamanan Siber dan Sandi Sektor Pemerintah Daerah,

Ditandatangani secara elektronik oleh:
Koor Manris PTK KSS Pemda

Nurchaerani
NIP. 196507081987102003

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elekronik (BSrE), Badan Siber dan Sandi Negara

KLASIFIKASI: RAHASIA