2025

LAPORAN

HASIL PENILAIAN
TINGKAT MATURITAS PENANGANAN INSIDEN (TMPI)
DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH KABUPATEN BANGKA

PENDAHULUAN

I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas *stakeholder* dalam penanganan insiden keamanan siber di Dinas Komunikasi, Informatika dan Statistik Pemerintah Daerah Kabupaten Bangka. Dengan adanya tingkat maturitas ini diharapkan dapat memberikan gambaran mengenai apa yang harus menjadi tindak lanjut baik oleh *stakeholder* (Pemerintah Kabupaten Bangka) maupun Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan kemampuan tingkat maturitas keamanan siber.

II. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek penanganan insiden meliputi :

1. Fase 1 : Persiapan
2. Fase 2 : Respon
3. Fase 3 : Tindak Lanjut

III. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen pemetaan TMPI, wawancara/diskusi, dan melihat ketersediaan dokumen penanganan insiden siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas tiap fase penanganan insiden.

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 (*Foundation*) : Rentang Level Kematangan 0 % s.d. 20 %
- Level 2 (*Emerging*) : Rentang Level Kematangan 21 % s.d. 40 %
- Level 3 (*Establishing*) : Rentang Level Kematangan 41 % s.d. 60 %
- Level 4 (*Dynamic*) : Rentang Level Kematangan 61 % s.d. 80 %
- Level 5 (*Optimise*) : Rentang Level Kematangan 81 % s.d. 100 %

IV. Pelaksanaan Kegiatan

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

   Pengisian Instrumen oleh internal *stakeholder* dilakukan pada tanggal 24 April 2025.

2. Validasi Pemetaan TMPI

   Validasi Pemetaan TMPI dilaksanakan untuk pengecekan hasil *self assessment* isian instrumen. Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen pendukung penanganan insiden siber. Kegiatan validasi dilaksanakan pada 14 Mei 2025.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi	: Dinas Komunikasi, Informatika dan Statistik (Dinkominfotik) Pemerintah Kabupaten Bangka	
Alamat	: Jl. Jenderal Ahmad Yani, Kecamatan Sungailiat, Kepulauan Bangka Belitung	
Email	: dinkominfotik@bangka.go.id	
Narasumber Instansi	: 1. Deva Rossiera Maretta, ST	Manggala Informatika Ahli Muda, Dinkominfotik Kabupaten Bangka
	2. Supidah, S.Sos.i	Sandiman Ahli Muda, Dinkominfotik Kabupaten Bangka
	3. Devy Ulya Rachman	Manggala Informatika Ahli Muda, Dinkominfotik Kabupaten Bangka
	4. Ikhsan Syahrizal, S.Kom	Manggala Informatika Ahli Pertama, Dinkominfotik Kabupaten Bangka
	5. Reskydianto Gustama Putra, S.Kom	Manggala Informatika Ahli Pertama, Dinkominfotik Kabupaten Bangka
	6. Faizal, A.Md	Sandiman Terampil, Dinkominfotik Kabupaten Bangka

	7. Anggi Yoan Liblwo, A.Md.T	Sandiman Terampil, Dinkominfotik Kabupaten Bangka
Asesor BSSN	: 1. Carissa Mega Yulianingrum, S.Tr.TP	Manggala Informatika Ahli Pertama pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III
	2. Yulyanti Hendriani, S.Tr.Kom	Sandiman Ahli Pertama Direktorat Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III
	3. Ryu Arifial, S.Kom	Penata Kelola Sistem dan Teknologi Informasi pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III

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 Kabupaten Bangka
3. Lokasi Aset : Dinas Komunikasi, Informatika dan Statistik Kabupaten Bangka
4. DATA CENTER (DC) :

(Data Center memiliki gedung khusus serta ruangan khusus dengan penjagaan fisik ruangan)

- [√] ADA, dalam ruangan khusus
- [ ] ADA, jadi satu dengan ruang kerja
- [ ] TIDAK ADA

5. DISASTER RECOVERY PLAN (DRC) :

(Jika ada, jelaskan kondisi DRC : colocation di pihak ketiga atau di Instansi lain termasuk pengelolaan keamanan DRC)

- [ ] ADA
- [√] TIDAK ADA

6. Status Ketersediaan Dokumen Penanganan Insiden Siber

Dokumen yang diperiksa:

1. Peraturan Daerah Kabupaten Bangka Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Pemerintah Kabupaten Bangka;
2. Peraturan Bupati Bangka Nomor 42 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintah Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Bangka;
3. Peraturan Bupati Bangka Nomor 100 Tahun 2021 tentang Perubahan Atas Peraturan Bupati Bangka Nomor 1 Tahun 2021 Tentang Kedudukan, Susunan Organisasi, Tugas Dan Fungsi Serta Tata Kerja Dinas Komunikasi, Informatika Dan Statistik Tipe A Kabupaten Bangka;
4. Peraturan Daerah (Perda) Kabupaten Bangka Nomor 7 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi Dan Komunikasi ; dan
5. Draf Keputusan Bupati Bangka tentang Pembentukan Tim Tanggap Insiden Siber Computer Security Incident Respon Team Kabupaten Bangka.

Bukti-bukti (rekaman/arsip) penerapan :

1. Bukti Topologi Jaringan.

III. Hasil Penilaian TMPI

Rekapitulasi Hasil Penilaian

Fase	Langkah		TK 1	TK 2	TK 3	TK 4	TK 5	Rata2	Rata2 per Fase
1	1	Penilaian kritikalitas	1,00	-	0,50	-	1,00	0,50	0,47
1	2	Analisis ancaman	-	-	-	-	-	-	
1	3	Orang, proses, teknologi, dan informasi	1,50	1,44	0,58	0,10	-	0,73	
1	4	Lingkungan kontrol	-	3,00	-	-	-	0,60	
1	5	Penilaian kematangan	-	-	1,50	1,00	-	0,50	
2	1	Identifikasi	1,00	-	-	1,00	-	0,50	0,44
2	2	Penyelidikan	-	0,75	-	0,20	0,33	0,26	
2	3	Aksi	0,33	1,00	-	1,60	-	0,59	
2	4	Pemulihan	1,00	0,40	0,17	-	0,50	0,41	
3	1	Identifikasi	-	-	-	-	-	-	-
3	2	Pelaporan	-	-	-	-	-	-	
3	3	Review pasca insiden	-	-	-	-	-	-	
3	4	Pembelajaran yg didapat	-	-	-	-	-	-	
3	5	Pempebarui informasi	-	-	-	-	-	-	
3	6	Analisis trend	-	-	-	-	-	-	
								Rata-rata	0,30

Perhitungan Indeks Kematangan

Fase	Kontribusi Indeks					Jumlah
	TK 1	TK 2	TK 3	TK 4	TK 5	
Bobot per Tingkat	30%	25%	20%	15%	10%	100%
Fase Persiapan	0,15	0,22	0,10	0,03	0,02	0,53
Fase Aksi	0,18	0,13	0,01	0,11	0,03	0,45
Fase Tindak Lanjut	-	-	-	-	-	-
					Indeks Kematangan	0,33

Berdasarkan hasil penilaian TMPI, diperoleh hasil sebagai berikut:

Total Score Indeks Kematangan : 0,33

Sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat 1

IV. Kekuatan/Kematangan TMPI

1. Fase Persiapan
   a. Organisasi memiliki minimal 1 personil yang ditugaskan untuk melakukan aktivitas respon terhadap insiden siber yang terjadi;
   b. Organisasi telah memiliki tim respon insiden yang ditunjuk;

c. Organisasi telah memiliki titik kontak pelaporan insiden siber secara resmi yang diumumkan secara formal dalam Organisasi;
d. Organisasi telah mengimplementasikan peralatan kontrol teknis terkait keamanan jaringan seperti Firewall, IDS/IPS, dll;
e. Prosedur yang dimiliki Organisasi sudah memiliki informasi yang cukup detail terkait infrastruktur IT dan topologi jaringan, sehingga memudahkan dalam melakukan tanggap insiden;
f. Organisasi secara sporadis memiliki daftar aset yg penting bagi Organisasi beserta penanggung-jawab-nya masing-masing;
g. Organisasi secara sporadis memiliki informasi aset dasar (baseline information asset) yang dapat membantu tim tanggap insiden (termasuk tim tanggap insiden dari pihak ketiga) untuk melakukan tanggap insiden;
h. Jika Organisasi mengalami insiden siber, secara umum akan mendapat bantuan dari spesialis keamanan teknis dengan cepat;
i. Organisasi telah secara umum menggunakan perangkat teknis untuk pemantau keamanan pada aset penting;
j. Umumnya tim respon insiden terbentuk secara dedicated, baik bersumber dari internal maupun eksternal; dan
k. Secara umum management senior berkomitmen di Organisasi dalam hal penyediaan alokasi sumber daya secara berkelanjutan.

2. Fase Respon
a. Organisasi tahu sebagian terjadinya insiden dari laporan karyawan;
b. Analisis penyidikan sebagian meliputi identifikasi sistem, jaringan dan informasi yang terkena gangguan;
c. Ruang lingkup pertahanan siber di Organisasi secara umum mencakup sebagian perangkat vital di internal jaringan;
d. Ruang lingkup pertahanan siber di Organisasi secara umum mencakup sebagian perangkat di internal jaringan di Organisasi; dan

e. Implementasi teknis pertahanan di Organisasi secara umum telah meliputi: segmentasi jaringan internal dan sistem back-up untuk data.

3. Fase Tindak Lanjut

-

V. Kelemahan/Kekurangan TMPI

1. Fase Persiapan
   a. Organisasi hanya mendata sebagian kecil aset yang penting bagi Organisasi;
   b. Aset yang didata belum disusun berdasarkan klasifikasi kritikalitas berbasis analisis resiko operasional;
   c. Klasifikasi kekritisan belum disusun secara sistematis dan terstruktur;
   d. Aset yang didata belum disusun berdasarkan klasifikasi kritikalitas berbasis analisis bisnis dan aspek strategis Organisasi;
   e. Organisasi belum menetapkan penanggung jawab setiap aset kritikal secara sistematis, masih dilakukan secara sporadis;
   f. Organisasi belum melakukan penilaian dampak kerugian operasional, bisnis, dan aspek hukum secara mendalam untuk setiap potensi insiden yang telah diidentifikasikan;
   g. Dokumen penilaian kerugian pada organisasi belum di-review dan diperbarui secara periodik;
   h. Organisasi belum melakukan analisis ancaman keamanan siber, termasuk potensi kerentanan dan mendokumentasikannya;
   i. Organisasi belum melakukan analisis ancaman siber secara priodik dan belum menggunakan sistematis yang jelas;
   j. Organisasi belum menyusun berbagai skenario penanganan kasus insiden keamanan siber berdasarkan evaluasi potensi resiko;
   k. Skenario penanganan insiden siber yang ada belum disusun, disimulasikan secara berkala;

l. Simulasi skenario yang dilakukan belum mencakup semua jenis platform teknologi yang ada, termasuk melibatkan mitra dan pihak eksternal (regulator, tim CSIRT lain);
m. Organisasi belum dilakukan pelatihan terhadap SDM internal yang terlibat pada penanganan insiden sesuai skenario yang disusun dan potensi kerentanan yang dihadapi;
n. Sumber informasi ancaman yang menjadi dasar analisis belum berasal dari berbagai sumber eksternal (vendor, konsultan) dan kerjasama antar Organisasi;
o. Belum terdapat evaluasi analisis ancaman beserta skenario yang mengadaptasi perubahan ancaman baru sesuai dengan dinamika ancaman siber yang diinformasikan;
p. Belum melakukan simulasi terhadap skenario ancaman;
q. Tim respon insiden siber di organisasi belum memiliki kemampuan menerima laporan secara sistematis, faham mekanisme eskalasi, belum mampu melakukan klasifikasi insiden, dan memiliki kompetensi berkomunikasi;
r. Tim respon insiden siber di Organisasi hanya memiliki sebagian rincian kontak dari seluruh pihak yang berkepentingan;
s. Organisasi belum program kesadaran ancaman dan penangangan insiden, serta ajakan peran aktif pada seluruh karyawan;
t. Organisasi belum memiliki program sosialisasi proses pelaporan inisiden siber;
u. Tim respon insiden siber di Organisasi belum memiliki kemampuan mendeteksi terjadinya insiden, melakukan analisis dan rekomendasi resolusi;
v. Tim respon insiden siber di organisasi belum memiliki berbagai metode pencatatan setiap insiden yang terjadi, minimal berupa template untuk memastikan pendekatan yang konsisten;
w. Tim respon insiden siber di organisasi belum memiliki kemampuan mendeteksi insiden tingkat lanjut (misalnya pencurian data, akses ilegal, penyusupan, aktivitas ilegal, dll);

x. Tim respon insiden siber di organisasi belum memiliki peralatan sumber daya analisis insiden (daftar host, packet snifer, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting);
y. Tim respon insiden siber di organisasi belum memiliki kemampuan berupa kompetensi forensik dan mendeteksi malware yang canggih (malware analysis, reverse engineering, dll);
z. Tim respon insiden siber belum memiliki alat pencitraan forensik;
aa. Organisasi belum memiliki dokumen prosedur operasional sistem IT dan jaringan;
bb. Organisasi belum memiliki kebijakan penanganan inisiden siber;
cc. Kebijakan penanganan insiden siber di organisasi belum selaras dengan kebijakan pengaturan kesinambungan Organisasi (Business Continuity Management) karena belum memiliki dokumen BCM;
dd. Organisasi belum memiliki dokumen prosedur penanganan insiden siber secara formal yang dikeluarkan oleh management senior (misalnya 1 level dibawah pimpinan tertinggi atau dipastikan berlaku di seluruh lingkup Organisasi, tidak hanya di unit pejabat bersangkutan) di Organisasi;
ee. Organisasi belum memiliki dokumen prosedur penanganan insiden siber secara formal yang dikeluarkan oleh manajemen senior yang dilengkapi dokumen SLA yang ditandatangani manajemen senior serta mengatur secara detail peranan penanggung jawab pada setiap proses;
ff. Organisasi belum mengimplementasikan pembatasan akses terhadap perangkat dan sistem melalui tata kelola akun dan password;
gg. Organisasi belum memiliki prosedur teknis yang mendukung tanggap insiden keamanan siber;
hh. Organisasi belum melakukan pencatatan/perekaman log yang tepat dan mengaktifkan fitur logging yang sesuai pada aset yang penting;
ii. Hasil perekaman log belum tersimpan dalam perangkat history log untuk periode yang cukup;

jj. Organisasi hanya memiliki sebagian kecil catatan informasi mengenai aset infrastruktur TI, beserta aset data yang diolah dengan infrastruktur TI tersebut;

kk. Jika terjadi insiden, tim tangggap insiden siber belum dapat mengakses informasi yang diperlukan dengan cepat;

ll. Organisasi tidak mencatat atau mendokumentasikan semua informasi terkait insiden yang terjadi;

mm. Jika terjadi insiden siber yang berdampak sangat serius, Organisasi belum memiliki prosedur untuk mendapat bantuan dengan cepat dari tim manajemen krisis;

nn. Jika terjadi insiden, tim tanggap insiden belum dapat dengan cepat mengakses informasi dari pihak ketiga yang berkaitan dengan pihak yang terkena insiden;

oo. Organisasi belum memiliki catatan informasi mengenai analisis dampak bisnis bila terjadi insiden;

pp. Jika terjadi insiden siber, tim tanggap insiden siber belum dapat dengan cepat mendapat bantuan dari tim atau unit kerja yang terkait dengan bagian bisnis, legal, SDM, dan juga komunikasi eksternal di Organisasi ;

qq. Organisasi belum memiliki prosedur kontrol untuk membantu mengurangi frekuensi kejadian dan/atau dampak insiden;

rr. Prosedur kontrol tersebut belum meliputi: klasifikasi informasi, access control, firewall, base line security;

ss. Prosedur-prosedur kontrol belum ditandatangani manajemen senior pada organisasi;

tt. Organisasi belum mengimplementasikan alat pemantau keamanan teknis berupa SIEM;

uu. Organisasi belum memiliki kontrol keamanan canggih berupa SOC dan pemisahan jaringan atau data sensitif;

vv. Prosedur kontrol belum meliputi tata kelola kerentanan dan sistem back up konfigurasi/data;

ww. Prosedur kontrol tersebut belum diperbarui secara regular berdasarkan informasi terbaru;

xx. Prosedur kontrol tersebut belum meliputi perlindungan malware;

yy. Prosedur kontrol tersebut belum direview efektivitas nya secara reguler oleh management senior di Organisasi ;

zz. Organisasi belum menetapkan mekanisme pengukuran tingkat kematangan terhadap pengelolaan insiden;

aaa. Organisasi belum mendefinisi "insiden keamanan siber" dalam fungsi Organisasi secara jelas;

bbb. Definisi insiden keamanan siber yang ditangani belum fokus mencakup insiden siber dasar dan insiden-insiden yang mudah diketahui;

ccc. Definisi insiden keamanan siber yang ditangani secara sporadis mencakup insiden keamanan canggih;

ddd. Organisasi secara umum telah memiliki program keperdulian tentang penanganan insiden namun belum secara rutin;

eee. Proses penanganan insiden yang terjadi belum di-review secara priodik;

fff. Pengukuran tingkat kematangan penanganan insiden belum dilakukan secara berkala pada tingkat manajemen senior dan dilaporkan ke tingkat manajemen puncak; dan

ggg. Kemampuan dan kapasitas penanganan insiden belum ditinjau secara berkala disesuaikan risiko bisnis.

2. Fase Respon

a. Organisasi belum dapat tahu suatu insiden dari hasil audit internal, masyarakat, dan pihak lain;

b. Organisasi secara sporadis menggunakan data log secara manual dalam mengidentifikasi detail suatu insiden;

c. Organisasi belum dapat tahu terjadinya insiden dari NMS atau alarm perangkat;

d. Organisasi belum menggunakan tools analisis pemantauan insiden dalam mengidentifikasi detail dari insiden;
e. Organisasi belum dapat tahu suatu insiden berdasarkan analisis sistem pemantauan insiden, seperti SOC (security operation center);
f. Organisasi belum menggunakan sumber informasi daftar potensi insiden yang tersedia umum;
g. Organisasi secara sporadis menggunakan jasa analisis spesialis dari pihak ketiga dalam mengidentifikasi detail dari insiden;
h. Organisasi tidak melakukan penyidikan/investigasi terhadap suatu insiden, jadi juga tidak menetapkan prioritas penyidikan untuk percepatan pemulihan;
i. Organisasi pada aktifitas penyidikan insiden belum melakukan triage
j. Sumber data analisis utama tidak diambil dari log perangkat;
k. Analisis penyidikan belum memiliki informasi rahasia yang diekspos/tercuri dan dampak operasional dari suatu insiden;
l. Organisasi belum memiliki personal yang berdedikasi sebagai perespon pertama sebuah insiden siber;
m. Sumber data analisis belum diambil dari peralatan monitoring keamanan;
n. Analisis penyidikan belum meliputi secara detail kejadian insiden terjadi dan siapa yang melakukan;
o. Analisis penyidikan belum meliputi dampak bisnis dan hukum dari suatu insiden;
p. Organisasi belum memiliki pengaturan eskalasi ke ahli/pakar insiden secara sistematis;
q. Organisasi secara sporadis memiliki tim management kritis yang mendukung insiden siber (tidak hanya insiden bencana) berupa surat penetapan;
r. Sumber data analisis belum berasal dari data eksternal;
s. Analisis penyidikan belum meliputi secara detail metode penyerangan terjadi, melakukan simulasi, dan menetapkan motif pelaku;
t. Organisasi secara sporadis memiliki bantuan pihak ketiga yang profesional;

u. Analisis penyidikan belum berhubungan dengan analisis dari berbagai peristiwa yang berbeda untuk melihat peluang kejadian tersebut berhubungan;
v. Tujuan utama pertahanan siber di Organisasi belum mencakup penjaminan fungsi IT beroperasi normal;
w. Ruang lingkup pertahanan siber di Organisasi secara umum belum mencakup pertahanan serangan dari luar;
x. Implementasi teknis pertahanan di Organisasi secara sporadis telah meliputi: penyaringan menggunakan firewall;
y. Tujuan pertahanan siber belum mencakup untuk menjamin bisnis beroperasi normal;
z. Implementasi teknis pertahanan di Organisasi telah secara sporadis meliputi: implementasi DMZ, sistem back up/ HA (high availbility) serta back up konfigurasi;
aa. Ketika terjadi insiden, laporan langkah-langkah yang dilakukan dalam rangka penanggulangan insiden belum dicatatkan;
bb. Tujuan pertahanan siber belum mencakup untuk keperluan analisis insiden;
cc. Ruang lingkup pertahanan siber di Organisasi belum mencakup pertahanan serangan dari dalam internal jaringan Organisasi;
dd. Implementasi teknis pertahanan di Organisasi telah secara umum meliputi: implementasi DC di jaringan internal dan pengaturan akses yang ketat berbasis fungsi/ tugas pemangku kepentingan;
ee. Laporan langkah-langkah yg dilakukan belum memiliki format yang baku;
ff. Tujuan pertahanan belum mencakup untuk keperluan remidiasi jangka panjang;
gg. Organisasi belum memiliki prosedur untuk pengambilan bukti serta laporan langkah-langkah yang melampirkan bukti yang relevan;
hh. Implementasi teknis pertahanan di Organisasi belum meliputi: implementasi DRC (*disaster recovery center*);
ii. Prosedur pengambilan bukti belum memenuhi persyaratan dalam hal aspek hukum positif;

jj. Tujuan proses pemulihan dari suatu insiden siber di organisasi secara sporadis mencakup menormalkan sistem sesegera mungkin, membatasi kerugian finansial dan memenuhi kewajiban regulasi, serta berupa aspek reputasi organisasi dan perlindungan data rahasia serta jaminan pihak lain (pelanggan, pihak ketiga, dll);

kk. Usaha pemulihan insiden pada Organisasi secara sporadis termasuk usaha untuk memperbaiki kerentanan agar insiden tidak berulang;

ll. Organisasi belum memiliki prosedur rencana pemulihan dasar;

mm. Prosedur rencana pemulihan insiden tersebut belum disusun berdasarkan sifat serangan;

nn. Setiap kejadian pemulihan dari insiden di Organisasi belum dibuatkan laporan pemulihannya;

oo. Usaha pemulihan belum termasuk usaha untuk memperbaiki kontrol keamanan;

pp. Rencana pemulihan belum sampai untuk insiden tingkat lanjut, masuk dalam skenario penanganan insiden, dan disusun berdasarkan aspek risiko bisnis;

qq. Laporan hasil pemulihan belum dilaporkan segera dan belum dicatat secara sistematis apalagi upaya secara aktif untuk merespon serangan;

rr. Laporan pemulihan belum direviu oleh manajemen senior di Organisasi;

ss. Usaha pemulihan belum termasuk usaha tindakan hukum pada pelaku kejahatan; dan

tt. Validasi pemulihan telah pulih melalui uji independen pihak lain.

3. Fase Tindak Lanjut

a. Organisasi belum melakukan identifikasi dari berbagai kasus insiden yang terjadi;

b. Organisasi belum memiliki prosedur penyelidikan insiden yang baku, sistematik, dan terstruktur;

c. Setiap insiden yang terjadi belum dilakukan analisis sampai pada tahap ditemukannya akar permasalahannya;

d. Organisasi belum menggunakan metode investigasi insiden siber mengacu pada internasional dan/atau best practice;

e. Organisasi belum menghitung dampak bisnis dari insiden keamanan siber;
f. Investigasi Organisasi belum terhubung dan selaras/sejalan dengan objektif Organisasi;
g. Organisasi belum membuat laporan insiden untuk setiap insiden siber;
h. Organisasi belum melaporkan laporan insiden sesuai dengan format yang baku;
i. Belum ada format pelaporan yang termasuk detail langkah-langkah yg telah dilakukan sampai pemulihan;
j. Format laporan insiden belum memuat aspek biaya kerugian dan pemulihan;
k. Laporan insiden yang terjadi belum dilaporkan ke manajemen puncak secara baku;
l. Format laporan insiden belum termasuk rekomendasi kontrol tindakan pencegahan;
m. Organisasi belum berperan serta dalam berbagi pengalaman dan masukan perbaikan sistem terkait kasus insiden yang dialami pada pihak lain;
n. Organisasi belum merekap laporan insiden yang terjadi dalam suatu periode
o. Organisasi belum mereviu terhadap rekap laporan tersebut;
p. Organisasi belum melakukan reviu pasca insiden terkait kebutuhan operasional;
q. Organisasi belum melakukan reviu pasca insiden terkait kecepatan tanggap dan waktu pemulihan;
r. Organisasi belum melakukan reviu terhadap prosedur terkait insiden;
s. Organisasi belum melakukan reviu pasca insiden terkait kemampuan SDM dalam menghadapi insiden;
t. Organisasi belum melakukan reviu pasca insiden terkait kelengkapan dan kesesuaian laporan;
u. Hasil reviu belum didistribusikan ke para pemangku kepentingan;
v. Hasil reviu belum digunakan untuk me-reviu kontrol yang ada;
w. Hasil reviu belum digunakan untuk tindakan pencegahan secara teknis;
x. Organisasi belum pernah melakukan simulasi penanganan insiden menggunakan SDM diluar tim penanganan insiden yang ada;

y. Proses reviu belum dilakukan evaluasi dan belum dilaporkan ke manajemen puncak;
z. Laporan insiden dan reviu belum diarsipkan dengan sistematik dan baik;
aa. Laporan dan reviu belum disusun menjadi materi pembelajaran untuk pencegahan perulangan kejadian;
bb. Informasi pasca insiden belum digunakan untuk perbaikan penanganan insiden siber di Organisasi;
cc. Pembaruan belum didokumentasikan dengan format dokumen formal;
dd. Pembaruan belum meliputi: aspek teknis dan prosedur penanganan insiden tertentu;
ee. Pembaruan belum mencakup skenario pelatihan/ simulasi menghadapi insiden;
ff. Pembaruan belum mencakup metodologi proses manajemen insiden;
gg. Pembaruan belum mencakup kontrol risiko;
hh. Pembaruan belum mencakup perubahan BCM;
ii. Laporan insiden dan reviu belum diarsipkan dan dicatat dengan baik; dan
jj. Organisasi belum memanfaatan data untuk analisis tren.

VI. Rekomendasi TMPI

Berdasarkan hasil penilaian, disampaikan rekomendasi berdasarkan prioritas utama pelaksanaan tindak lanjut sebagai berikut:

a. Kebijakan
   a. Menyusun kebijakan dan prosedur teknis yang mendukung penyelenggaraan keamanan pada sistem elektronik diantaranya : Peraturan Bupati terkait SMKI dan kebijakan teknis turunannya, prosedur teknis penanganan insiden, penetapan klasifikasi kritikalitas berdasarkan analisa risiko, dan pemenuhan NSPK pengelolaan insiden siber lainnya;
   b. Menyusun daftar aset berdasarkan klasifikasi kritikalitas berbasis analisis risiko operasional, berbasis analisis bisnis, aspek strategis organisasi, serta penanggung jawab setiap aset kritikal yang disusun secara sistematis dan terstruktur;

c. Menyusun dokumen penilaian dampak kerugian operasional, bisnis, dan aspek hukum secara mendalam untuk setiap potensi insiden yang telah diidentifikasikan;
d. Menyusun dokumen analisis ancaman keamanan siber (termasuk potensi kerentanan) beserta berbagai skenario penanganan kasus insiden siber mencakup semua jenis platform teknologi yang ada disusun secara sistematis yang jelas dan disimulasikan;
e. Menyusun dokumen prosedur operasional IT dan jaringan serta kebijakan penanganan insiden yang dilengkapi dengan dokumen SLA;
f. Menyusun dokumen BCP (*Business Continuity Plan*), DRP (*Disaster Recovery Plan*), dan BCM (*Business Continuity Management*) untuk melindungi proses bisnis yang kritis dari kegagalan/bencana alam atau yang dibuat manusia dengan ketidaktersediaan untuk proses bisnis secara normal;
g. Mereviu dan memperbaharui kebijakan dan prosedur yang ada berdasarkan analisis ancaman, keamanan siber, termasuk potensi kerentanan;
h. Menyusun analisa ancaman dan skenario ancaman terbaru sesuai dengan dinamika ancaman siber.

b. Rencana tanggap insiden
   a. Mendefinisikan sumber daya dan dukungan manajemen yang diperlukan untuk memelihara dan menyempurnakan kapabilitas respon insiden secara efektif;
   b. Melengkapi tim respon insiden siber di organisasi dengan peralatan sumber daya analisis insiden (daftar host, packet snifer, analisis protokol, dokumen protokol keamanan, diagram jaringan, daftar aset penting, dll) serta alat pencitraan forensik;
   c. Mengimplementasikan pembatasan akses terhadap perangkat dan sistem, mengimplementasikan peralatan kontrol teknis terkait keamanan jaringan, serta melakukan pengaktifan fitur perekaman log dengan periode yang cukup;
   d. Menghimpun catatan informasi mengenai aset infrastruktur TI (termasuk *baseline information asset*) berserta aset data yang diolah;

e. Menyediakan indikator dalam mengukur kapabilitas respon suatu insiden;
f. Menyusun, menetapkan, mendokumentasikan dan sosialisasi mengenai prosedur teknis untuk memfasilitasi implementasi kebijakan tanggap insiden dan kontrol tanggap insiden yang berkaitan;
g. Melakukan reviu terhadap rencana respon insiden secara berkala serta melakukan pembaharuan terhadap rencana respon insiden terkait.

c. Pelaksanaan tanggap insiden
   a. Melakukan implementasi tanggap insiden melalui kegiatan persiapan, deteksi dan analisis, *containment*, *eradication* dan upaya pemulihan yang terstruktur sesuai prosedur yang ditetapkan;
   b. Melakukan konfigurasi komponen sistem informasi sesuai standar dalam meningkatkan aspek keamanan seperti : konfigurasi router, daftar kontrol akses, parameter sistem deteksi/pencegahan intrusi, konfigurasi filter, konfigurasi firewall, dll;
   c. Menyusun berbagai skenario penanganan insiden siber dan menyimulasikannya;
   d. Melakukan pembelajaran dan tindak lanjut setelah terjadi insiden termasuk prosedur, kebutuhan pelatihan dan pengujian serta hasil implementasi;
   e. Menumbuhkan kesadaran keamanan kepada personil melalui berbagi informasi terkait regulasi, kebijakan dan tren insiden siber;
   f. Menyelenggarakan program peningkatan kapabilitas bagi SDM tanggap insiden terkait tugas dan tanggung jawab dibidang tanggap insiden menyesuaikan dengan metode, teknik, cara-cara baru serta sistem informasi yang sedang tren.

d. Monitoring insiden
   a. Mendokumentasikan dan memonitoring terkait insiden sistem informasi;
   b. Menggunakan otomatisasi mekanisme yang dapat membantu memonitor maupun pengumpulan data terkait pelaksanaan tanggap insiden;

c. Melakukan pengukuran tingkat kematangan terhadap pengelolaan insiden secara berkala pada tingkat manajemen senior dan dilaporkan kepada manajemen puncuk untuk ditinjau secara periodik.

e. Pelaporan
   a. Melaksanakan pelaporan pelaksanaan tanggap insiden dengan format standar termasuk detail langkah yang dilakukan sampai pemulihan kepada manajemen puncak termasuk pihak eksternal terkait;
   b. Menggunakan berbagai metode pencatatan setiap insiden yang terjadi, menyusun rekap sesuai periode yang ditetapkan untuk dilaporkan kepada manajer puncak, didistribusikan kepada pihak ekstrenal, ditinjau, dan dijadikan bahan pembelajaran.

f. Paska insiden
   a. Melaksanakan rekap atas laporan insiden dalam satu periode yang dilanjutkan dengan melakukan reviu terkait prosedur penanganan insiden, kebutuhan organisasi, kecepatan dan tenggat waktu pemulihan, kemampuan SDM dalam menghadapi insiden sehingga hasil reviu dapat digunakan untuk memperbaiki dan memperbaharui kontrol yang ada, serta digunakan dalam tindakan perbaikan dan pencegahan;
   b. Hasil reviu disusun dan didokumentasikan secara formal serta didistribusikan menjadi materi pembelajaran dan pencegahan perulangan kejadian serta digunakan untuk mengidentifikasi berbagai tren tentang dampak bisnis, biaya penanganan insiden dan investasi sistem pencegahan.

PENUTUP

Demikian hasil penilaian tingkat maturitas insiden siber di Dinas Komunikasi, Informatika dan Statistik Pemerintah Daerah Kabupaten Bangka, sebagai bahan masukan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Depok, 19 Mei 2025

Kepala Dinas Komunikasi, Informatika dan Statistik Pemerintah Daerah Kabupaten Bangka

Ditandatangani secara elektronik oleh :
KEPALA DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK

Drs. TEDDY SUDARSONO, M.Si
Pembina Utama Muda (IV/c)

Tim Badan Siber dan Sandi Negara

Dokumen Ini ditandatangani secara elektronik oleh:
Manggala Informatika Ahli Pertama

CARISSA MEGA YULIANINGRUM, S.Tr.TP.
Penata Muda Tingkat I (III/b)

Dokumen Ini ditandatangani secara elektronik oleh:
Sandiman Ahli Pertama

YULYANTI HENDRIANI, S.Tr.Kom
Penata Muda (III/a)

Ditandatangani secara elektronik oleh:
Penata Kelola Sistem dan Teknologi Informasi pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III

Ryu Arifial, S.Kom.
CPNS (III/a)