BADAN SIBER & SANDI NEGARA

PEMBENTUKAN CSIRT

DIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH,
DEPUTI BIDANG PENANGGULANGAN DAN PEMULIHAN – BSSN

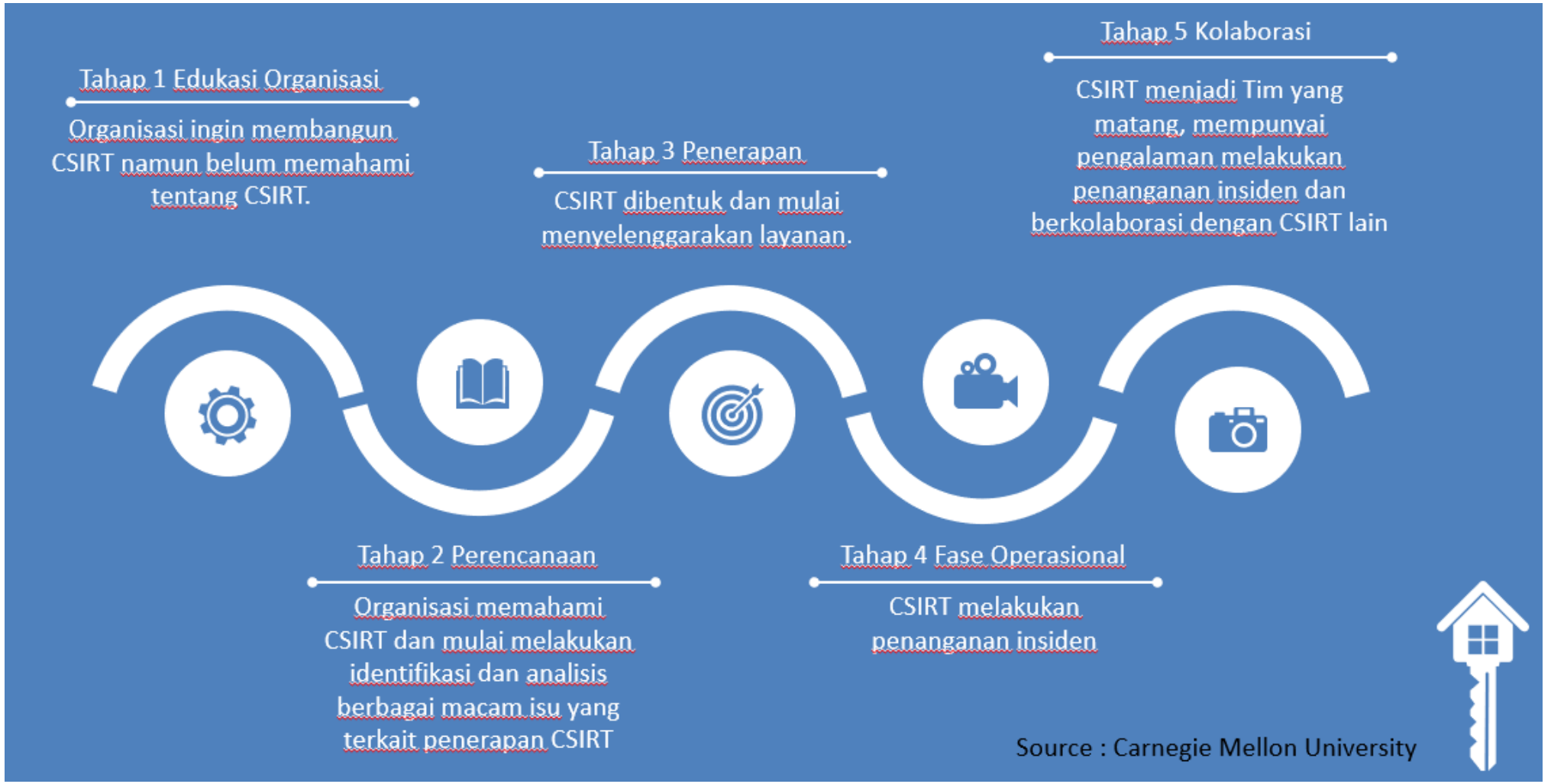
CSIRT

Tahapan Pembentukan CSIRT

Komponen CSIRT

Deklarasi CSIRT

TAHAPAN PEMBENTUKAN CSIRT



BADAN SIBER & SANDI NEGARA

EDUKASI ORGANISASI

- Memahami Aturan Hukum dan Regulasi
- Memahami Tujuan CSIRT
- Memahami Aset yang Dilindungi
- Memahami Model CSIRT
- Memahami Mekanisme Kerja CSIRT
- Memahami SDM CSIRT
- Memahami Pendanaan
- Memahami Layanan CSIRT

PERENCANAAN (PLANNING)

CSIRT
Computer Security Incident Response Team

- Merumuskan Visi dan Misi
- Mendefinisikan Tugas dan Kewenangan
- Identifikasi Kompetensi Staff
- Menyusun Rencana Kerja dan Anggaran
- Identifikasi Standar, Pedoman dan Regulasi
- Identifikasi Metode Membangun Kepercayaan, Komunikasi dan Koordinasi

PENERAPAN (IMPLEMENTATION)

- Memperoleh Pendanaan
- Deklarasi CSIRT
- Komunikasi dan Koordinasi
- Implementasi *Security Policy* pada Infrastruktur Jaringan dan Sistem Informasi
- Penerapan Kebijakan dan Prosedur operasional
- Identifikasi dan Rekrutmen Staff

OPERASIONAL (OPERATIONAL)

CSIRT
Computer Security Incident Response Team

- Menjalankan layanan CSIRT
- Mengembangkan dan Menerapkan Mekanisme Evaluasi CSIRT
- Adaptif Perubahan Lingkungan (Regulasi, Kebijakan, Konstituen)
- Peningkatan Kompetensi Staff
- Mengembangkan Kebijakan dan Prosedur

KOLABORASI (COLLABORATION)

- Partisipasi Pertukaran Informasi
- Partisipasi "Alert dan Warning" ke Komunitas dan CSIRT Lain
- Peningkatan Kualitas Operasional CSIRT
- Kolaborasi dengan CSIRT Lain
- Evaluasi Proses Manajemen Insiden

KOMPONEN CSIRT

DEKLARASI CSIRT

Umumnya menggunakan RFC-2350

BADAN SIBER & SANDI NEGARA

RFC-2350

- RFC adalah singkatan dari *Request for Comments*, yaitu seri dokumen informasi dan standar internet bernomor yang di ikuti secara luas oleh perangkat lunak untuk digunakan dalam jaringan, internet, dan beberapa sistem operasi jaringan, mulai dari Unix, Windows, dan Novell NetWare.
- RFC kini diterbitkan di bawah arahan Internet Society (ISOC) dan badan-badan penyusun-standar teknisnya, seperti Internet Engineering Task Force (IETF) atau Internet Research Task Force (IRTF).
- Contoh RFC yg umum antara lain : RFC-791 (Internet Protocol), RFC 793 (Transmission Control Protocol).
- RFC-2350 adalah standar yang dikeluarkan oleh IETF bulan Juni 1998 oleh N. Brownlee (Univ. of Auckland) dan E.Guttman (Sun Microsystem).
- Tujuan dokumen RFC-2350 untuk menggambarkan secara garis besar CSIRT, menyediakan informasi detail dalam suatu dokumen berformat legal, dimana konstituen dapat melihat kebijakan dan prosedur layanan CSIRT.
- Dokumen RFC-2350 dipublikasikan pada laman website CSIRT yang dibentuk.

RFC-2350

- Berikut dokumen RFC-2350, dimana terdapat 7 (tujuh) bagian.

BADAN SIBER & SANDI NEGARA

```
1 Document Information
1.1 Date of Last Update
1.2 Distribution List for Notifications
1.3 Locations where this Document May Be Found

2 Contact Information
2.1 Name of Team
2.2 Address
2.3 Time Zone
2.4 Telephone Number
2.5 Facsimile Number
2.6 Other Telecommunication
2.7 Electronic Mail Address
2.8 Public Keys and Encryption Information
2.9 Team Members
2.10 Other information
2.11 Points of Customer Contact

3 Charter
3.1 Mission Statement
3.2 Constituency
3.3 Sponsorship and/or Affiliation
3.4 Authority

4 Policies
4.1 Types of Incident and Level of Support
4.2 Co-operation, Interaction and Disclosure of Information
4.3 Communication and Authentication

5 Services
5.1 Incident Response
5.2 Proactive activities

6 Incident Reporting Forms

7 Disclaimers
```

RFC-2350

```
1 Document Information
1.1 Date of Last Update
1.2 Distribution List for Notifications
1.3 Locations where this Document May Be Found
```

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 20 Desember 2018.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Versi terbaru dari dokumen ini tersedia pada :
https://govcsirt.bssn.go.id/static/rfc2350/rfc2350-id.pdf (versi Bahasa Indonesia)
https://govcsirt.bssn.go.id/static/rfc2350/rfc2350-en.pdf (versi Bahasa Inggris)

RFC-2350

```
2 Contact Information
2.1 Name of Team
2.2 Address
2.3 Time Zone
2.4 Telephone Number
2.5 Facsimile Number
2.6 Other Telecommunication
2.7 Electronic Mail Address
2.8 Public Keys and Encryption Information
2.9 Team Members
2.10 Other information
2.11 Points of Customer Contact
```

2.1. Nama Tim

Government - Computer Security Incident Response Team (CSIRT) Indonesia
Disingkat : Gov-CSIRT Indonesia

2.2. Alamat

BSSN
Jl. Harsono RM No.70,
Ragunan - 12550
Pasar Minggu, Jakarta Selatan
Indonesia

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Telepon (021) 78833610

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

2.7. Alamat Surat Elektronik (*E-mail*)

bantuan70[at]bssn.go.id

RFC-2350

2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

Bits : 4096
ID : 0x73802BD6
Key Fingerprint : 1A35 DAEF E63B BE93 C314 3272 CE5D 2119 7380 2BD6

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBFtex4QBEADfLdjiJbwGTgOXUwyt/emyua3wIfYufUgpAKAzk2Dz8t9aj5bt
Co3adcXQw+5WnKSHbD7Q2VFUgLd+whIVuf6rAUraMcMrR10xWvvq2x4kEIEQiBXQ
CZOLgbN/9n+u2GqcD3x/XimyUDSN+I7DGh8+CioTWcahRQfcX70AqTlw5+VNFHT6
mrwAYfH8aQN2aPG+vW7j5K3AIEHVYFLYnU8F0FqBpcyFFlAWhqRgp6Jscsn9w0Ty
dR/v8laoaX1iE35XVyX3TXjS8TH+DCBuSP3BV0LVJJylSoEO4X0plKmERGW5UzaQ
CEbawtopt73QgWKcO5DTgMI247X3kekMchU8ENf25LdzrZ8znw8+DH/PggcCu6Hh
R/bccgXoFhQbrieZbDtuXKYn22/jJMWDKpJMQkGsPV2+qlMdYOXRrU87MhBE4dk2
dXLYCJki2qYnwddZp0HxRn6zznQ2VIrF+N3cBnQQB8izBFqcgy6gvkmJiUrGRn9n
upRryX7Wp1djfA13Veb1HftQNauOcWsJQt//fj5+MC9P6r3A4S2rgnojQv3zuPxP
XUVuvZOE0ywqXTfxPd7DdJE3ilP8fLvdWEZoFHlZkBkAZtFFsbjNlEhUc7IBQtOR
B7wRptGQxajH26ru/atRpcfxAFx6pfYG5Hr0X1a7xqmpvPdxFcs5dQ0NnwARAQAB
tDRCYW50dWFuNzAgUHVzb3Bza2Ftc2luYXMgQlNTTiA8YmFudHVhbjcwQGJzc24u
Z28uaWQ+iQJUBBMBCAA+FiEEGjXa7+Y7vpPDFDJyzl0hGXOAK9YFAltex4QCGyMF
CQlmAYAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQzl0hGXOAK9Y9IA/+NULC
uXxF+Ko/l3x482/7yJS6oElhqY17nskNFjmBqM6fwTFdQybarqs1AgxN3ne26MWs
VcmhSLsOaiN7tEnD0jPlRgqCZ4SnXeqthbuloCb6cMI4Mae1gRRM4pb1ec4OyriW
infNAa+zWolZNuQG0cz/xuVme34lmv3Nv9WutCuyjGR3RenixIg68Sww7tV4x3gw

RFC-2350

2.9. Anggota Tim

Ketua Gov-CSIRT Indonesia adalah Direktur Penanggulangan dan Pemulihan Pemerintah, Deputi Bidang Penanggulangan dan Pemulihan, BSSN. Yang termasuk anggota tim adalah seluruh staf BSSN di sektor pemerintah.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Gov-CSIRT Indonesia

Metode yang disarankan untuk menghubungi Gov-CSIRT Indonesia adalah melalui *e-mail* pada alamat bantuan70[at]bssn.go.id atau melalui nomor telepon (021) 78833610 ke Pusopskamsinas yang siaga selama 24/7.

RFC-2350

```
3 Charter
3.1 Mission Statement
3.2 Constituency
3.3 Sponsorship and/or Affiliation
3.4 Authority
```

BADAN SIBER & SANDI NEGARA

3.1. Misi

Tujuan dari Gov-CSIRT Indonesia, yaitu :

a. membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor pemerintah
b. membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah
c. membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah
d. mendorong pembentukan CSIRT (*Computer Security Incident Response Team*) pada sektor pemerintah

RFC-2350

3.2. Konstituen

Konstituen Gov-CSIRT Indonesia meliputi Pemerintah Pusat, Pemerintah Daerah wilayah I, dan II yaitu :

a. Pemerintah Pusat adalah Presiden Republik Indonesia yang memegang kekuasaan pemerintahan negara Republik Indonesia yang dibantu oleh Wakil Presiden dan Menteri sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
b. Pemerintah Daerah Wilayah I adalah Pemerintah Daerah Provinsi yang meliputi wilayah Provinsi Aceh, Sumatera Utara, Riau, Sumatera Barat, Kepulauan Riau, Jambi, Sumatera Selatan, Bangka Belitung, Bengkulu, Lampung, Daerah Khusus Ibu Kota Jakarta, Jawa Barat, Banten, Jawa Tengah, Daerah Istimewa Yogyakarta, Jawa Timur, dan Bali
c. Pemerintah Daerah Wilayah II adalah Pemerintah Daerah Provinsi yang meliputi wilayah Provinsi Kalimantan Barat, Kalimantan Tengah, Kalimantan Selatan, Kalimantan Timur, Kalimantan Utara, Sulawesi Utara, Gorontalo, Sulawesi Tenggara, Sulawesi Tengah, Sulawesi Selatan, Sulawesi Barat, Nusa Tenggara Timur, Nusa Tenggara Barat, Papua Barat, Papua, Maluku, dan Maluku Utara

RFC-2350

3.3. Sponsorship dan/atau Afiliasi

Gov-CSIRT Indonesia merupakan bagian dari BSSN sehingga seluruh pembiayaan bersumber dari APBN.

3.4. Otoritas

Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang BSSN sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017, Gov-CSIRT Indonesia memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada sektor pemerintah.
Gov-CSIRT Indonesia melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

RFC-2350

```
4 Policies
4.1 Types of Incident and Level of Support
4.2 Co-operation, Interaction and Disclosure of Information
4.3 Communication and Authentication
```

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

Gov-CSIRT Indonesia memiliki otoritas untuk menangani berbagai insiden keamanan siber yang terjadi atau mengancam konstituen kami (dapat dilihat pada Subbab 3.2).
Dukungan yang diberikan oleh Gov-CSIRT Indonesia kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Gov-CSIRT Indonesia akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.
Seluruh informasi yang diterima oleh Gov-CSIRT Indonesia akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa Gov-CSIRT Indonesia dapat menggunakan alamat *e-mail* tanpa enkripsi data (*e-mail* konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada *e-mail*.

BADAN SIBER & SANDI NEGARA

RFC-2350

5 Services
5.1 Incident Response
5.2 Proactive activities

5.1. Respon Insiden

Gov-CSIRT Indonesia akan membantu konstituen untuk melakukan penanggulangan dan pemulihan insiden keamanan siber dengan aspek-aspek manajemen insiden keamanan siber berikut :

5.1.1. Triase Insiden (*Incident Triage*)

a. Memastikan kebenaran insiden dan pelapor
b. Menilai dampak dan prioritas insiden

5.1.2. Koordinasi Insiden

a. Mengkoordinasikan insiden dengan konstituen
b. Menentukan kemungkinan penyebab insiden
c. Memberikan rekomendasi penanggulangan berdasarkan panduan/SOP yang dimiliki Gov-CSIRT Indonesia kepada konstituen
d. Mengkoordinasikan insiden dengan CSIRT atau pihak lain yang terkait

5.1.3. Resolusi Insiden

a. Melakukan investigasi dan analisis dampak insiden
b. Memberikan rekomendasi teknis untuk pemulihan pasca insiden
c. Memberikan rekomendasi teknis untuk memperbaiki kelemahan sistem

Gov-CSIRT Indonesia menyajikan data statistik mengenai insiden yang terjadi pada sektor pemerintah sebagai bentuk sentra informasi keamanan siber pada sektor pemerintah.

RFC-2350

5.2. Aktivitas Proaktif

Gov-CSIRT Indonesia secara aktif membangun kesiapan instansi pemerintah dalam melakukan penanggulangan dan pemulihan insiden keamanan siber melalui kegiatan :

a. *Cyber Security Drill Test*
b. *Workshop* atau Bimbingan Teknis
c. Asistensi Pembentukan CSIRT organisasi

RFC-2350

6 Incident Reporting Forms

7 Disclaimers

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke bantuan70[at]bssn.go.id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. *Disclaimer*

Tidak ada

UNIT KERJA YG MENANGANI CSIRT

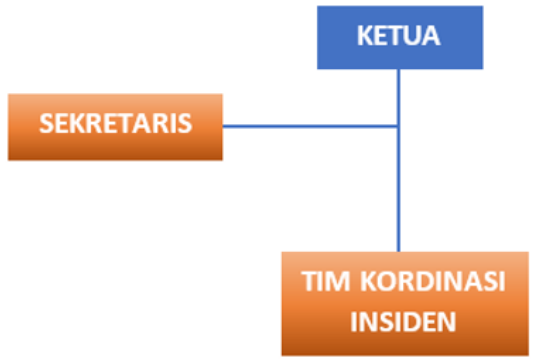
Pelayanan CSIRT berada di unit kerja yang menyelenggarakan fungsi TIK dan Keamanan informasi sehingga CSIRT dilaksanakan oleh Unit Kerja yang memiliki kewenangan di bidang tersebut.

- Kementerian /Lembaga (K/L) : Pusdatik /Pusdatin /Pusdasi
- Pemerintah Daerah (Pemda) : Diskominfo

BADAN SIBER & SANDI NEGARA

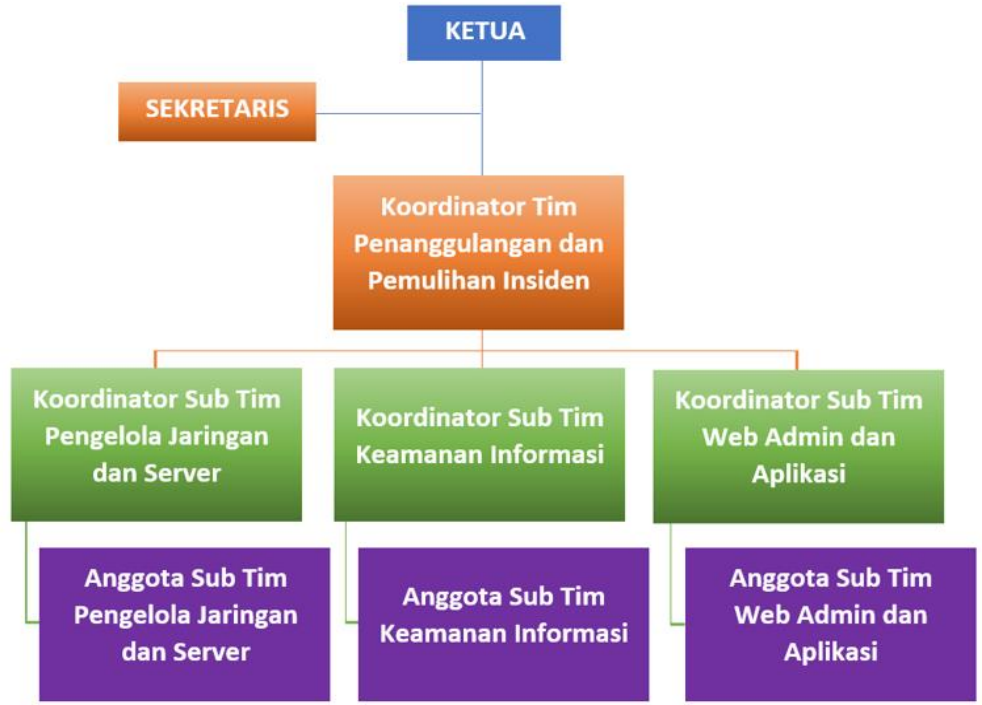
BAGAIMANA MENYUSUN TIM CSIRT

Tim CSIRT dibentuk berdasarkan layanan yang diberikan kepada konstituen dan keahlian staf yang dimiliki.

LAYANAN	TIM INTERNAL	STRUKTUR CSIRT
KOORDINASI INSIDEN	TANPA TIM INTERNAL	

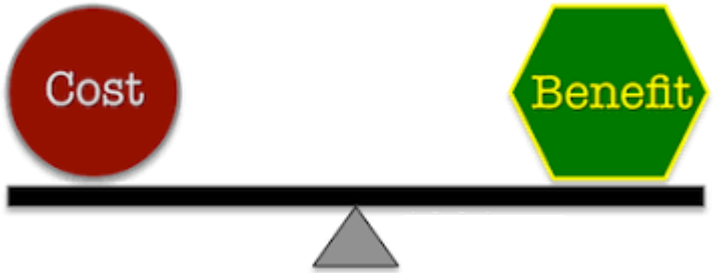
Hindari struktur dibuat tapi layanan tidak ada.

CONTOH

LAYANAN	TIM INTERNAL	STRUKTUR CSIRT
RESPON INSIDEN	MEMILIKI TIM INTERNAL	

KEBUTUHAN BIAYA OPERASIONAL CSIRT

Kebutuhan biaya operasional CSIRT, berdasarkan Layanan yang diberikan serta jumlah staf CSIRT /keahliannya. Sebaiknya manfaat yang diberikan sebanding dengan biaya yang dikeluarkan.

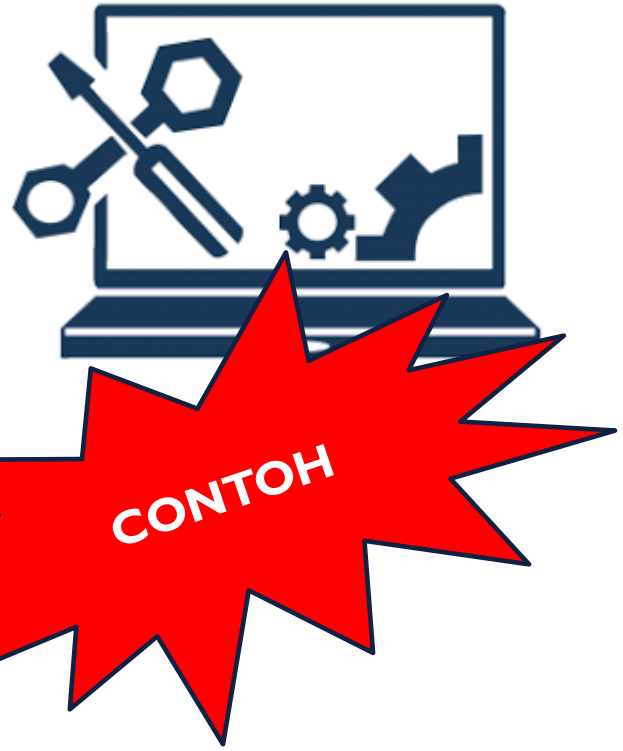


- Pengelolaan web CSIRT
- Tim piket
- Biaya respon
- Seminar /workshop /pelatihan

BADAN SIBER & SANDI NEGARA

PERANGKAT YANG DIBUTUHKAN

LAYANAN	TIM INTERNAL	PERANGKAT
KOORDINASI INSIDEN	TANPA TIM INTERNAL	❑ Publikasi web CSIRT Digabungkan dengan website utama ❑ Pembuatan web K/L atau Pemda CSIRT Server, Aplikasi Web, Firewall, AntiVirus
RESPON INSIDEN	MEMILIKI TIM INTERNAL	❑ Publikasi web CSIRT Digabungkan dengan website utama ❑ Pembuatan web K/L atau Pemda CSIRT Server, Aplikasi Web, Firewall, AntiVirus ❑ Log Analyzer, Vulnerability Scanner, Forensic, Analisa Malware



BADAN SIBER & SANDI NEGARA

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH