2021

LAPORAN

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

DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

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 tindak lanjut hasil rekomendasi tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Jawa Timur 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. Pelaksanaan Kegiatan

BSSN melakukan validasi tindak lanjut rekomendasi instrumen CSM dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Jawa Timur secara *online* melalui media platform pada:

Hari/Tanggal: Kamis/6 Januari 2022

Waktu : Pukul 14.00 sd.16.30 WIB

link zoom : https://us02web.zoom.us/j/82299769082

Tim BSSN yang terlibat:

1) Nurchaerani, S.E.
2) Nurman Yohan Sopandji, S.ST, M.T.
3) Diah Sulistyowati, S.Kom.
4) Aris Munandar, S.S.T.MP
5) Mochamad Jazuly, S.S.T.TP.

Narasumber Instansi/Lembaga :

1) Aulia Bahar Pernama, S.Kom, M.ISM
2) Raden Makaryo Nugrahadi, S.Kom, M.MT
3) Adi Kurniawan, S.Kom., M.Kom
4) Taufiq Ramadhany, S.T.
5) Ali Firman Herlambang, S.T.

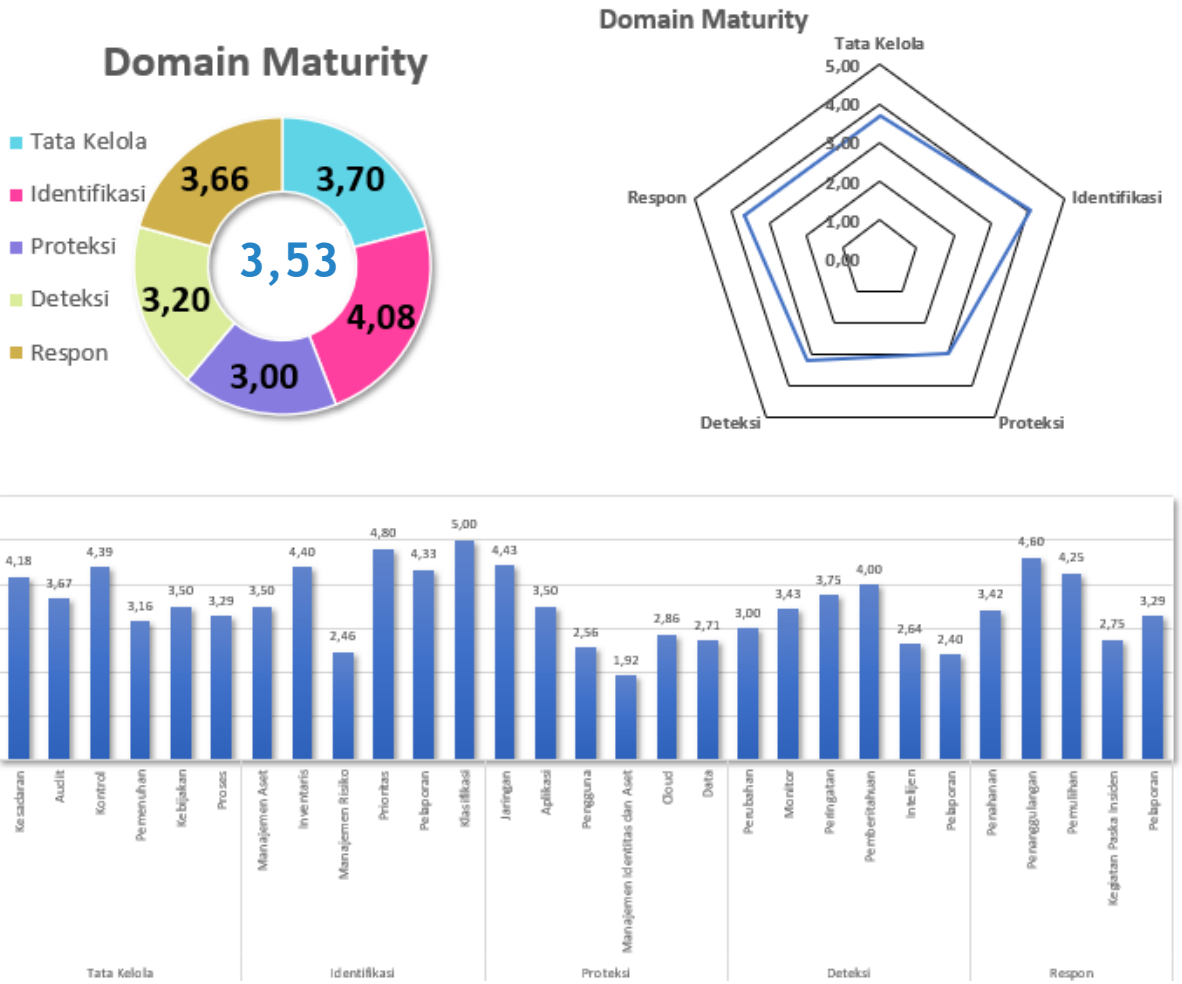
I. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

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

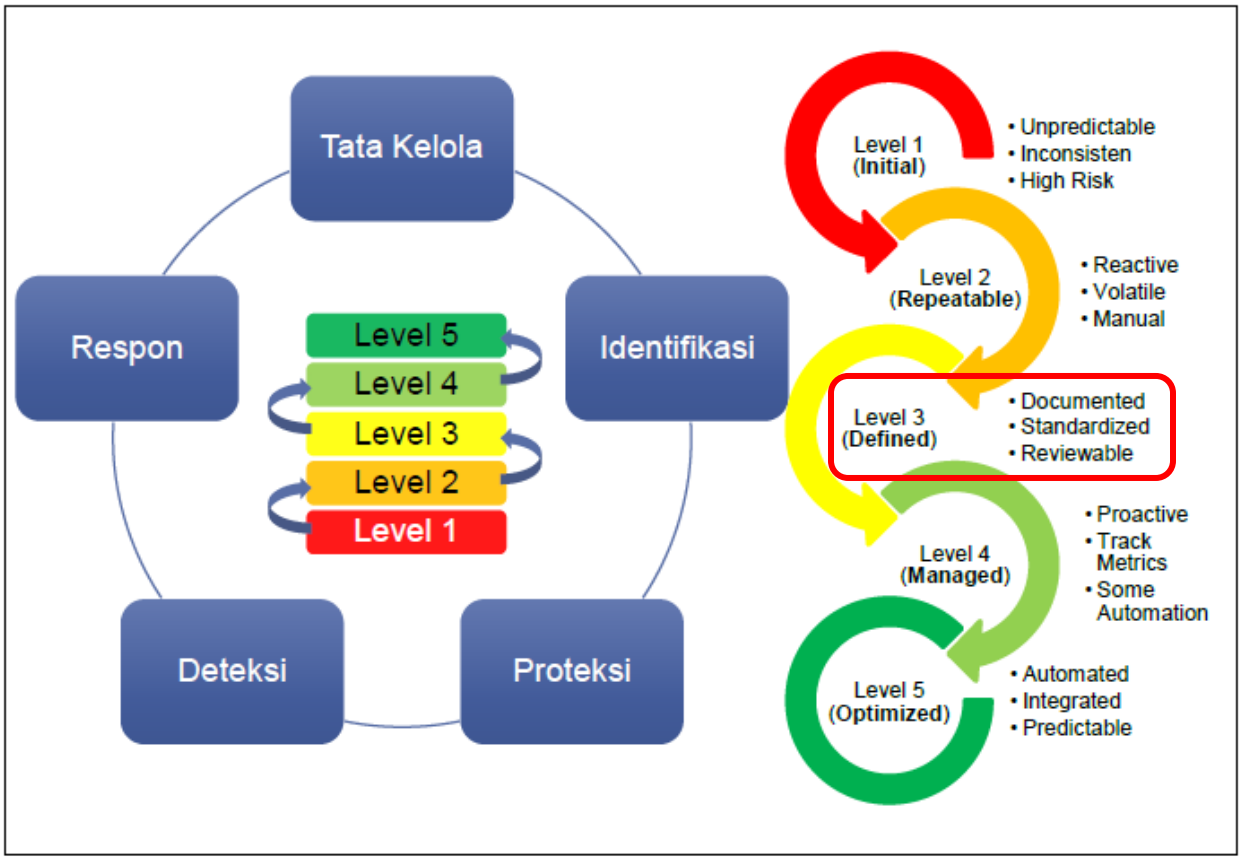
II. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 3,53**, sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat 3



Gambar 2. Capaian Level Kematangan

Level Kematangan 3:

Level kematangan 3 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi dan Informatika Provinsi Jawa Timur 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 3,27, dengan merujuk pada hasil evaluasi tindak lanjut rekomendasi kegiatan keamanan siber yang telah dilakukan pada tahun 2021, terdapat kenaikan 0,26 poin menjadi 3,53 dengan kategori level masih berada pada level III.

III. Tindak Lanjut Rekomendasi

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
	Area Tata Kelola	
1	Menyelenggarakan simulasi *phising* setidaknya setiap tahun.	Belum melakukan simulasi *phising*, eksisting yang sudah dilakukan adalah melakukan analisis *data breach* berdasarkan kegiatan *cyberdrill* yang diselenggarakan oleh BSSN.
2	Menginformasikan kepada stakeholder tentang teknik atau kerentanan siber yang berkembang saat ini yang dapat digunakan dalam peningkatan risiko *fraud*/penipuan.	• Merujuk pada program kerja keamanan siber yang dilakukan pemprov Jatim secara periodik tiap bulan, seperti *sharing* terkait dengan adanya *vulnerability* pada suatu sistem, insiden SIM *swap fraud* dll yang diteruskan kepada tim CSIRT Jatim dan Dinas Kominfo. • *Sharing* informasi tersebut masih dilakukan secara internal, belum dilakukan kepada stakeholder/klien/konsumen baik publik maupun perangkat daerah lainnya.
3	Menyusun kebijakan perlindungan data stakeholder secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi dan aturan yang berkaitan dengan data pribadi antara lain: a. Kebijakan mencakup keharusan penerapan perlindungan data pribadi. b. Menunjuk personil yang ditunjuk secara khusus bertanggungjawab untuk pengembangan dan implementasi kebijakan dan prosedur perlindungan data pribadi. c. Menyampaikan/menginformasikan kebijakan data privasi kepada stakeholder segera setelah terjalin kerjasama karena belum ada kebijakan data privasi. d. Menyusun kebijakan atau prosedur mengenai pemberitahuan jika terjadi pelanggaran terhadap data pribadi dan mendokumentasikan. e. Menyusun kebijakan dan prosedur terkait pemberitahuan dan keputusan stakeholder untuk memilih tidak membagikan data mereka.	• Untuk saat ini yang telah dilakukan adalah peningkatan program *security awareness*, namun untuk perlindungan data pribadi belum dilakukan. • Mengingat kejahatan terhadap penyalahgunaan data pribadi seseorang sering kali ditemukan pada sebuah organisasi, karena tidak mengetahui bagaimana data tersebut dikelola dan diamankan secara tepat, maka penting untuk menyusun kebijakan dan menyampaikan terkait dengan pentingnya PDP. • Pengelolaan data pribadi menjadi sangat penting untuk meminimalisir kejahatan pencurian atau pembobolan data dan informasi serta kejahatan jual beli data dan informasi *online* sehingga perlu dibutuhkan sebuah peraturan yang berkaitan dengan perlindungan data dalam lingkup pemprov Jatim.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
	f. Dalam memberikan data stakeholder kepada pihak ketiga, stakeholder memiliki kewenangan untuk mengetahui mengenai distribusi data milik mereka.	
4	Penggunaan akun khusus dalam melakukan *vulnerability scanning*. Dan setiap akun pengguna atau sistem yang digunakan dalam melakukan *penetrating testing* dikontrol dan dipantau untuk memastikan bahwa akun tersebut hanya digunakan untuk tujuan yang sah, dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan.	• Untuk tahun 2021 masih menggunakan *blackbox testing* dan menjadi relatif lebih rentan karena metode tersebut dapat menjadi sumber kelemahan manakala terdapat beberapa celah di situs dan tidak ditemukan oleh pengetes, sehingga masalah menjadi belum terselesaikan. • Untuk tahun 2022, Pemprov Jatim akan mengalokasikan usulan untuk mengadakan tool Burp Suite, Cpanel.
5	Melaksanakan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan	• Telah menerapkan *surveilence* dengan iso 27001, pelaksanaannya dilakukan bulan Oktober 2021,dimana Pemprov Jatim telah secara periodik melakukan kegiatan ini dari tahun 2018. • Dalam rangka menjaga konsistensi penerapan ISMS terhadap kontrol pada ISO 27001, surveyor secara periodik melakukan pengecekan terhadap kebijakan dan panduan yang telah ada termasuk adalah dengan melihat kesesuaian terhadap hak akses dari akun pengguna yang dilakukan pengecekan setiap bulan
6	Pembentukan *Red Team* dan *Blue Team* serta melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.	• Pemprov Jatim belum membentuk *red team* dan *blue team* dikarenakan keterbatasan personil yang ada. • Disarankan dapat mengoptimalkan pembentukan tim tersebut dengan memberdayakan personil pada bidang lain yang menguasai IT dan keamanan. • Kedua tim ini sangat membantu dalam meningkatkan keamanan siber karena memiliki peranan yang saling melengkapi, di mana *red team* akan fokus pada pengujian penetrasi berbagai sistem dan *blue team*

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
		akan mempertahankan, mengubah dan mengelompokkan kembali mekanisme pertahanan untuk membuat respons insiden jauh lebih kuat
7	Melakukan filterisasi terhadap seluruh jenis file lampiran email.	• Pemprov Jatim telah menggunakan shopos *email security* dimana fitur di dalamnya telah menggunakan mekanisme *filtering email*. • Sebelumnya telah menggunakan Barracuda Email Security Gateway namun untuk lisensi 2 tahun ini tidak aktif, untuk 2022 akan dialokasikan kembali.
8	Menerapkan metode *sandbox* terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap *malicious behaviour*.	• Pemprov Jatim telah menerapkan shopos dimana sesuai default standar di dalamnya telah terdapat fitur *sandbox* • Untuk meningkatkan aktivitas analisis terhadap *malware* dapat menggunakan tool Any.Run yang akan membantu melakukan pemindaian analisis *malware* yang memungkinkan pengguna untuk mengetahui adanya *malware* dan virus secara aman.
9	Menyusun kebijakan terkait penetapan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.	• Belum ada kebijakan terkait dengan penetapan sanksi terhadap karyawan yang tidak patuh • SMKI hanya di lingkup *data center*, untuk lingkup secara luas (Pemprov) belum diberlakukan. • Perlu penambahan kebijakan komitmen pimpinan dalam penerapan SMKI baik pada lingkup DC maupun lingkup lainnya dan perangkat daerah lainnya dalam menjaga terwujudnya penerapan SMKI secara menyeluruh.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
10	Menyusun kebijakan keamanan informasi mengatur mengenai *single* ID yang unik untuk melakukan semua otentikasi	• Pemprov Jatim Belum menerapkan *Single Sign On*/SSO. • Permasalahan yang dihadapi *user* yaitu terdapat banyak yang lupa dengan *user account* dan *password* yang dimilikinya karena harus mengingat semua *username* dan *password* untuk login ke setiap sistem yang berbeda-beda. • Kebijakan dapat berupa regulasi *single* ID atau surat edaran penerapan SSO
11	Menyusun kebijakan yang mengatur semua akun di organisasi memiliki tenggat waktu kadaluwarsa.	Berdasarkan ketentuan pada kontrol ISO 27001, telah tercantum kebijakan pengaturan akun dengan durasi tenggat waktu kadaluwarsa yang telah ditentukan dimana pengecekannya telah dilakukan setiap bulan sekali
12	Menyusun kebijakan terminasi diterapkan dengan masa tenggang yang diizinkan terkait hak akses karyawan ke dalam sistem informasi	Pemprov Jatim telah memiliki kebijakan masa tenggang bagi karyawan yang keluar atau pindah hal ini selaras dengan kontrol yang menjadi klausul pada ISO 27001.
13	Menyusun kebijakan yang mengakomodir laporan karyawan ataupun stakeholder terkait kehilangan perangkat laptop/*smartphone* yang kemungkinan dapat digunakan sebagai kegiatan penipuan/kejahatan	• Pemprov Jatim belum memiliki mekanisme, prosedur laporan kehilangan perangkat, namun telah memiliki rekaman/catatan aset. • Perlu NSPK yang menjadi dasar dalam mengantisipasi adanya kehilangan perangkat, terdapat langkah-langkah yang perlu diambil dalam rangka mengamankan dan melindungi data/informasi serta mengantisipasi terjadinya kegiatan penipuan/kejahatan yang akan berdampak bagi pribadi maupun organisasi.
14	Menyusun kebijakan metode penghapusan data	Pemprov Jatim telah memiliki kebijakan metode penghapusan data.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
15	Dalam pengembangan *software* di organisasi secara internal/mandiri perlu diterapkan beberapa aspek keamanan sebagai berikut: a. Menerapkan praktik *secure coding* yang sesuai dengan bahasa pemrograman dan *development environment* yang digunakan. b. Memastikan bahwa pengecekan kesalahan secara eksplisit dilakukan dan didokumentasikan untuk semua *input*, termasuk ukuran, tipe data, dan rentang atau format yang diterapkan. c. Melakukan analisis statis dan/atau dinamis untuk memverifikasi bahwa praktik secure coding benar-benar diterapkan pada *software* yang dikembangkan secara internal. d. *Source code* yang dibuat secara mandiri dilakukan reviu kerentanannya terlebih dahulu sebelum masuk ke *production*. e. Melakukan pelatihan dalam membuat *secure code* yang baik kepada personil yang terlibat.	• Pemprov Jatim masih melakukan kegiatan *sharing knowledge* melalui *security awareness* tentang pentingnya penerapan secure coding melalui sosialisasi. • Saat ini belum melakukan penerapan *secure coding* dalam setiap pengembangan sistem elektronik yang disusun oleh tiap perangkat daerah. • Pemprov Jatim dapat melakukan penanganan kerentanan web server dengan merujuk pada panduan pedoman tata kelola Keamanan Aplikasi Berbasis Web dimana di dalamnya terdapat cek *list* penanganan kerentanan dan web server yang akan membantu pemda dalam mengetahui/memitigasi adannya ancaman yang terjadi.
Area Identifikasi		
16	Melakukan identifikasi maupun pembatasan akses perangkat yang tidak diizinkan oleh organisasi.	Pemprov Jatim telah melakukan identifikasi aset dan menerapkan VPN ketika akan bersentuhan dengan aset kritikal serta menggunakan SSH.
17	Melakukan analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.	• Belum melakukan. • Melakukan analisa yang dimaksud dalam rangka penyusunan standar keamanan informasi.
18	Menyusun kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.	• Belum menyusun kebijakan pembatasan penggunaan asset organisasi. • Ada baiknya organisasi menyusun kebijakan ini untuk menghindari adanya kepentingan pribadi dengan menggunakan aset organisasi.
19	Tidak mengizinkan karyawan memiliki akses sebagai administrator pada perangkat (laptop, personal *computer*, dll) milik organisasi. Dan tidak mengizinkan pihak ketiga untuk menggunakan aset mereka pada jaringan organisasi.	• Belum menyusun dan mengimplementasikan kebijakan terkait akses administrator pegawai.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
		• Membatasi akses administrator bagi pegawai adalah salah satu Tindakan preventif dalam keamanan siber.
20	Mendokumentasikan alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.	• Telah memiliki sistem *monitoring* jaringan, namun secara umum menggunakan *firewall* (*monitoring traffic*) dan hanya *monitoring* anomali saja. • Menyusun dokumentasi terkait informasi yang diproses dan dikelola oleh tim Pemprov Jatim maupun pihak ketiga.
21	Menyusun kebijakan dan melakukan implementasi mengenai retensi data sensitif termasuk data stakeholder di organisasi dengan kebijakan regulasi dan kebutuhan bisnis.	Telah menyusun kebijakan terkait, dokumen ini termasuk dokumen pendukung dalam proses resertifikasi ISO/IEC 270001.
22	Membuat metadata sensitif termasuk data stakeholder yang disimpan (secara elektronik dan *hardcopy*) dan memuat metadata informasi periode retensi, pemilik data, dan penggunaan data.	• Belum membuat metadata sensitif. • Memulai merancang terkait apa saja yang menjadi metadata sensitif yang akan dikelola sembari menunggu pusat data nasional terbentuk.
23	Menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi.	• Bagian asset telah memiliki kebijakan terkait penghapusan aset. • Secara rutin mengecek asset yang sudah tidak digunakan untuk di nonaktifkan untuk mencegah adanya kerentanan yang terdapat pada aset akibat tidak dilakukan *maintenance*.
24	Data otentikasi tidak diperbolehkan disimpan di perangkat browser *end user*.	• Belum dilakukan. • Dapat membuat edaran kepada pegawai terkait himbauan untuk tidak menyimpan data otentikasi seperti *username* dan *password* di browser.
25	Memperbaharui *roadmap* keamanan TI organisasi dalam jangka waktu tertentu.	Telah memiliki dokumen *roadmap* TI atau rencana induk TIK dan setiap tahun di review.
26	Melakukan klasifikasi terhadap *cyber threats* yang ditemukan pada organisasi.	Telah dilakukan dengan adanya laporan bulanan yang memuat keamanan siber.
Area Proteksi		
27	Organisasi diharapkan mampu menerapkan otentikasi terpusat.	• Secara umum belum dilakukan.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
		• Jika Pemprov Jatim menggunakan produk CISCO, maka dapat dioptimalkan fungsi otentikasi menggunakan AD/AP.
28	Organisasi diharapkan dapat menerapkan pembatasan komunikasi antar *workstation*, pembatasan fitur *wireless*, koneksi *peer-to-peer* pada *wireless client*.	Sudah menerapkan segmentasi dan khusus *data center* hanya orang terotentikasi saja yang dapat mengaksesnya.
29	Organisasi diharapkan dapat menerapkan pembatasan aplikasi yang diunduh, di *install* dan di operasikan.	• Belum dapat melakukan pembatasan aplikasi yang diunduh, sehingga melakukan tindakan preventif dengan menyediakan antivirus sampai dengan level pegawai. • Pembatasan aplikasi yang diunduh dapat dilakukan salah satunya dengan membatasi hak akses administrator pada aset yang digunakan pegawai.
30	Organisasi diharapkan dapat menerapkan pengecekan otomatis terhadap *spam/phising/malware* yang ada di *cloud*.	• Telah menggunakan SHOPOS untuk implementasi *email system*, sehingga memiliki fitur untuk pengecekan otomatis. • Untuk *cloud* sendiri belum memiliki fitur pengecekan otomatis dimaksud.
31	Organisasi diharapkan dapat menerapkan ada pembatasan penggunaan *scripting tools*.	• Belum dapat melakukan pembatasan penggunaan *scripting tools*. • Pembatasan ini dapat dilakukan salah satunya dengan membatasi hak akses administrator pada aset yang digunakan pegawai.
32	*Master image* sebaiknya disimpan.	• *Master image* belum disimpan. • Sebaiknya master *image* disimpan di tempat yang aman untuk digunakan *restore* apabila terjadi kegagalan sistem yang tidak diinginkan.
33	Organisasi perlu menerapkan pembatasan penggunaan *add-on* dan *plugin* aplikasi.	• Belum dapat melakukan pembatasan penggunaan *add-on* dan *plugin*. • Pembatasan ini dapat dilakukan salah satunya dengan membatasi hak akses administrator pada aset yang digunakan pegawai.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
34	Organisasi diharapkan dapat menerapkan otomatisasi permohonan kata sandi pada perangkat yang tidak aktif.	• Beberapa aplikasi sudah menerapkan skema ini. • Memastikan seluruh aplikasi telah menerapkan skema ini.
35	Perlu adanya pembatasan fitur *auto-run content* dan pengaturan akses *read/write* pada perangkat USB.	• Belum dapat melakukan pembatasan fitur *auto-run content* dan pengaturan akses *read/write* pada perangkat USB. • Pembatasan ini dapat dilakukan salah satunya dengan membatasi hak akses administrator pada aset yang digunakan pegawai.
36	Enkripsi sebaiknya dilakukan pada perangkat eksternal organisasi.	• Belum melakukan enkripsi pada perangkat eksternal. • Pengamanan dapat dilakukan dengan memanfaatkan aplikasi dari BSSN maupun bawaan dari produk penyimpanan eksternal.
37	Perlu adanya pembatasan akun pada laptop organisasi.	• Belum dapat melakukan pembatasan akun pada laptop. • Pembatasan ini dapat dilakukan salah satunya dengan membatasi hak akses administrator pada aset yang digunakan pegawai.
38	Perlu adanya pemanfaatan *identity and access management system, Multi-Factor Authentication*.	• Belum menerapkan MFA. • Implementasi MFA ini penting untuk menghindari serangan masif seperti *bruteforce attack*.
39	Organisasi sebaiknya memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.	Penerapan otentikasi pada saluran terenkripsi dapat mengimplementasikan SSL atau VPN dan penambahan OTP sebagai pencegahan akses yang tidak sah.
40	Organisasi diharapkan dapat mengoptimalkan penggunaan IP *reputation*.	• Belum menggunakan IP *reputation*. • IP *reputation* ini dapat mencegah adanya akses pada beberapa IP yang diduga mencurigakan dan berbahaya.
41	Organisasi diharapkan dapat meningkatkan kemampuan untuk melacak dan mendeteksi perilaku anomali dari karyawan ataupun stakeholder.	• Belum melakukan kegiatan terkait. • Kegiatan ini dapat dilakukan salah satunya dengan terlebih dahulu menyusun

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
		kebijakannya dan menerapkan SIEM yang di-*embed* pada aset.
42	Organisasi diharapkan dapat melakukan identifikasi perangkat yang terhubung.	• Belum melakukan identifikasi pada perangkat yang terhubung. • Identifikasi ini penting untuk mengetahui aset mana yang terdaftar dan yang tidak, serta dapat menjadi *backtrace* ketika terjadi insiden keamanan siber.
43	Akses akun *database* dilakukan oleh akun khusus selain admin.	*Database* hanya diakses oleh administrator saja.
44	Organisasi diharapkan dapat menerapkan SSO, pembatasan IP dan MMA pada akses *cloud*.	• Belum menerapkan SSO. • SSO diimplementasikan untuk mencegah adanya akses yang tidak sah dan mencatat setiap log yang berjalan pada sistem.
45	Organisasi sebaiknya memiliki *Data Center Redudancy* terkait *cloud* yang ada di organisasi.	• Belum memiliki DCR terkait *cloud*. • Ketika telah menerapkan *cloud*, perlu dipertimbangkan untuk memiliki DCR guna sebagai cadangan ketika adanya kegagalan sistem *cloud*.
46	Organisasi perlu melakukan pengujian *data integrity* pada data yang di-*backup*.	• Belum melakukan pengujian data yang di *backup*. • Pengujian ini penting dilakukan dan dicatat untuk memastikan bahwa data yang akan di-*restrore* tidak termodifikasi yang sebelumnya telah disisipkan *malware* untuk *backdoring*.
47	Data yang disimpan dan dikirim sebaiknya dilakukan enkripsi.	Sebagian besar data yang dikirim telah dilakukan enkripsi pada jalur yang aman, namun untuk penyimpanan masih belum dilakukan.
Area Deteksi		
48	Melakukan deteksi perubahan konfigurasi pada peralatan jaringan sehingga dapat terdeteksi secara otomatis.	• Belum dilakukan. • Perubahan konfigurasi ini biasanya menjadi fitur perangkat, sehingga dapat dieksplorasi kembali.
49	Organisasi diharapkan memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data sensitif (seperti *File Integrity Monitoring* atau *Event Monitoring*).	• Belum dilakukan. Tahun 2022 akan mengimplementasikan SIEM – OSSIM.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
		• Memaksimalkan fitur pada OSSIM untuk *File Integrity Monitoring* dan Event *Monitoring*.
50	Organisasi diharapkan memiliki mekanisme *monitoring* dan deteksi terhadap penggunaan enkripsi yang tidak sah.	• Belum dilakukan. • Deteksi penggunaan enkripsi yang tidak sah dapat dilakukan salah satunya menggunakan bantuan SIEM, misalnya pada penggunaan SSH yang tidak sah.
51	Organisasi perlu menerapkan SIEM atau *Log Analytic Tools* untuk keperluan dokumentasi, korelasi, dan analisis *log*.	Belum dilakukan. Tahun 2022 akan mengimplementasikan SIEM – OSSIM.
52	Organisasi diharapkan mampu menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.	Telah memiliki perangkat *log system* terpusat.
53	Organisasi diharapkan dapat memantau aktivitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.	• Belum melakukan pemantauan aktivitas pihak ketiga. • Pemantauan ini dapat dilakukan baik secara fisik maupun non-fisik, secara fisik misalkan ketika kegiatan pemeliharaan ditemani oleh personil diskominfo, non-fisik misalkan memaksa pihak ketiga untuk menanam *agent* agar dapat di-*monitoring* pada SIEM.
54	Log hasil deteksi *malware* diharapkan dapat terhubung dengan perangkat *antimalware administrations* dan *event log servers* sehingga dapat digunakan untuk analisis.	• Belum menerapkan skema terkait. • Memaksimalkan fitur pada OSSIM untuk deteksi *malware*.
55	*Escalation profile* seharusnya dibuat untuk setiap *security event* yang ditemukan, dan dapat disimpan sebagai panduan untuk digunakan di masa mendatang.	*Escalation profile* telah dimuat dalam laporan bulanan yang disampaikan kepada pimpinan.
56	Organisasi sebaiknya menerapkan *event notification* yang berbeda-beda untuk setiap jenis eskalasi.	• Belum menerapkan *event notification*. • Event *notification* berguna sebagai tanda bahwa *ekskalasi* pernah terjadi dan dapat ditangani sebagaimana yang dilakukan ekskailasi sebelumnya.
57	Organisasi diharapkan dapat memperoleh informasi dari *multiple threat intelligence feeds* untuk mendeteksi serangan siber.	• *Feed* masih didapatkan dari BSSN. • Jika menggunakan OSSIM, maka akan mendapatkan fitur *threat intelligence*, sehingga dapat dimaksimalkan sebagai kewaspadaan dan *threat hunting*.

No	Rekomendasi	Tindak Lanjut Tahun 2021 dan Saran perbaikan
58	Organisasi diharapkan dapat menjalankan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber.	• Pernah menggunakan accunetix, namun telah habis lisensinya. • Dengan menggunakan SIEM-OSSIM dapat dimaksimalkan fiturnya untuk *vulnerability assessment*.
59	Organisasi sebaiknya memiliki unit yang melakukan *Cyber Threat Intelligence* (CTI).	• Belum memiliki unit khsus untuk melakukan CTI. • CTI ini penting dilakukan untuk menghindari adanya false positve pada *vulnerabililty scanning* dan menghindari *zero day attack*.
Area Respon		
60	Organisasi diharapkan menerapkan penilaian insiden dalam rangka triase insiden.	Telah melakukan triase insiden, salah satunya dengan menggunakan aplikasi *ticketing*.
61	Diskoneksi segmen jaringan diharapkan dapat ditingkatkan.	Telah mengimplementasikan 2 buah *firewall*.
62	Organisasi diharapkan dapat menjamin penyerang tidak dapat mengakses server *backup* apabila DMZ terkena serangan siber.	• Belum pernah memastikan. • Dapat dilakukan ITSA khusus pada jaringan, sehingga dapat diketahui apakah ada kerentanan yang menyebabkan *attacker* dapat mengakses server *backup*.
63	Rekap insiden siber diharapkan dapat disampaikan ke *Top Management* dan distribusikan pada pemangku kepentingan.	Rekap insiden siber telah dilaporkan setiap bulannya kepada pimpinan.
64	Organisasi diharapkan memiliki SLA penanganan insiden.	• Belum memiliki SLA penanganan insiden. • Diharapkan dapat menyusun SLA guna menjadi *trigger* tim insiden dalam melakukan penanganan insiden dan menjadi nilai tambah kepercayaan stakeholder.
65	Organisasi dapat menyimpan dan melaporkan rekaman insiden dan pelanggaran di organisasi.	Telah dilakukan pelaporan setiap bulannya.
66	Organisasi diharapkan memiliki perhitungan ROI dalam penganggaran di organisasi.	• Belum memiliki perhitungan ROI. • ROI dalam pemerintahan dapat diasumsikan bukan dalam nilai investasi untuk keuntungan, namun lebih kepada investasi untuk kepercayaan publik yang diberikan.

s

PENUTUP

Demikian disampaikan laporan Penilaian Tindak Lanjut Rekomendasi CSM pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Depok, Januari 2022

Kepala Seksi Persandian dan Keamanan Informasi	Koordinator Kelompok Manajemen Risiko dan Pengukuran Tingkat Kematangan Keamanan Siber dan Sandi Sektor Pemerintah Daerah
Dokumen ini telah ditandatangani secara elektronik oleh: KEPALA SEKSI PERSANDIAN DAN KEAMANAN INFORMASI AULIA BAHAR PERNAMA, S.Kom., M.ISM. NIP. 19851024 200912 1 012	Ditandatangani secara elektronik oleh: Koor Manris PTK KSS Pemda Nurchaerani NIP. 196507081987102003
(Aulia Bahar Pernama, S.Kom, M.ISM)	(Nurchaerani, S.E)