Perencanaan Strategis Pembentukan Pusat Respon Insiden Keamanan Informasi Pemerintah

Strategic Planning for Development of The Government Information Security Incident Response Center

Ahmad Budi Setiawan
Puslitbang APTIKA dan IKP, Badan Litbang SDM,
Kementerian Komunikasi dan Informatika
Jl. Medan Merdeka Barat No. 9. Jakarta Pusat 10110,
e-mail: ahma003@kominfo.go.id

Naskah diterima: 11 Maret 2013,direvisi: 11 April 2013,disetujui: 24 Mei 2013

Abstrak

Seiring dengan pesatnya penggunaan Teknologi nformasi dan Komunikasi (TIK) di kalangan instansi pemerintah, terdapat juga masalah keamanan informasi yang timbul dalam bentuk insiden keamanan informasi. Untuk mengatasi serangan keamanan pada sistem informasi tersebut, pemerintah perlu membentuk Pusat Respon Keamanan Informasi Pemerintah. Penelitian ini mengusulkan sebuah rencana strategis untuk pembentukan Pusat Penanganan Keamanan Informasi Pemerintah. Perencanaan strategis bagi Pusat Penanganan Keamanan Informasi Pemerintah menggunakan metode yang dikembangkan oleh *Carnegie Mellon University* (CMU) dan disesuaikan dengan karakteristik organisasi. Hasil penelitian ini adalah rekomendasi dan sebuah rencana strategis berupa peta jalan pembentukan pusat respon insiden keamanan informasi untuk diimplementasikan pada instansi pemerintah.

Kata Kunci: perencanaan strategis, pusat penanganan keamanan informasi pemerintah, kerangka kerja *Carnegie Mellon University*

Abstract

Along with the rapidly use of Information and Communication Technology (ICT) among government agencies, there are also problems that arise in the field of information security in the form of information security incidents. To deal with security attacks on information systems, the Government needs to establish their Government Information Security Incident Response Center. This research proposes a strategic plan for the establishment of the Government Information Security Incident Response Center. Strategic Planning for Government Information Security Incident Response Center's method is developed by Carnegie Mellon University which is adjusted with the characteristics of the organization. The results of this study are recommendations and strategic planning in the shape of a roadmap on the establishment of an information security incident response center to be implemented in government agencies.

Keywords: *strategic planning, government information security incident response center, Carnegie Mellon University framework*

PENDAHULUAN

Saat ini, peranan Teknologi Informasi dan Komunikasi (TIK) pada berbagai aspek kehidupan semakin dominan. Seiring dengan masifnya penggunaan TIK tersebut, terdapat pula masalah yang muncul di bidang keamanan informasi dalam bentuk insiden keamanan informasi. Ketergantungan terhadap TIK membuat individu dan organisasi menjadi sangat rentan akan serangan terhadap infrastruktur TIK, seperti *hacking, cyberterrorism, cybercrime* dan lain-lain, termasuk organisasi Pemerintahan sebuah Negara. Insiden keamanan informasi adalah suatu kejadian tunggal atau serangkaian kejadian keamanan informasi yang tidak diduga atau tidak dikehendaki yang mempunyai kemungkinan besar mengganggu operasi bisnis dan mengancam keamanan informasi (Badan Standardisasi Nasional, 2008).

Begitu banyak jenis insiden yang terjadi di dunia maya, mulai dari yang sangat sederhana hingga yang sangat kompleks modus operandinya. Berdasarkan hasil Kajian Kesiapan Keamanan Informasi Pemerintah (Puslitbang APTIKA&IKP, 2012), menyebutkan bahwa banyak situs web penyedia layanan informasi di instansi pemerintah masih rentan serangan. Hal ini desebabkan karena situs *web* dan sistem *online* ketika dirancang tidak memperhitungkan aspek keamanan yang kuat sehingga sistem mudah dijebol. Masalah menjadi lebih berat karena terdapat banyak instansi pemerintah yang tidak memiliki standard prosedur *recovery* untuk mengantisipasi setiap terjadinya insiden keamanan informasi.

Melihat begitu banyaknya insiden keamanan informasi yang menyerang instansi pemerintah baik pusat maupun daerah, maka pemerintah Indonesia telah membentuk Tim Respon Insiden Keamanan Informasi Pemerintah (*Gov-CERT*) berdasarkan surat keputusan (SK) Dirjen APTIKA No.: 01/SK/DJAI/KOMINFO /01/ 2012. Berdasarkan SK tersebut, Direktorat Keamanan Informasi, Ditjen Aplikasi Informatika, Kementerian Komunikasi dan Informatika telah ditunjuk sebagai koordinator Tim Respon Insiden Keamanan Informasi Pemerintah atau dinamakan dengan Gov-CSIRT Indonesia, Direktorat Keamanan Informasi yang bertanggung jawab untuk merespon dan sebagai pusat koordinasi setiap terjadinya insiden keamanan informasi di lingkungan instansi Pemerintah.

Berdasarkan hal tersebut, maka Direktorat Keamanan Informasi harus menjalankan peran dan tanggung jawab dalam merespon dan menindaklanjuti setiap insiden keamanan informasi yang terjadi di lingkungan instansi pemerintahan. Dengan demikian, permasalahan yang telah dijabarkan sebelumnya, maka rumusan masalah yang menjadi pertanyaan pada peneltian ini adalah bagaimana perencanaan strategis Pusat Respon Insiden Keamanan Informasi Pemerintah (GovCSIRT)?

Secara garis besar tujuan penelitian ini adalah untuk membuat sebuah perencanaan strategis Organisasi Pusat Respon insiden Keamanan Informasi Pemerintah yang selaras dengan visi-misi serta tujuan bisnis Kementerian Komunikasi dan Informatika, khususnya Direktorat Keamanan Informasi. Adapun manfaat yang diperoleh dari penelitian ini adalah:

1. Hasil penelitian ini dapat digunakan sebagai kerangka acuan untuk mengimplementasikan Pusat Respon Insiden Keamanan Informasi Pemerintah menggunakan *blue print* yang dihasilkan dari penelitian ini, sehingga dapat diimplementasikan pada instansi pemerintah lainnya baik tingkat pusat maupun daerah
2. Manfaat praktis yang dapat diberikan oleh hasil penelitian ini adalah berupa sumbangan pemikiran bagi instansi pemerintah baik pusat maupun daerah untuk menerapkan tim respon insiden keamanan informasi pada masing-masing instansi dan bagaimana prosedur pelaksanaannya serta model komunikasi antar tim respon insiden keamanan informasi lainnya.

Kajian ini berkaitan dengan teori-teori yang berkaitan dengan objek kajian. Teori

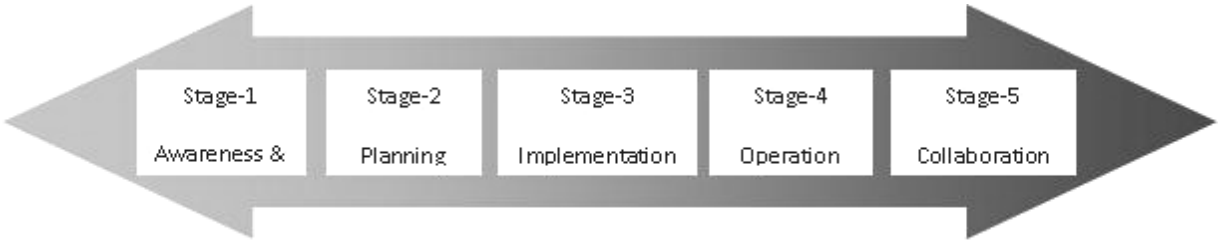
yang digunakan terkait dengan teori Perencanaan Strategis Kelembagaan Organisasi dan Sistem Informasi serta terkait juga dengan teori Keamanan Informasi. Secara umum Informasi didefinisikan sebagai sebuah produk abstrak dan merupakan hasil dari aktivitas mental yang ditransmisikan melalui sebuah medium. Dalam bidang TIK, informasi adalah sekumpulan fakta hasil dari sebuah pemrosesan, manipulasi dan pengaturan data yang dapat ditransmisikan (UN-APCICT/ESCAP, 2011). Sementara definisi informasi menurut standar ISO/IEC 27001 adalah sebuah aset yang memiliki nilai dan harus dilindungi (ISO/IEC 27001, 2005). Dalam masyarakat berbasis informasi dan pengetahuan, informasi adalah aset penting yang sangat berharga karena dengan kemampuan untuk mendapatkan, menganalisis dan menggunakan informasi dapat memberikan keunggulan bersaing bagi negara mana pun. Keamanan informasi dapat juga disebut sebagai sebuah tindakan menghargai nilai informasi sebagai sebuah aset yang berharga dengan melindungi informasi tersebut dari berbagai ancaman.

Adapun pusat Respon Insiden Keamanan Informasi atau lebih populer dalam Bahasa Indonesia disebut dengan Tim Respon Insiden Keamanan Informasi dan secara Internasional dikenal dengan istilah *Computer Emergency Response Team* (CERT) merupakan tim koordinasi teknis terkait insiden jaringan internet di seluruh dunia. Inisiatif pendirian Computer CERT dilakukan pada tahun 1988 oleh *Carneigie Mellon Software Engineering Institute* dengan membentuk CERT sebagai lembaga nirlaba (West-Brown et al., 2003). Tujuan dibentuknya lembaga ini untuk secara bersama menganalisis dan merespon ancaman keamanan sistem informasi yang terjadi di suatu wilayah tertentu.

Belakangan, tim ini disempurnakan lagi melalui RFC 2350 dengan nama CSIRT (*Computer Security Incident Response Team*). CERT maupun CSIRT di setiap negara umumnya dibangun oleh komunitas. Walaupun ada juga yang didukung oleh negara seperti halnya KrCERT (Korea Selatan), JPCERT (Jepang), AusCERT (Australia), dan sebagainya. CERT di setiap negara memiliki beragam kewenangan pekerjaan dan konstituen yang digarap. Setiap CSIRT di dunia memiliki pola yang berbeda di satu negara dengan negara lainnya.

Salah satu metode yang digunakan dalam melakukan perencanaan strategis pengembangan Pusat Respon Insiden Keamanan Informasi adalah metode buatan CMU (*Carnegie Melon University*) yang merupakan lembaga inisiator pendirian CERT. Metodologi CMU tersebut berisikan kerangka kerja (*framework*), arahan dan strategi yang dapat digunakan dalam pengembangan sebuah tim respon insiden keamanan informasi. Setiap CSIRT memiliki kriteria tersebut di atas yang berbeda-beda dan harus mendefinisikan kriteria masing-masing sesuai dengan lingkungan dan konstituennya (Danny Smith, 1994). Gambar 1. menjelaskan metode pengembangan sebuah CSIRT.

Tahapan pengembangan sebuah CSIRT yang dikembangkan oleh CMU, seperti yang



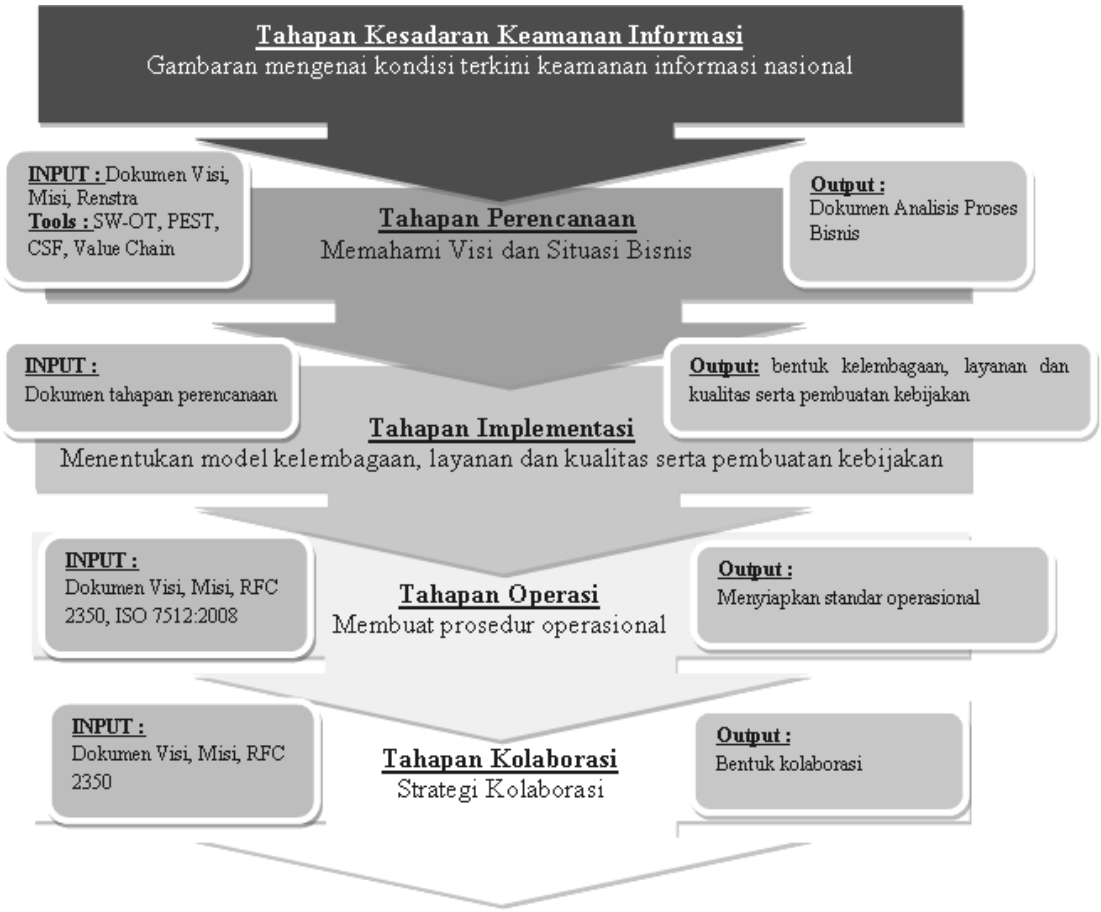
Gambar 1. Tahapan Pengembangan *CSIRT* versi CMU SEI.
(Sumber: West-Brown et al., 2003)

ditunjukkan oleh Gambar 2, terdiri dari 5 (lima) tahapan, yaitu:

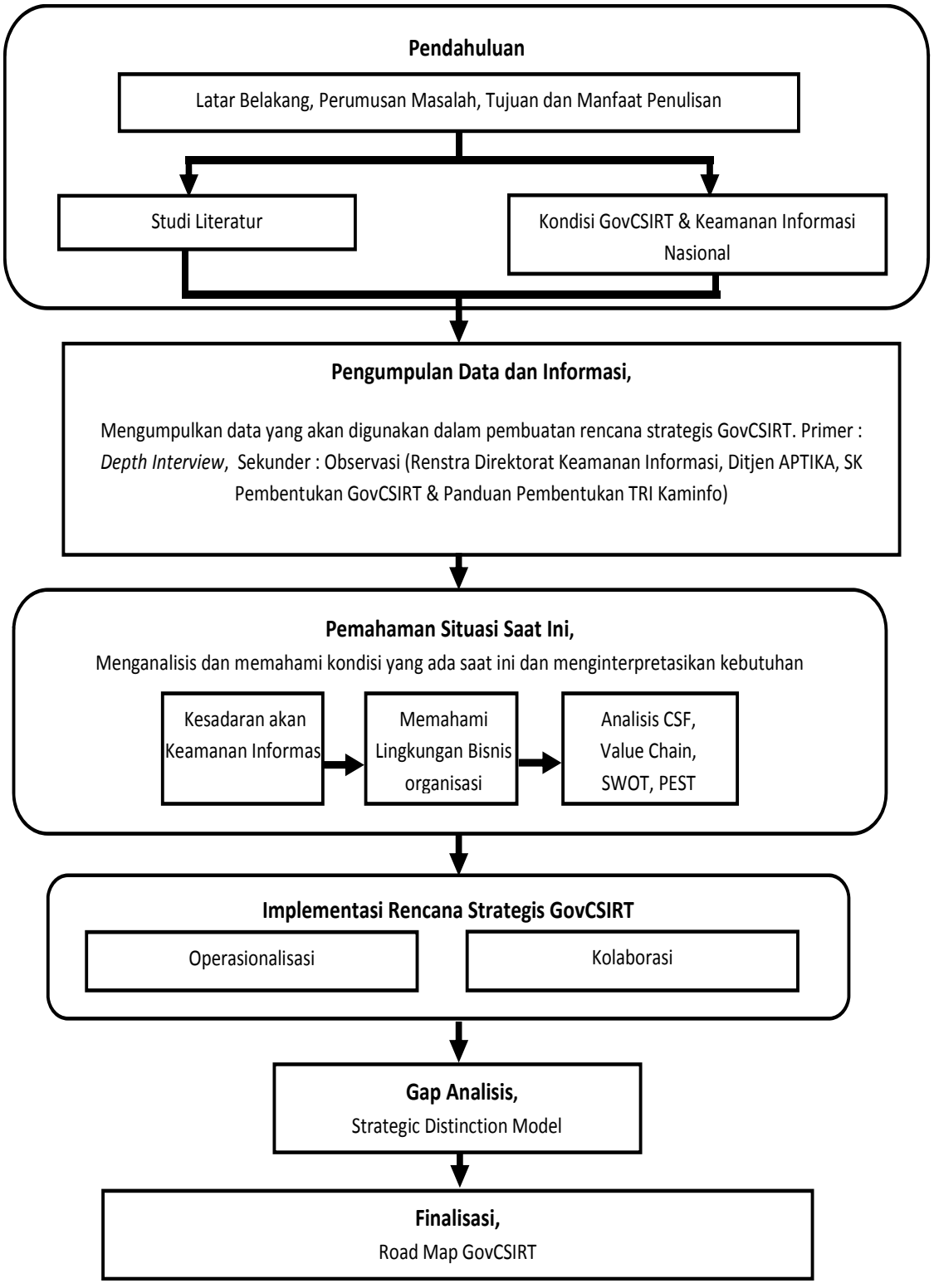
- Tahapan-1 : Pendidikan dan Pembinaan Kesadaran.
  Fase pendidikan, pembinaan kesadaran akan keamanan informasi kepada para pemangku kepentingan (*stakeholder*).
- Tahapan-2 : Perencanaan.
  Dalam tahapan ini dilakukan perencanaan pengembangan CSIRT secara spesifik mulai dari mendefinisikan visi-misi dan penentuan tujuan organisasi.
- Tahapan-3: Implementasi.
  Pada tahapan ini, kedua fase tahapan pengembangan CSIRT sebelumnya diformalisasikan.
- Tahapan-4: Operasional CSIRT.
  Pada tahapan ini, organisasi CSIRT telah mulai diimplementasikan dan infrastruktur telah terpasang.
- Tahapan-5: Kolaborasi.
  Pada tahapan akhir ini, CSIRT telah resmi beroperasi dan organisasi CSIRT telah matang (*mature*).

METODE

Untuk membahas permasalahan dalam penelitian ini digunakan metode yang diturunkan dari kerangka kerja pembentukan tim respon insiden keamanan informasi dari CMU SEI yaitu CSIRT framework yang disesuaikan dengan karakteristik dan kebutuhan organisasi. Penelitian ini menggunakan pendekatan kualitatif. Adapun tahapan/alur metode yang dilakukan dijelaskan pada Gambar 3.



Gambar 2. *Framework* Perencanaan Strategis Pusat Respon insiden Keamanan Informasi
(Sumber: CMU framework West-Brown, et.al, 2003)



Gambar 3. Alur Metode

Analisis dan interpretasi data dilakukan peneliti adalah menggunakan metode analisis kualitatif dengan pendekatan logika induktif, dimana penarikan kesimpulan dibangun berdasarkan pada hal-hal khusus atau data di lapangan yang bermuara pada kesimpulan-kesimpulan umum. Analisis data kualitatif adalah upaya yang dilakukan dengan cara mengorganisasikan data dengan memilah-milahnya menjadi satuan yang dapat dikelola kemudian mensintesanya. Kemudian berdasarkan proses tersebut, ditemukan apa yang penting dan apa yang dapat dipelajari untuk menunjang keputusan. Dalam hal analisa, pada penelitian ini digunakan unit analisis *supply chain*, SWOT, dan CSF.

Alur metode didasarkan pada kerangka kerja (*framework*) perencanaan strategis pembentukan pusat respon insiden keamanan informasi yang merujuk pada kerangka kerja CMU. Metode tersebut menjadi kerangka kerja bagi penelitian yang dilakukan. Adapun kerangka kerja menyajikan arsitektur dengan kemampuan untuk memvisualisasikan keseluruhan sistem dan dengan menilai opsi/pulihan lainnya serta mengkomunikasikan desain lebih jelas sebelum mengambil resiko dalam implementasi (Cernosek & Naiburg, 2004).

HASIL DAN PEMBAHASAN

Bagian ini membahas mengenai analisis penelitian Perencanaan Strategis Pusat Respon insiden Keamanan Informasi Pemerintah sesuai dengan tahapan-tahapan kerangka kerja pengembangan CSIRT versi CMU. Analisis dilakukan terhadap data yang dikumpulkan seputar profil organisasi dan kondisi organisasi saat ini.

Analisis Perencanaan Strategis Pembentukan Tim Respon Insiden Keamanan Informasi Pemerintah

Bagian dari tahapan perencanaan ini bertujuan untuk mengidentifikasi persyaratan yang dibutuhkan dalam mengembangkan GovCSIRT. Identifikasi dilakukan dengan melibatkan beberapa aktivitas seperti mengidentifikasi peraturan hukum dan peraturan yang mempengaruhi GovCSIRT dan tren insiden saat ini untuk menentukan fokus layanan yang akan diberikan GovCSIRT. Analisis dilakukan dengan menggunakan analisis *value chain*, matriks SWOT (*Strength, Weakness, Opportunity*, *Threats*), TOWS, dan Analisis CSF.

Penurunan analisis pembentukan CSIRT dimulai dari mendefinisikan visi-misi CSIRT. Pernyataan misi sebuah CSIRT harus fokus pada aktivitas inti tim, yaitu untuk menindaklanjuti laporan insiden keamanan informasi dan mendukung konstituen dalam menangani insiden (Brownlee & Guttman, 1998). Adapun visi GovCSIRT adalah ”Membangun Kesadaran Keamanan Informasi dan Kenyamanan dalam Menggunakan Teknologi Internet pada Lingkungan Pemerintah”, sementara misi GovCSIRT adalah ”Melakukan Bimbingan Teknis dan Sosialisasi Keamanan Informasi, Guna Menumbuhkan Kesadaran Keamanan Informasi serta Memberikan Pemantauan Keamanan Informasi pada Pemerintah“[1].

a. Analisis *Value Chain*.

Analisis *value chain* (mata rantai nilai) digunakan untuk mengidentifikasikan dan menghubungkan berbagai aktivitas strategis pada organisasi agar dapat memberikan nilai tambah bagi organisasi dalam memberikan layanan kepada pelanggan (Porter, 1998). Sebagaimana surat keputusan Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika No.: 01/SK/DJAI/KOMINFO/01/2012 Tentang Pembentukan Tim Pusat Monitoring dan Penanganan Tanggap Darurat Keamanan Informasi Instansi Pemerintah (GovCSIRT), bahwa dalam rangka mendukung pelaksanaan program monitoring, evaluasi dan tanggap darurat keamanan informasi instansi Pemerintah, GovCSIRT mempunyai tanggung jawab sebagai berikut:

[1] Situs resmi GovCSIRT. 2013. http://insting.kominfo.go.id.

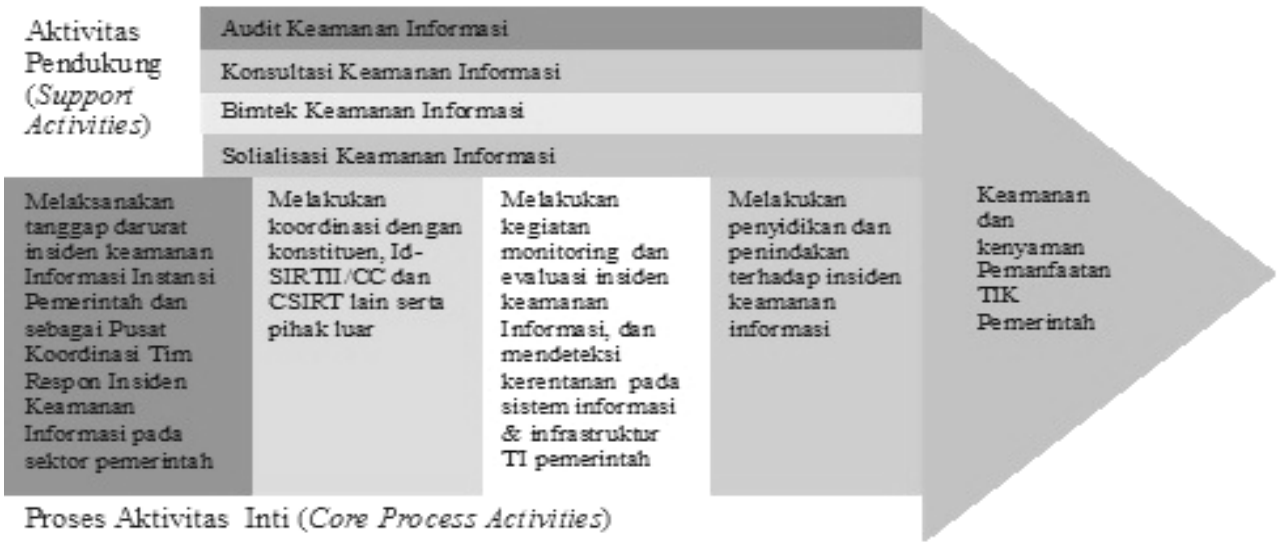
1. Memberikan layanan dan melakukan Penanganan Tanggap Darurat Keamanan Informasi Instansi Pemerintah (GovCSIRT).
2. Menyusun prosedur, standar operasional dan kebijakan untuk analisis, dan evaluasi serta monitoring terhadap insiden keamanan informasi di instansi pemerintah.
3. Melakukan analisis data hasil Pusat Monitoring dan Penanganan Tanggap Darurat Keamanan Informasi Instansi Pemerintah (GovCSIRT).
4. Menyusun rencana kerja dan jadwal pelaksanaan untuk pelaksanaan analisis, dan evaluasi serta monitoring terhadap insiden keamanan informasi di instansi pemerintah.
5. Mengumpulkan bahan yang berkaitan dengan Pusat Monitoring dan Penanganan Tanggap Darurat Keamanan Informasi Instansi Pemerintah (GovCSIRT).
6. Melakukan konsinyering/Rapat dengan satuan kerja terkait untuk membahas materi-materi Pusat Monitoring dan Penanganan Tanggap Darurat Keamanan Informasi Instansi Pemerintah (GovCSIRT).

Analisa *Value Chain* merupakan suatu metode untuk merinci suatu rangkaian dari bahan baku hingga produk akhir yang digunakan, menjadi kegiatan strategi yang relevan untuk memahami perilaku biaya dan perbedaan sumber daya. Analisa *Value Chain* pada GovCSIRT dapat dilihat pada Gambar 4.

b. Analisis *Critical Success Factor* (CSF)

Analisis *CSF* dapat ditentukan jika objektif organisasi telah diidentifikasi. Tujuan dari *CSF* adalah menginterpretasikan objektif secara lebih jelas untuk menentukan aktivitas yang harus dilakukan dan informasi apa yang dibutuhkan (Wedhasmara, 2009). Faktor penentu keberhasilan (CSF) adalah istilah untuk sebuah elemen yang diperlukan untuk suatu organisasi atau proyek untuk mencapai misinya. Ini merupakan faktor penting atau kegiatan yang diperlukan untuk memastikan keberhasilan sebuah perusahaan atau organisasi. Istilah ini awalnya digunakan dalam dunia analisis data, dan analisis bisnis (Rockart, 1979).

Sebagai organisasi yang baru didirikan pada tahun 2011, GovCSIRT dibebani dengan permasalahan yang sangat besar terkait



Gambar 4. Diagram Analisis *Value Chain* GovCSIRT
(Sumber: situs resmi GovCSIRT[1])

dengan keamanan informasi. GovCSIRT dituntut untuk memberikan layanan tanggap darurat insiden keamanan informasi pada instansi pemerintah. Data statistik yang dimiliki baik oleh Id-SIRTII ataupun ID-CERT menunjukkan terdapat banyak insiden yang menyerang infrastruktur TIK pemerintah. Dengan demikian, tidak mudah untuk mencapai tujuan strategis organisasi. Dibutuhkan perancangan strategi yang baik agar visi dan misi organisasi dapat dicapai dalam target waktu yang ditentukan. Analisa CSF pada bidang keamanan informasi nasional dan GovCSIRT untuk memetakan layanan bisnis yang ada sehingga diperoleh gambaran internal bisnis GovCSIRT seperti dapat dilihat pada Tabel 1.

c. Analisis SWOT

GovCSIRT merupakan salah satu domain dari Strategi Keamanan Informasi Nasional. Kebijakan di bidang keamanan informasi diampu oleh Kementerian Komunikasi dan Informatika melalui Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika. Adapun hasil analisis SWOT Keamanan Informasi Nasional ditunjukkan oleh Tabel 2.

Tabel 1. Analisis CSF Keamanan Informasi Nasional, Direktorat Keamanan Informasi

Fungsi	CSF	Prime Measures
• Perumusan kebijakan, norma dan standar serta pelaksanaan di bidang strategi dan kerja sama keamanan informasi,	Pengambilan keputusan dan pembuatan kebijakan di bidang keamanan informasi	terlaksananya kebijakan di bidang keamanan informasi
• Penyusunan kebijakan, standar dan prosedur di bidang strategi dan kerja sama keamanan informasi;	Tata Kelola keamanan informasi	tersusunnya kebijakan di bidang strategi dan kerja sama keamanan informasi
• Penyusunan kebijakan, standar dan prosedur serta pelaksanaan kebijakan di bidang teknologi keamanan informasi;	Pengelolaan teknologi keamanan informasi	tersedianya teknologi keamanan informasi
• Penyusunan kebijakan, standar dan prosedur di bidang penanganan monitoring, evaluasi, dan tanggap darurat keamanan informasi;	Monitoring, evaluasi, dan tanggap darurat keamanan informasi	Terselenggaranya monitoring, evaluasi, dan tanggap darurat keamanan informasi
• Pelaksanaan di bidang penyidikan dan penindakan keamanan informasi;	Penyidikan dan penindakan	Terlaksananya penyidikan dan penindakan di bidang keamanan informasi
• penyelenggaraan bimbingan teknis di bidang budaya keamanan informasi;	Pembentukan budaya dan promosi keamanan informasi	Tersosialisasinya budaya dan promosi keamanan informasi

Sumber: Direktorat Jenderal APTIKA(2010)

Tabel 2. Analisis SWOT Bidang Keamanan Informasi Nasional

Kekuatan (*Strength*)	**Kelemahan (*Weakness*)**
1. Komitmen dan dukungan Pimpinan dalam hal Keamanan Informasi 2. Tersedianya Peraturan Perundangan di bidang Transaksi Elektronik (UU ITE) 3. Inpres No.3 Tahun 2003 Tentang penyelenggaraan *e-government* di Indonesia 4. Surat Edaran No. 05/SE/M.KOMINFO/07/2011 Tentang Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik 5. Surat Edaran Menteri Kominfo No.: 01/SE/M.KOMINFO/02/2011 tentang Penyelenggaraan Sistem Elektronik Untuk Pelayanan Publik 6. Peraturan Pemerintah RI No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem Transaksi Elektronik	1. Masih rendahnya tingkat pengetahuan pegawai negeri sipil tentang keamanan informasi 2. Regulasi bidang keamanan informasi yang dihasilkan pemerintah belum maksimal 3. Banyak penyedia layanan informasi di instansi pemerintah yang masih rentan terhadap serangan 4. Belum tersedianya standar layanan dan aplikasi untuk manajemen resiko keamanan informasi pemerintah. 5. Budaya sangat terbuka dengan informasi dan rendahnya kesadaran (*awareness*) pegawai akan keamanan informasi 6. Kesiapan keamanan informasi pada instansi pemerintah pusat dan daerah sangat beragam.
Peluang (*Opportunity*)	**Ancaman (*Threat*)**
1. Pesatnya perkembangan teknologi keamanan informasi. 2. Adanya SNI 7512:2008 tentang Pengelolaan insiden keamanan informasi yang diadopsi dari ISO/IEC TR 18044:2004, *Information Security Incident Management* dan Adanya Standar ISO/IEC 27001: *Information Security Management System* 3. Adanya Kerja sama berupa koordinasi dengan multipihak untuk permasalahan keamanan informasi	1. Meningkatnya insiden serangan keamanan informasi terhadap infrastruktur milik Pemerintah 2. Kehilangan aset informasi pemerintah yang bernilai oleh karena bocornya informasi penting yang bersifat rahasia 3. Dampak pada terganggunya pelayanan publik yang berbasis elektronik. 4. Turunnya kepercayaan masyarakat terhadap pemerintah

Sumber: Direktorat Jenderal APTIKA(2010)

d. Analisis PEST

Analisis PEST merupakan alat yang penting dan banyak digunakan untuk menganalisis konstituen dengan tujuan untuk memahami situasi politik, ekonomi, sosial budaya dan teknologi dari lingkungan dimana GovCSIRT beroperasi. Hal ini akan membantu untuk menentukan apakah perencanaan masih selaras dengan lingkungan dan mungkin membantu untuk menghindari tindakan yang diambil keluar dari asumsi yang salah. Adapun hasil analisis PEST GovCSIRT dapat dilihat pada Tabel 3.

Implementasi Perencanaan Strategis Kelembagaan Pusat Respon insiden Keamanan Informasi Pemerintah

Kelembagaan Pusat Respon insiden Keamanan Informasi atau Tim Respon Insiden Keamanan Informasi Pemerintah berdasarkan

Tabel 3. Analisis PEST Gov CSIRT

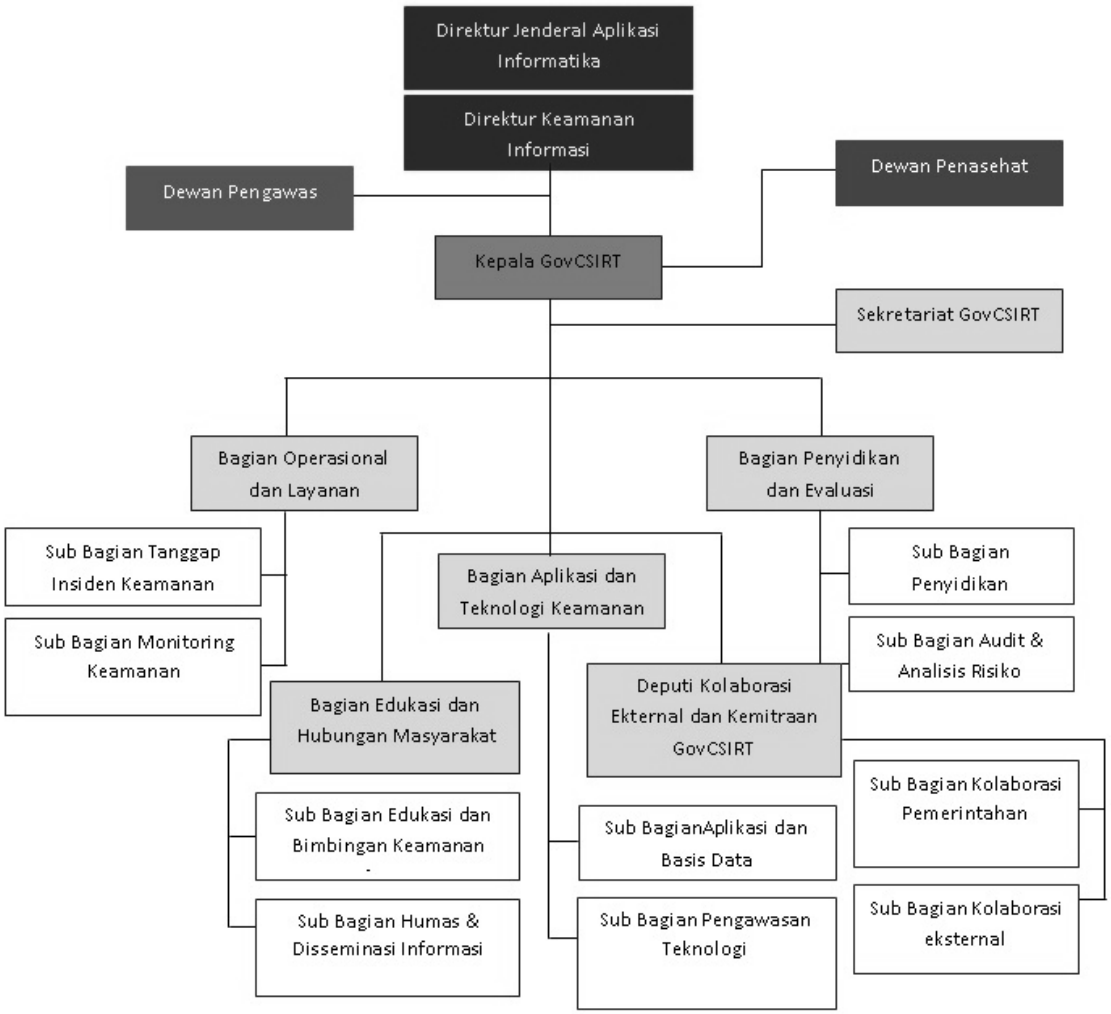
Politik	Ekonomi
1. Pengaruh politik mempunyai dampak yang besar dalam pemanfaatan TIK di Indonesia, dalam hal ini untuk implementasi e-government 2. Pemerintah telah menetapkan Peraturan Perundangan di bidang Transaksi Elektronik, yaitu UU ITE 3. Pemerintah juga telah mengeluarkan Surat Edaran No. 05/SE/M.KOMINFO/07/2011 Tentang Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik	1. Berdasarkan data yang dimilki oleh Direktorat e-Business, Direktorat Jenderal Aplikasi Informatika, transaksi pada pasar *e-commerce* Indonesia hingga tahun 2012 sudah mencapai sekitar Rp. 37 Triliun 2. Potensi besar internet untuk sektor ekonomi juga berpotensi mendatangkan dampak yang besar terjadinya kerugian yang dikarenakan adanya insiden/serangan keamanan informasi 3. Banyaknya investor asing yang tertarik untuk berinvestasi dalam bidang TI di Indonesia
Sosial	**Teknologi**
1. Pemanfaatan media jejaring sosial, seperti: seperti facebook, twitter dan BBM di Indonesia semakin meningkat. Di sisi lain, budaya masyarakat Indonesia yang sangat terbuka terhadap Informasi berdampak pada penyebarluasan Informasi berharga melalui situs jejaring sosial tanpa disadari 2. Pemerintah Indonesia melalui Direktorat Keamanan Informasi sedang menggalakkan budaya keamanan informasi terutama kepada instansi Pemerintah	1. Dalam rangka penerapan e-government, pemerintah mengupayakan adanya layanan terintegrasi 2. Tren teknologi jaringan komputerisasi pemerintah menuju tren teknologi komputasi awan (*cloud computing*) untuk mengefisiensikan investasi di bidang TIK 3. Pemerintah Indonesia saat ini sedang aktif menggalakkan pemanfaatan Sistem Operasi dan aplikasi *Open source* melalui *Indonesia Go Open source*

Surat Keputusan Direktorat Jenderal Aplikasi Informatika No. : 01/SK/DJAI/KOMINFO/01/2012, berinduk pada Direktorat Keamanan informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Kominfo. Saat ini, fungsi tim respon keamanan informasi pemerintah masih menyatu pada masing-masing Sub Direktorat pada Direktorat Keamanan Informasi. Tim Respon Insiden Keamanan Informasi Pemerintah rencananya akan dijadikan sebagai sebuah unit layanan tersendiri yang berada di bawah koordinasi Direktorat Keamanan Informasi, Ditjen Aplikasi Informatika, Kementerian Komunikasi dan Informatika.

Organisasi dan Koordinasi GovCSIRT

Berdasarkan beberapa alasan tersebut, maka struktur organisasi yang disarankan untuk GovCSIRT mengikuti model organisasi Id-SIRTII dan berada di bawah koordinasi Id-SIRTII yang merupakan *Coordinating Center* CSIRT di Indonesia. GovCSIRT merupakan CSIRT sektoral di bidang Pemerintahan. Adapun GovCSIRT akan mengoordinasi tum-

buhnya CSIRT subsektor di seluruh Indonesia. Gambar 5 adalah bagan GovCSIRT yang diusulkan:



Gambar 5. Bagan Organisasi GovCSIRT yang diusulkan

Pada struktur yang disarankan tersebut, dapat dijelaskan bahwa otoritas tertinggi sebagai penanggung jawab kinerja kerja GovCSIRT di Indonesia dipegang oleh Direktur Jenderal Aplikasi Informatika yang dilimpahkan secara langsung kepada Direktur Keamanan Informasi. Sebagai penanggung jawab implementasi sehari-hari ditunjuklah pimpinan GovCSIRT yaitu Ketua Pelaksana GovCSIRT. GovCSIRT akan berkoordinasi dengan konstituennya, yaitu pengelola TI dan keamanan TI pada seluruh instansi Pemerintah. Setiap bagian pada GovCSIRT juga akan bersinergi dengan masing-masing Sub Direktorat yang ada pada Direktorat Keamanan Informasi.

Strategi Implementasi GovCSIRT

Kegiatan pada tahapan implementasi merupakan kegiatan penerapan rencana yang telah disusun pada kegiatan pra-operasi/ perencanaan. Aktivitas pada tahapan tersebut antara lain:

- Membangun basis data kontak.
  Basis data kontak diperlukan CSIRT Nasional beserta para pemangku kepentingan untuk berkoordinasi. Database kontak memuat data nama, nomor telepon PSTN, faksimile, *e-mail*, nomor telepon seluler, dari para pemangku kepentingan CSIRT

Nasional. Strategi membangun basis data kontak bagi GovCSIRT dapat dilakukan melalui forum *e-Government*, dimana anggota forum tersebut adalah para pengelola TIK di lingkungan instansi Pemerintah baik Kementerian, Pemerintah Pusat maupun Pemerintah Daerah. Strategi ini dilakukan melalui sosialisasi-sosialisasi yang dilakukan dengan melibatkan forum tersebut.

- Menerapkan aplikasi Insiden Trouble Ticket.
  GovCSIRT memberlakukan aplikasi *trouble ticket* sebagai formulir aduan insiden keamanan informasi untuk dilakukan tindakan respon insiden. Aplikasi tersebut merupakan inti dari aplikasi *e-aduan keamanan informasi* sebagaimana yang dibahas dalam perencanaan sistem informasi GovCSIRT. Aplikasi tersebut berbentuk form isian yang digunakan konstituen untuk melaporkan insiden yang terjadi kepada GovCSIRT. CSIRT harus berhati-hati dalam memberikan bantuan melalui laporan yang tidak layak (Grance et al., 2004).

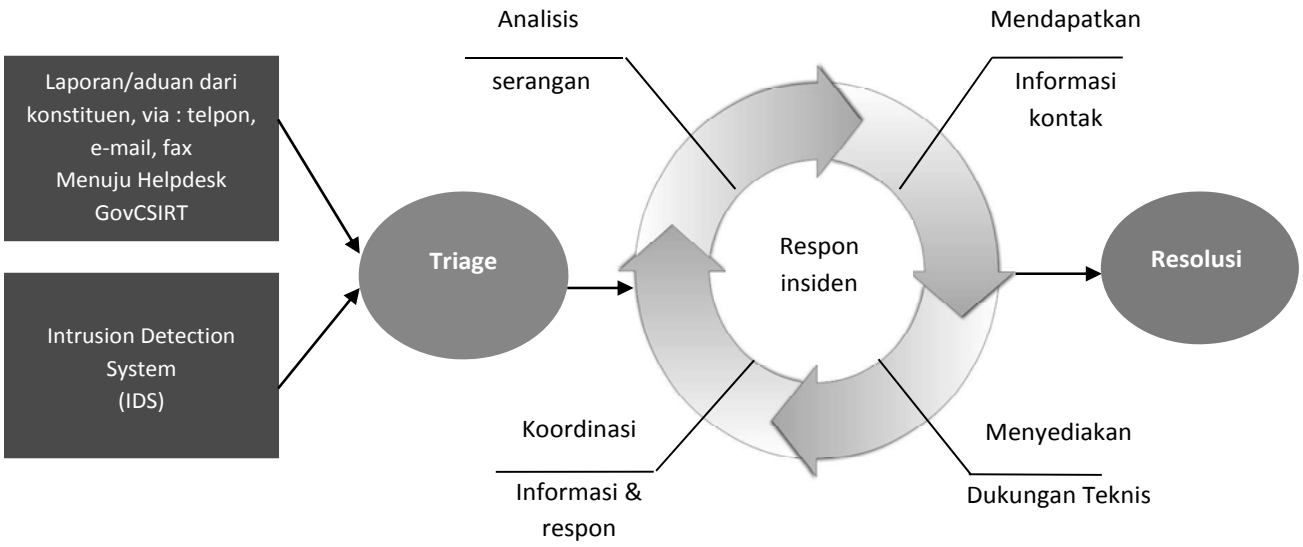
Strategi Operasional GovCSIRT

Pada tahapan operasional, layanan dasar yang harus disediakan oleh GovCSIRT didefinisikan. Berdasarkan hasil tersebut, rincian operasional disusun dan ditingkatkan. Beberapa aktivitas pada tahapan ini di antaranya:

1. Mendefinisikan operasi rutin dan kegiatan berkala.

Operasi Rutin merupakan aktifitas rutin yang dijalankan sebuah CSIRT Nasional, seperti *Incident Handling* dan penerbitan *Security Advisories*. Sedangkan Operasi Berkala adalah sejumlah aktifitas yang dilakukan pada kurun waktu tertentu. Respon insiden adalah operasi rutin yang dijalankan oleh GovCSIRT. GovCSIRT akan menangani insiden dengan memanfaatkan aplikasi *trouble ticket* insiden. Berdasarkan laporan yang masuk, GovCSIRT akan menyusun laporan statistik insiden yang dipublikasikan. Alur respon insiden keamanan informasi yang lebih rinci dijelaskan pada Gambar 6.

Penanganan insiden dimulai dari laporan yang berasal dari konstituen atau dari CSIRT lainnya. Laporan insiden juga dapat berasal dari deteksi IDS (*Intrusion Detection System*). Kemudian dilakukan triase *(triage*), yaitu mengklasifikasikan insiden serangan



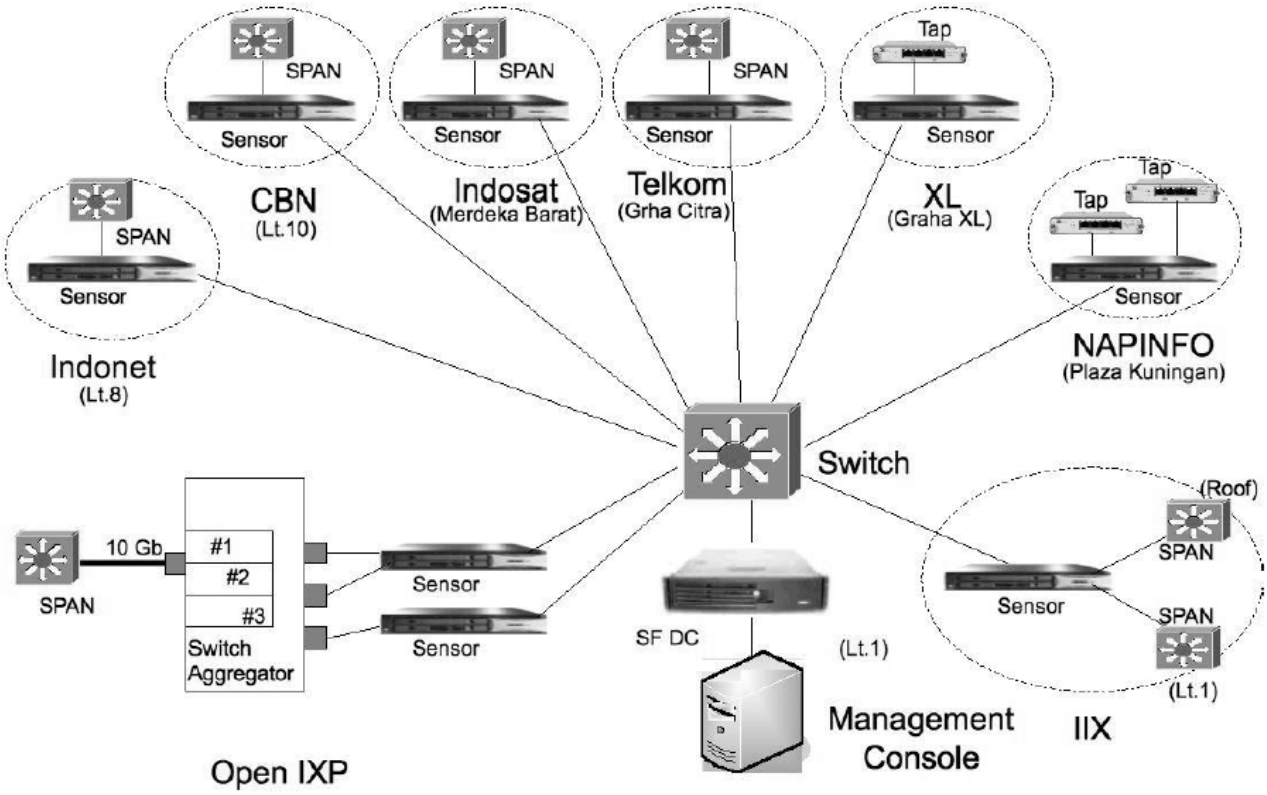
Gambar 6. Alur respon insiden keamanan informasi GovCSIRT
(Sumber: West-Brown et.al., (2003)

yang terjadi. Berdasarkan tahapan tersebut, didapatkan informasi mengenai jenis serangan, asal serangan dan kualifikasi serangan. Tahapan berikutnya adalah siklus respon insiden, yang terdiri dari analisa serangan, mencari informasi kontak pada basis data kontak untuk menghubungi sumber serangan, melakukan bantuan teknis dan mengkoordinasikan respon insiden ke pihak yang terkait hingga kemudian menghasilkan resolusi dan membuat laporan mengenai seluruh tahapan tersebut.

2. Monitoring Aktivitas Internet.

Proses pemantauan (*monitoring*) aktivitas Internet dilaksanakan dengan cara penempatan sejumlah perangkat sensor pada *gateway* utama NAP (*Network Access Provider*), terutama infrastruktur kritis. Perangkat sensor difungsikan secara pasif, tidak digunakan untuk melakukan tindakan preventif maupun defensif yang bersifat intervensi terhadap jaringan NAP. Sensor akan dihubungkan secara tidak langsung ke jaringan NAP melalui perangkat *mirror*, tidak secara *inline*. Sehingga, topologi ini akan menghilangkan resiko *down time* pada saat instalasi maupun karena kerusakan. Sensor juga dipasang di *Internet Exchange*. Skema instalasi monitoring jaringan dijelaskan pada Gambar 7.

Penempatan perangkat sensor bukanlah bentuk dari *lawful interception* melainkan sebagai bagian dari sistem deteksi dini (*Early Warning System*) nasional terhadap kemungkinan terjadinya penyebaran *worm*, trojan, virus maupun dikenalinya sejumlah kerawanan pada aplikasi dan layanan yang saat itu sedang berlangsung di dalam jaringan dan kemungkinan terjadinya ancaman, gangguan dan serangan terhadap infrastruktur Internet sehingga insiden dapat diantisipasi sejak dari awal. Nantinya NAP juga akan diberikan akses *Dashboard Management Console* yang dapat diakses juga pada aplikasi *monitoring* sehingga dapat berperan serta memantau jaringannya sendiri. Metode monitoring ini telah dilakukan

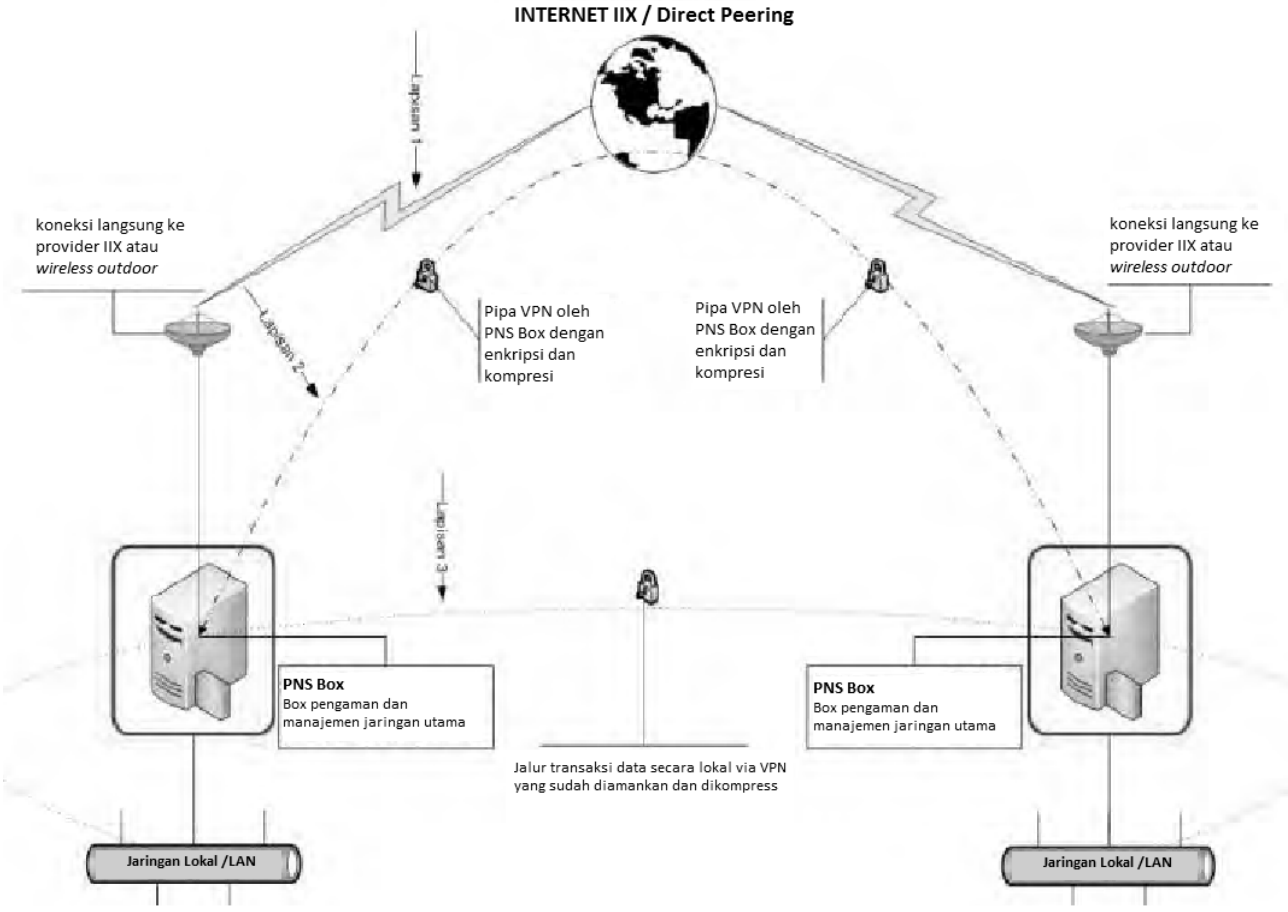


Gambar 7. Instalasi Monitoring Aktivitas Internet.
(sumber: Id-SIRTII/CC,2009)

oleh Id-SIRTII/CC dengan kekuatan hukum, yaitu Peraturan Menteri Kominfo No.: 27/PER/M.KOMINFO/9/2006 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Strategi monitoring GovCSIRT adalah dengan memanfaatkan PNS Box. Aplikasi PNS Box diinstalasikan pada server *cloud computing e-Govenrmnet* yang dipantau terus oleh GovCSIRT untuk melakukan monitoring dan deteksi keamanan informasi. Sementara untuk koordinasi dengan Id-SIRTII/CC untuk berkolaborasi mengenai data monitoring aktifitas internet yang dilakukan oleh Id-SIRTII/CC dapat dilakukan melalui *sharing* data (berbagi data) antara GovCSIRT dan Id-SIRTII/CC. *Dashboard Management Console* pada system Id-SIRTII/CC dapat diakses juga oleh GovCSIRT secara *share* dengan memanfaatkan ASP *Inter Government*. Skema kerja PNS Box dijelaskan pada Gambar 8.

Melalui sensor yang ada dapat diperoleh seluruh data yang diinginkan untuk dianalisa karakteristik dan polanya (Indrajit, 2011). Perangkat sensor *Intrusion Detection System* (IDS) pada PNS Box merupakan bagian dari sistem deteksi dini (*Early Warning System*) terhadap sejumlah kerawanan pada aplikasi dan layanan Pemerintah yang terkoneksi dalam sistem komputasi awan (*Cloud Computing*) atau *cloud government* Pemerintahan dan juga kemungkinan terjadinya penyebaran *worm*, trojan, virus pada sistem yang saat itu sedang berlangsung di dalam jaringan serta kemungkinan terjadinya ancaman, gangguan dan serangan terhadap infrastruktur Internet sehingga insiden dapat diantisipasi sejak dari awal.



Gambar 8. Implementasi PNS Box
(Sumber: Direktorat e-Government, Ditjen APTIKA, 2012)

3. Pembaharuan *Database* Kontak.

Untuk menjaga agar database kontak tetap akurat, perlu dilakukan pemeliharaan dan pembaruan. *Update database* kontak perlu dilakukan minimal sekali dalam setahun. *Update* dilakukan dengan memverifikasi kontak lama, penambahan kontak baru dan penghapusan kontak yang sudah kedaluwarsa.

4. *National Security Survey.*

Annual National Security Survey atau survei tahunan tentang Keamanan Informasi tingkat nasional perlu dilakukan untuk mengetahui jenis dan layanan pengamanan informasi apa saja yang perlu ditingkatkan oleh CSIRT Nasional pada tahun-tahun berikutnya serta mengetahui tren keamanan maupun insiden *cyber* apa saja yang tengah terjadi. Dengan adanya *National Security Survey* ini, diharapkan dapat menjadi tolok ukur kematangan negara dalam menangani masalah keamanan informasi.

5. *National Security Drill.*

National Security Drill merupakan simulasi insiden siber dimana terdapat skenario-skenario yang dibuat dan disimulasikan dengan melibatkan *stakeholder* yang ada. *National security drill* perlu dilakukan guna mengetahui layanan apa saja yang perlu ditingkatkan serta apa saja kelemahan yang ada. Simulasi ini dilaksanakan minimal sekali dalam setahun.

6. Berbagi *Database* Kontak.

CSIRT Nasional selain membangun *database* kontak, juga perlu tukar-menukar *database* kontak yang ada dengan CSIRT lain di Indonesia. *Sharing* ini akan sangat membantu tim CERT lain yang baru mulai beroperasi. Tentunya perlu dilakukan pemilahan data mana saja yang bisa dibagi dan data mana yang tidak perlu dibagi.

7. *Penetration Test.*

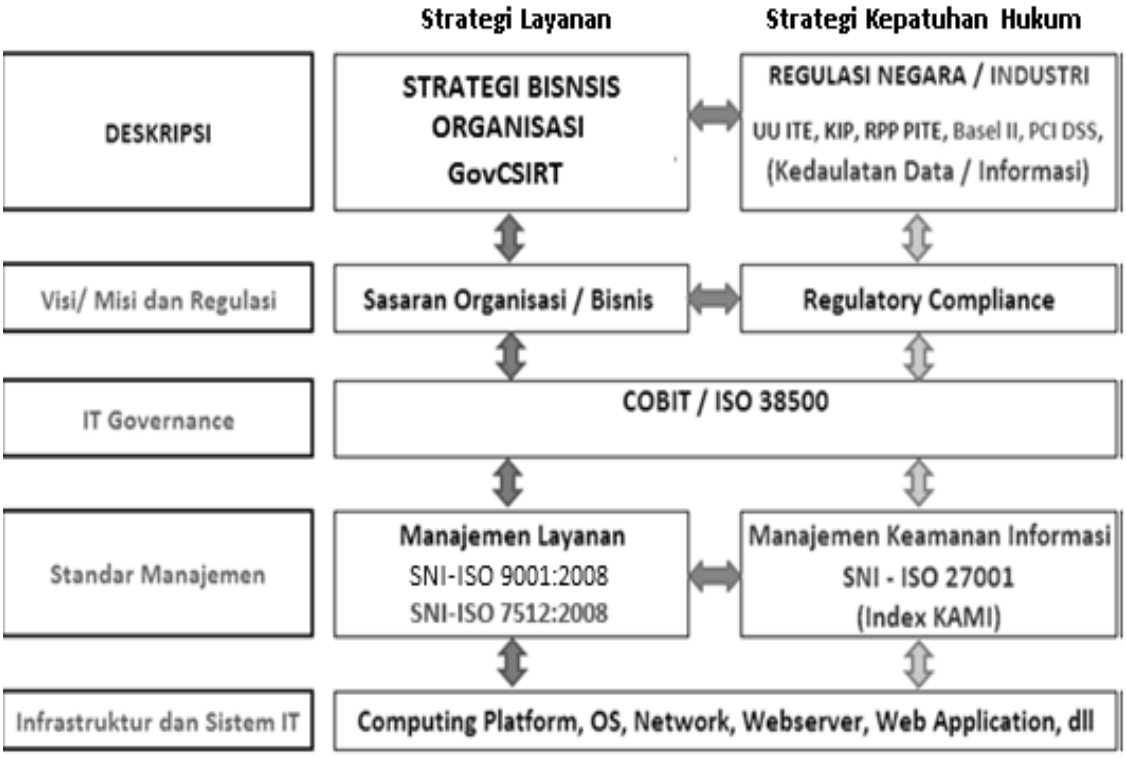
Penetration test atau dikenal juga dengan pentest adalah sebuah metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan menyimulasikan serangan dari luar berbahaya (yang tidak memiliki sarana berwenang mengakses sistem organisasi) dan dalam berbahaya (yang memiliki beberapa tingkat berwenang akses). Proses ini melibatkan analisis aktif pada sistem untuk setiap kerentanan potensial yang didapat dari hasil konfigurasi sistem yang tidak benar, baik dikenal dan tidak dikenal, hardware atau software, kekurangan atau kelemahan operasional dalam proses atau penanggulangan teknis. Analisis pentest pada GovCSIRT ini dilakukan dengan melakukan penyerangan terhadap situs atau sistem informasi milik Pemerintah. Penyerangan dilakukan dari posisi penyerang potensial dan dapat melibatkan eksploitasi aktif dari kerentanan keamanan situs milik Pemerintah.

8. Mendefinisikan kualitas.

GovCSIRT dituntut untuk memiliki strategi manajemen pelayanan yang prima untuk seluruh konstituennya. Peningkatan mutu layanan merupakan tantangan yang harus dilakukan oleh manajemen GovCSIRT. Profesionalisme dalam memberikan layanan kepada konstituen merupakan hal utama yang harus dipenuhi dimana salah satunya adalah tingkat *availability* layanan e-Pengaduan GovCSIRT yang tinggi. Tingginya tingkat *availability* layanan merupakan hal pokok / utama dari perwujudan proses usaha govCSIRT untuk memuaskan kebutuhan dan harapan konstituen.

Dalam hal peningkatan mutu layanan GovCSIRT dan terkait dengan penerapan tata kelola TIK, berdasarkan kerangka kerja yang dijelaskan pada Gambar 9, strategi yang dapat dilakukan GovCSIRT adalah sebagai berikut:

- Menerapkan standar Manajemen Mutu Layanan SNI-ISO 9001:2008 sebagai standar untuk meningkatkan standar mutu layanan GovCSIRT.



Gambar 9. Kerangka kerja strategi layanan dan kepatuhan hukum pada GovCSIRT
(Sumber: Ir. Hogan Kusnadi M.Sc dalam Puslitbang APTIKA & IKP, 2012)

- Menerapkan standar Pengelolaan insiden Keamanan Informasi SNI-ISO 7512:2008 sebagai arahan dalam melakukan aktivitas layanan.

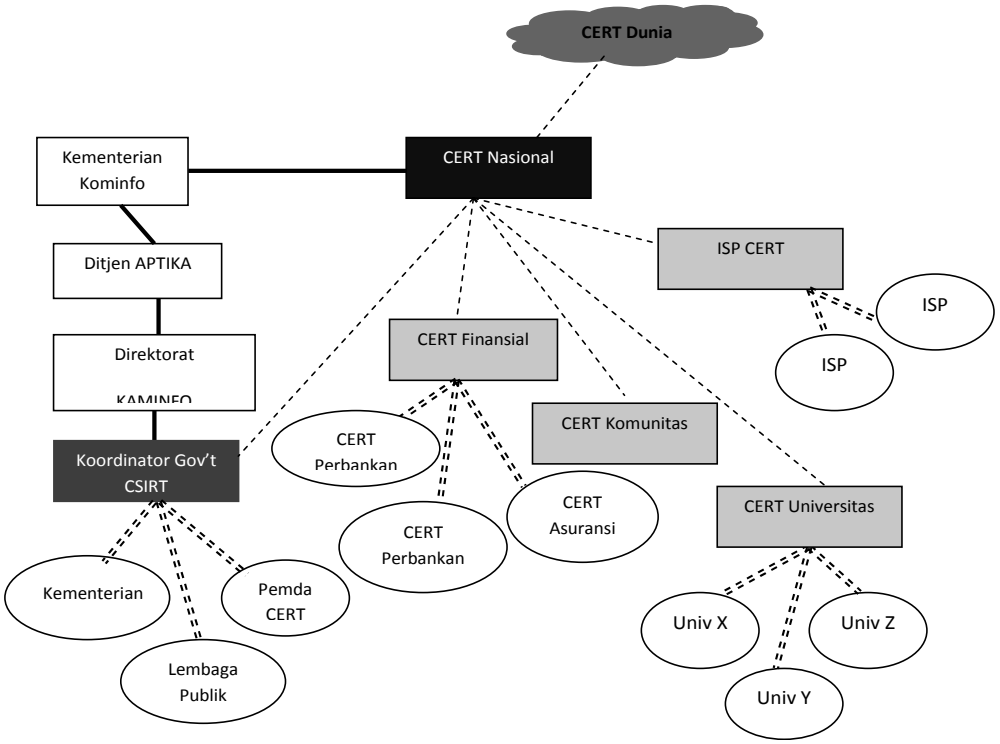
- Menerapkan standar SNI-ISO 27001 yang telah diadopsi oleh Indeks Keamanan Informasi, sebagai sebuah Standar Manajemen Keamanan Informasi yang memberikan arahan dalam menerapkan tata kelola keamanan informasi pada instansi Pelayanan Publik.

Strategi Kolaborasi GovCSIRT

Berdasarkan model para pemangku kepentingan CSIRT, maka GovCSIRT akan berkolaborasi dengan pihak-pihak yang terkait. Fungsi kolaborasi dari sebuah CSIRT merupakan sebuah fungsi yang cukup penting, dimana GovCSIRT diharapkan dapat menjembatani dan saling memperkenalkan pihak-pihak yang belum pernah berhubungan langsung sebelumnya, dengan cara yang aman dan terpercaya.

Id-SIRTII/CC merupakan *Coordination Center* atau Pusat Koordinasi seluruh CSIRT di Indonesia. Id-SIRTII menjadi *vocal point* Indonesia di dunia dalam menangani insiden keamanan informasi. Sementara itu GovCSIRT berada di bawah kewenangan Direktorat Keamanan Informasi dan menjadi koordinator bagi sektor Pemerintahan. Model kolaborasi antar CSIRT di Indonesia dijelaskan pada Gambar 10.

CSIRT/CC biasanya meminta agar setiap konstituen atau CSIRT sektoral di bawahnya untuk menginformasikan setiap aktivitas internet untuk mendapatkan seluruh informasi aktivitas dan transaksi dalam domain mereka dan memberitahukan kepada pihak lainnya untuk bersama memantau terkait dengan aktivitas tersebut dalam rangka memonitor aktivitas transaksi internet (Moira, 1999).



Gambar 10. Kolaborasi CSIRT di Indonesia
(Sumber : Puslitbang APTIKA dan IKP, 2011)

Roadmap Lima Tahun GovCSIRT

Roadmap CSIRT seperti tampak pada Tabel 4 disusun dengan batasan waktu 5 (lima) tahun, terhitung dari awal 2011 hingga akhir 2015. Idealnya setahun sekali dilakukan peninjauan kembali (*re-alignment)* terhadap

Tabel 4. *Roadmap* Lima Tahun GovCSIRT

Tahapan GovCSIRT	2011	2012	2013	2014	2015
Pra operasi					
membangun kesadaran					
Perencanaan					
Implementasi					
identifikasi situs pemerintah					
membangun db kontak					
aplikasi insiden trouble ticket					
Operasional rutin					
respon insiden					
monitoring aktivitas internet					
Operasional berkala					
update database situs Pemerintah					
update database kontak					
penetration test (pentest) berkala					
National Security Drill					
Kolaborasi					
Membangun Kolaborasi					
Pembinaan Kolaborasi					

roadmap ini. Peninjauan kembali bisa dilakukan di setiap awal tahun atau di akhir tahun dengan mempertimbangkan faktor internal yaitu pencapaian atas roadmap yang telah disusun dan faktor eksternal yaitu dinamika kondisi lingkungan.

Berdasarkan Roadmap CSIRT tersebut, dapat dijelaskan bahwa penyusunan Roadmap CSIRT disusun berdasarkan tahapan-tahapan kerangka kerja pembentukan GovCSIRT yang digunakan dalam penelitian ini.

PENUTUP

Simpulan

Berdasarkan hasil analisis dan pembahasan mengenai perencanaan strategis Pusat Respon insiden Keamanan Informasi Pemerintah yang telah dilakukan pada GovCSIRT, Direktorat Keamanan Informasi, Kementerian Kominfo, maka dapat diambil beberapa kesimpulan yaitu:

Pertama, penelitian ini memberikan usulan perencanaan strategis pembentukan Pusat Respon insiden Keamanan Informasi Pemerintah yang dinamakan GovCSIRT, meliputi perencanaan strategis sistem informasi pada organisasi tersebut sebagai solusi atas permasalahan yang dimiliki GovCSIRT, yaitu belum adanya master plan atau perencanaan strategis pembentukan organisasi GovCSIRT. Permasalahan tersebut berdampak pada belum terbentuknya struktur kelembagaan yang baku, belum tersedianya perencanaan infrastruktur SI/TI yang memadai. Dengan adanya perencanaan strategis pembentukan Tim Respon Insiden Keamanan Informasi Pemerintah dan sistem informasi yang dibangun secara terintegrasi, maka dapat mendukung kinerja GovCSIRT sebagai pengawas keamanan informasi di lingkungan instansi Pemerintah secara maksimal.

Kedua, perencanaan strategis pembentukan GovCSIRT yang saling selaras untuk mencapai tujuan strategis GovCSIRT. Dalam strategi pembentukan kelembagaan GovCSIRT, diusulkan bentuk struktur kelembagaan yang mengadopsi bentuk kelembagaan Id-SIRTII/CC yang merupakan pusat koordinasi CSIRT di Indonesia dan merujuk pada layanan yang tersedia pada GovCSIRT.

Ketiga, adanya keterbatasan sumber daya infrastruktur dan keterbatasan keahlian sumber daya manusia di GovCSIRT saat ini serta untuk mengefisienkan penggunaan dana untuk investasi perangkat yang mahal, maka perlu diterapkan strategi kolaborasi dengan Id-SIRTII/CC untuk menerapkan perencanaan strategis sistem informasi ini.

Saran

Berdasarkan uraian dan pembahasan yang telah dilakukan pada bab-bab sebelumnya, maka diberikan saran antara lain:

Pertama, GovCSIRT Direktorat Keamanan Informasi dapat memanfaatkan forum-forum instansi pemerintah seperti forum *e-Government* dan Bakohumas untuk menyosialisasikan program-program keamanan informasi nasional dan membuat koordinasi kerja dengan instansi Pemerintah baik pusat maupun daerah serta mendapatkan *database* kontak.

Kedua, keberadaan GovCSIRT perlu didukung dengan regulasi yang lebih kuat, yaitu regulasi yang dikeluarkan setara dengan peraturan atau kebijakan yang dikeluarkan oleh menteri untuk memperkuat posisi GovCSIRT di kalangan instansi pemerintah dan memudahkan koordinasi.

Ketiga, untuk memudahkan kinerja GovCSIRT, Direktorat Jenderal Aplikasi Informatika perlu mengeluarkan regulasi mengenai pembentukan tim khusus yang menangani insiden keamanan informasi pada masing-masing instansi pemerintah baik kementerian tingkat pusat maupun Pemerintahan Daerah.

Keempat, GovCSIRT perlu menyusun standar prosedur operasi yang sesuai dengan penggunaan SI/TI sehingga visi dan misi perusahaan dapat dicapai.

Kelima, perlu dirancang perencanaan infrastruktur TI yang lebih detail pada arsitektur enterprise GovCSIRT terutama untuk mengantisipasi kebutuhan yang akan datang

serta mengantisipasi pertumbuhan perusahaan pada penelitian berikutnya.

DAFTAR PUSTAKA

Badan Standardisasi Nasional. SNI 7512:2008. *Teknik keamanan - Pengelolaan insiden keamanan informasi*. Indonesia: BSN, 2008.

Brownlee, N dan E. Guttman. *Expectation for Computer Security Incident Response*. Network Working Group, 1998. Diakses 18 Februari 2013. http://www.ietf.org/rfc/rfc2350.txt

Direktorat e-Government, Ditjen APTIKA. *Konsep Keamanan Informasi Untuk Jaringan Pemerintah.* Jakarta, Indonesia: Dit. E-government, Ditjen APTIKA Kominfo, 2012.

Direktorat Jenderal APTIKA, Rencana Strategis Direktorat Jenderal Aplikasi Informatika 2010-2014, Jakarta: Ditjen APTIKA, Kominfo, 2010

Cernosek, Gary & Eric Naiburg. The Value of Modeling in "*IBM whitepapers*". USA: IBM Publishing, 2004.

Grance, T., K. Kent, & B. Kim. *Computer Security Incident Handling.* Gaithersburg, USA: NIST Special Publication, 2004.

Id-SIRTII. *Implementasi Teknis Id-SIRTII untuk monitoring Jaringan Internet.* Jakarta, Indonesia: Id-SIRTII, 2009.

Indrajit, Richardus Eko. "Tim Pengawas Keamanan Internet" dalam Manajemen Keamanan Informasi dan Internet di edit oleh Tim Direktorat Keamanan Informasi, Ditjen APTIKA Kemkominfo. Jakarta: Penerbit Informatika dan Kemkominfo, 2011.

ISO/IEC 27001. Information Technology-Security-Technique-Information Security Management Standard. Geneva, Switzerland: ISO/IEC Publisher, 2005.

Moira, W. "International Infrastructure for Global Security Incident Response". *CMU conference*, *Carnegie Mellon University* (1999). Diakses 19 Februari 2013. http://www.first.org/conference/1999/ACDA-WP-GSIR.pdf

Porter, M. E. *Competitive Advantage.* New York, USA: The Free Press, 1998.

Puslitbang APTIKA&IKP. *Studi Kelembagaan CERT Nasional.* Jakarta: Balitbang SDM, 2011.

Puslitbang APTIKA & IKP. Kajian Kesiapan Keamanan Informasi Pemerintah. Jakarta: Balitbang SDM, 2012

Rockart, John F., "Chief executives define their own data needs", *Harvard Business Review,* 1979 (2), pages 81-93

Situs Resmi GovCSIRT. "Pusat Monitoring dan Penanganan Insiden Keamamanan Informasi Instansi Pemerintah". Diakses 15 Januari 2013. http://insting.kominfo.go.id

Smith, Danny. *Forming an Incident Response Team*. Queensland University, Brisbane, Autralia: Prentice Center, 1994

UN-APICICT/ESCAP. *Information Security and Privacy – Academy of ICT Essentials for Government Leader 2nd Edition*. Incheon City, Korea: KISA, UN-APCICT/ESCAP, 2011.

Wedhasmara, A. Lngkah-Langkah Perencanaan Strategis Sistem Informasi Dengan Metode Ward and Peppard. *Jurnal Sistem Informasi,* 2009.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Kilcrece, G., Ruefle, R., & Zajicek, M. *Handbook for Computer security Incident Response Teams (CSIRTs).* Pittsburgh, USA: Carnegie Mellon University Publisher, 2003