BADAN SIBER &
SANDI NEGARA

Ditandatangani secara elektronik oleh:
KEPALA SUBDIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH WILAYAH I

SRIYANTO, S.Sos., M.M
NIP. 19630921 198311 1 002

PENILAIAN TINGKAT MATURITAS PENANGANAN INSIDEN KEAMANAN SIBER INSTANSI PEMERINTAH

TINGKAT MATURITAS PENANGANAN INSIDEN KEAMANAN SIBER

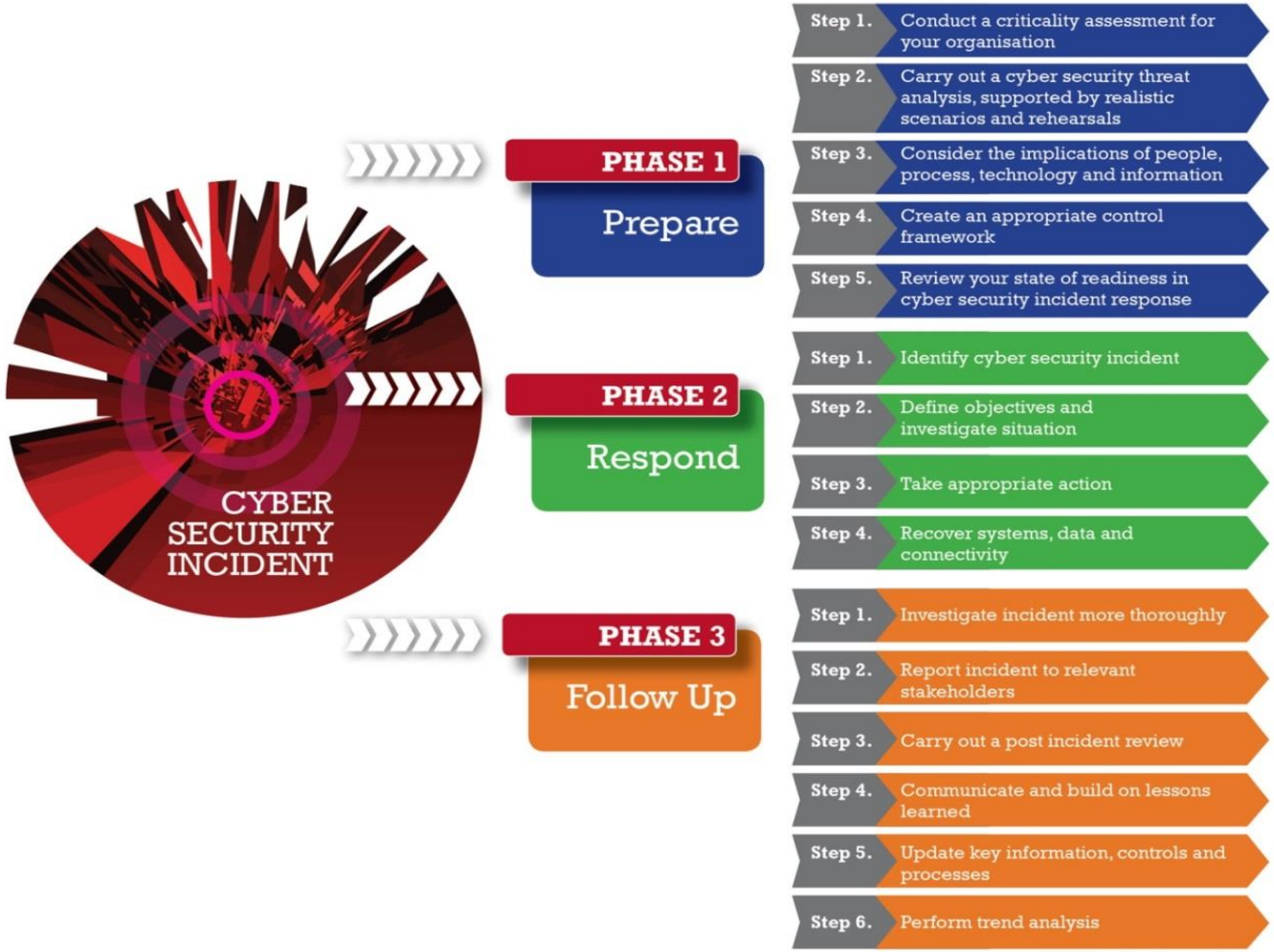
Insiden Keamanan Siber dapat terjadi sewaktu - waktu dan mempunyai eskalasi dampak yang beragam mulai dari yang ringan hingga berat tergantung tingkat dan jenis insidennya. Oleh karena itu, setiap Instansi Pemerintah harus mengembangkan kemampuan penanganan insiden keamanan siber dengan mengadopsi pendekatan yang sistematis dan terstruktur.

Untuk menilai kemampuan Instansi Pemerintah dalam menangani Insiden Keamanan Siber dapat dilakukan melalui pendekatan penilaian kesiapan/kematangan dengan alat bantu berupa **Instrumen Pengukuran Tingkat Maturitas Penanganan Insiden Keamanan Siber**

INSTRUMEN PENGUKURAN TINGKAT MATURITAS PENANGANAN INSIDEN KEAMANAN SIBER

Instrumen pengukuran tingkat maturitas penanganan insiden keamanan siber yang digunakan merujuk pada CREST - *CSIR Cyber Security Incident Response guide ver. 1.0,* berupa sejumlah pertanyaan yang didasarkan pada 15 langkah dalam 3 fase proses penanganan insiden keamanan siber yaitu :

1. Fase Persiapan
2. Fase Respon/ Tanggap Insiden Keamanan Siber
3. Fase Tindak Lanjut



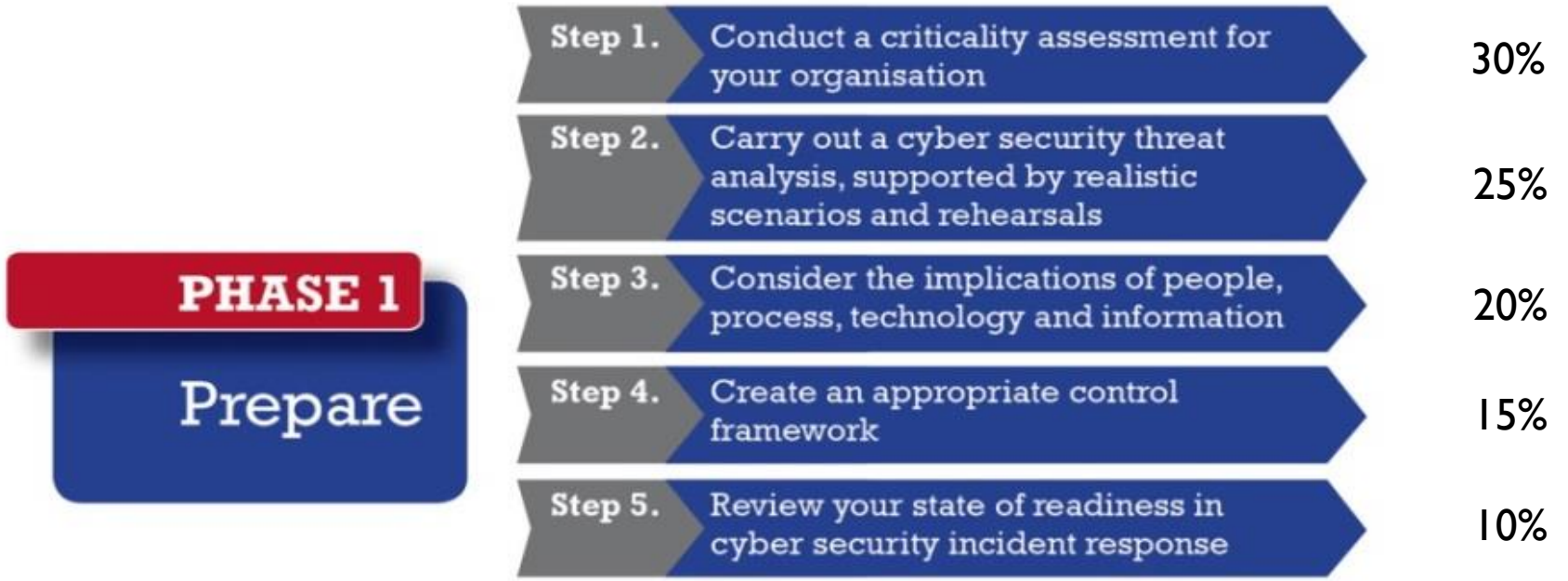
METODE PENGUKURAN

Seluruh pertanyaan dalam Instrumen ini merupakan pertanyaan dengan jawaban pilihan ganda

NO	PILIHAN JAWABAN	KRITERIA
0	Belum Dijawab	-
1	Tidak/Belum Dilakukan	Belum dilaksanakan, atau masih dalam **wacana** perencanaan (tidak ada dokumen resmi rencana penerapan)
2	Sporadis	Sudah menjadi rencana resmi instansi dan akan dilaksanakan melalui kegiatan internal atau proyek. Sudah ada dokumen kebijakan/ prosedur pengamanan siber dalam **versi draft**.
3	Umumnya/Sebagian Besar	Kegiatan/ Proyek sedang berjalan atau diterapkan secara bertahap. Dokumen kebijakan/ prosedur pengamanan siber sudah dirilis **secara resmi** tetapi masih tahap implementasi.
4	Ya/ Seluruhnya	Sudah berjalan di seluruh area sesuai dengan ruang lingkup yang didefinisikan

BOBOT PENILAIAN

- Prinsipnya tidak ada pembobotan secara spesifik
- Total bobot dalam 1 fase adalah 100%



30%

25%

20%

15%

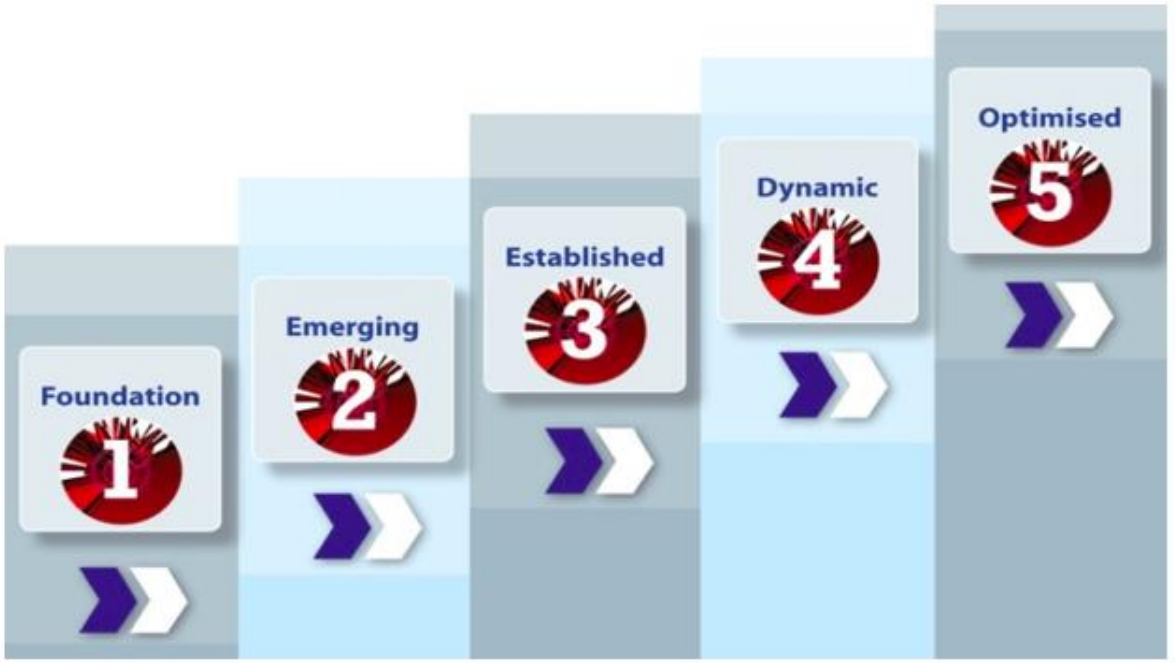
10%

Total 100%

BADAN SIBER & SANDI NEGARA

TINGKAT MATURITAS

- Instrumen Pengukuran Tingkat Maturitas Penanganan Insiden Keamanan Siber ini terdapat 5 tingkat Maturitas kemampuan penanganan insiden keamanan siber suatu instansi (organisasi), mulai dari IK1 (paling tidak efektif) hingga IK5 (paling efektif)



BADAN SIBER & SANDI NEGARA

TINGKAT MATURITAS

TINGKAT MATURITAS	KRITERIA
IK I	• Belum ada kebijakan, strategi dan prosedur manajemen insiden • Apabila sudah terjadi insiden, belum dapat diselesaikan dengan baik, memerlukan waktu yang lama, terjadi gangguan pada layanan/operasional yang signifikan

TINGKAT MATURITAS

TINGKAT MATURITAS	KRITERIA
IK 2	• Sudah ada kebijakan dan atau prosedur yang terkait dengan manajemen insiden, akan tetapi belum efektif/konsisten diterapkan • Apabila sudah terjadi insiden, sudah ada proses yang diupayakan berjalan akan tetapi penyelesaiannya tidak selalu efektif, memerlukan waktu dan berakibat gangguan pada layanan/operasional
IK 3	• Sudah ada kebijakan, strategi dan prosedur yang khusus membahas manajemen insiden • Sudah dilakukan simulasi penanganan insiden secara berkala • Pemahaman SDM yang ditugaskan sudah cukup, baik dari sisi kompetensi keamanan informasi, penanganan insiden maupun terkait operasional infrastruktur TI yang ada • Apabila sudah terjadi insiden, proses penanganannya sudah berjalan dengan baik/konsisten, penyelesaian insiden secara umum sudah sesuai dengan yang direncanakan, dan gangguan pada layanan/operasional dapat dibatasi

TINGKAT MATURITAS

TINGKAT MATURITAS	KRITERIA
IK 4	• Kebijakan, strategi dan prosedur yang khusus membahas manajemen insiden dikaji ulang sesuai secara berkala • Simulasi penanganan insiden dilakukan secara berkala, mencakup semua jenis platform teknologi yang ada, termasuk melibatkan mitra dan pihak eksternal (regulator, tim CSIRT lain) • SDM yang ditugaskan memiliki kompetensi formal di bidang manajemen insiden dan terlibat dalam upaya meningkatkan kesiapan manajemen insiden di internal organisasi • Apabila sudah terjadi insiden, deteksi dan proses penanganannya berjalan dengan efektif, keseluruhan penyelesaian insiden sesuai dengan yang direncanakan, dan gangguan pada layanan/operasional tidak signifikan

TINGKAT MATURITAS

TINGKAT MATURITAS	KRITERIA
IK 5	• Kebijakan, strategi dan prosedur yang khusus membahas manajemen insiden dikaji ulang sesuai dengan perkembangan risiko dan perubahan organisasi • Simulasi penanganan insiden dilakukan secara berkala termasuk melibatkan mitra dan pihak eksternal (regulator, tim CSIRT lain), dan melakukan simulasi terkait ancaman baru atau informasi insiden yang dilaporkan dari sumber eksternal • SDM yang ditugaskan merupakan pakar di bidangnya, terlibat dalam peningkatan kesiapan di sektor atau industry • Apabila sudah terjadi insiden, deteksi dan proses penanganannya berjalan sangat efektif, termasuk deteksi dan pencegahan secara dini.

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH