PERENCANAAN STRATEGIS SISTEM INFORMASI PADA PUSAT PENANGANAN INSIDEN KEAMANAN INFORMASI SEKTOR PEMERINTAH

INFORMATION SYSTEM STRATEGIC PLANNING ON THE CENTER OF INFORMATION SECURITY INCIDENT HANDLING FOR GOVERNMENT SECTOR

Ahmad Budi Setiawan

Puslitbang APTIKA & IKP, Badan Litbang SDM. Kementerian Kominfo.
Jl. Medan Merdeka Barat No. 9 Jakarta 10110. Telp./Fax.: 021-3800418
e-mail: ahma003@kominfo.go.id

Naskah diterima tanggal 20 Maret 2014, direvisi tanggal 28 Mei 2014, disetujui pada tanggal 9 Juni 2014

Abstract

Information security incident is a form of attack on the security of information that can occur in all sectors. The government sector is one of the targets of information security incidents. Central Government Information Security Incident Handling was established with the aim to address all forms of attacks on information security in government sector. The sustainability Central of Government Information Security Incident Handling (GovCSIRT) needs to be supported with information system infrastructure that's sophisticated and sufficiently. This research aims to create an information system strategic planning at the Center for Government Information Security Incident Handling. Implementation of Information Systems in an organization must adapt to the vision, mission, goals and needs of the organization. Therefore, the Information Systems Strategic Planning at the Government Information Security Management Center must be performed using appropriate methodologies. There are a wide variety of methodologies in information systems Strategic Planning. This study used a Cassidy methodology which is developed by Annita Cassidy. These results are used as input in the development of infrastructure or basic Information Systems Security Management Center Information Government to realize the use of ICT in a safe and convenient administration. The results of this research is used as input or recommendation in the development of the Government Information Security Incident Response Center to actualize the use of ICT in government that is safe and comfortable.

Keywords : *Strategic Planning for Information System; Government CSIRT; Cassidy's Framework*

Abstrak

Insiden keamanan informasi merupakan bentuk serangan terhadap keamanan informasi yang dapat terjadi pada seluruh sektor. Sektor Pemerintah merupakan salah satu target insiden keamanan informasi. Pusat Penanganan Insiden Keamanan Informasi Pemerintah didirikan dengan tujuan untuk menangani segala bentuk serangan terhadap keamanan informasi pada sektor Pemerintah. Keberlangsungan Pusat Penanganan Insiden Keamanan Informasi Pemerintah perlu ditunjang oleh infrastruktur Sistem Informasi yang mutakhir dan memadai. Penelitian ini bertujuan untuk membuat sebuah perencanaan strategis sistem informasi pada Pusat Penanganan Insiden Keamanan Informasi Pemerintah. Implementasi Sistem Informasi pada sebuah organisasi harus menyesuaikan dengan visi, misi, tujuan dan kebutuhan organisasi tersebut. Oleh karena itu, Perencanaan Strategis Sistem Informasi pada Pusat Penanganan Keamanan Informasi Pemerintah harus dilakukan dengan menggunakan metodologi yang tepat. Terdapat berbagai macam metodologi dalam Perencanaan Strategis sistem Informasi. Dalam penelitian untuk perencanaan strategis ini, metodologi Cassidy yang digunakan dikembangkan oleh Annita Cassidy. Hasil penelitian ini digunakan sebagai masukan atau dasar dalam pengembangan infastruktur Sistem Informasi Pusat Penanganan Keamanan Informasi Pemerintah untuk mewujudkan penggunaan TIK dalam pemerintahan yang aman dan nyaman.

Kata Kunci: Perencanaan Strategis Sistem Informasi; Pusat Penanganan Insiden Keamanan Informasi; Kerangka Kerja Cassidy

PENDAHULUAN

Latar Belakang

Sektor Pemerintah memiliki banyak sekali aset Informasi strategis yang menyangkut stabilitas dan kedaulatan Bangsa. Seiring dengan pesatnya penggunaan TIK di kalangan instansi pemerintah dan diimplementasikannya tata kelola pemerintah berbasis elektronik (*e-goverment*), seluruh aset informasi tersebut dikelola secara elektronik. Implementasi TIK pada sektor Pemerintah memiliki berbagai kendala, salah satunya terdapat berbagai masalah keamanan informasi yang timbul dalam bentuk insiden keamanan informasi. Hal ini disebabkan banyak pihak yang tidak bertanggung jawab yang melakukan penyerangan terhadap infrastruktur TIK pemerintah dengan tujuan mencuri informasi, bahkan merusak.

Informasi merupakan aset penting yang harus dilindungi. Hasil riset - kajian kesiapan keamanan informasi (Puslitbang APTIKA&IKP, 2012), menyebutkan; 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 ditembus. Untuk mengatasi serangan keamanan pada sistem informasi tersebut, Pemerintah Indonesia telah membentuk Tim Respon Insiden Keamanan Informasi Pemerintah (*Gov-CERT*) berdasarkan Surat Keputusan Dirjen APTIKA berdasarkan SK No. 01/SK/DJAI/KOMINFO/01/2012.

Berdasarkan Surat Keputusan 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.

Pusat Penanganan Insiden Keamanan Informasi atau lebih populer dalam Bahasa Indonesia disebut dengan Tim Respon Insiden Keamanan Informasi dan secara Internasional dikenal dengan istilah CERT (*Computer Emergency Response Team*) 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, Stikvoort, Kossakowski, Kilcrece, Ruefle, & Zajicek, 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*) (Smith, 1994). 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 (Kilcrece, 2003). Setiap CSIRT didunia memiliki pola yang berbeda di satu negara dengan negara lainnya.

Keberlangsungan Pusat Penanganan Insiden Keamanan Informasi pada sektor Pemerintah membutuhkan dukungan infrastruktur Teknologi Informasi dan Komunikasi yang mutakhir dan handal. Keberadaan Pusat Penanganan Insiden Keamanan Informasi Pemerintah yang dibentuk oleh Direktorat Keamanan Informasi, Kementerian Kominfo belum bekerja secara maksimal. Kondisi ini menyebabkan insiden keamanan informasi yang menyerang infrastruktur sistem informasi pemerintah semakin meningkat. Dari sisi kelembagaan, Pusat Penanganan Insiden Keamanan Informasi Pemerintah yang telah dibentuk belum memiliki rencana strategis dan belum memiliki struktur kelembagaan yang jelas

serta belum diketahui oleh seluruh instansi Pemerintah. Di sisi lain, pengamanan infrastruktur TIK Pemerintah masih bersifat *Silo System* (berjalan masing-masing) dan belum melaksanakan tata kelola TIK dengan baik dan benar.

Permasalahan lainnya adalah minimnya infrastruktur yang dimiliki oleh Pusat Penanganan Insiden Keamanan Informasi Pemerintah dan dari sisi prosedur, belum ada standar dan prosedur baku yang diterapkan untuk menangani insiden keamanan informasi. Kedua hal tersebut menyebabkan organisasi Pusat Penanganan Insiden Keamanan Informasi Pemerintah tidak dapat bekerja secara maksimal.

Adanya permasalahan tersebut juga mengakibatkan banyaknya insiden keamanan informasi yang menyerang instansi Pemerintah tidak termonitor dengan baik, sementara itu kerentanan sistem TI pada instansi Pemerintah sudah banyak diketahui (*common vulnerability*). Keseluruhan hal tersebut disebabkan oleh karena belum adanya perencanaan strategis pada Pusat Penanganan Insiden Keamanan Informasi yang telah dibentuk oleh Direktorat Keamanan Informasi, Kementerian Kominfo.

Berdasarkan hal tersebut, maka Direktorat Keamanan Informasi harus menjalankan peran dan tanggung jawab dalam merespon dan menindaklanjuti setiap insiden keamanan informasi yang terjadi dilingkungan instansi Pemerintahan. Dengan demikian, permasalahan yang telah dijabarkan sebelumnya, maka rumusan masalah yang menjadi pertanyaan pada penelitian ini adalah, sebagai berikut:

Bagaimana perencanaan strategis Sistem Informasi Pusat Penanganan Insiden Keamanan Informasi pemerintah (GovCSIRT)?

Tujuan Penelitian

Secara garis besar tujuan penelitian ini adalah untuk membuat sebuah perencanaan strategis Organisasi Pusat Penanganan Insiden Keamanan Informasi Pemerintah yang selaras dengan visi-misi serta tujuan bisnis Kementerian Komunikasi dan Informatika, khususnya Direktorat Keamanan Informasi.

Ruang lingkup penelitian ini adalah:

1. Penelitian ini dilakukan terbatas pada ruang lingkup perencanaan strategi pembentukan tim respon insiden keamanan informasi untuk lingkungan instansi pemerintah
2. Perencanaan strategis SI/ TI dan aplikasi
3. Penelitian ini dilakukan menggunakan kerangka kerja (*framework*) Cassidy untuk implementasi sistem Informasi pada Pusat Penanganan Insiden Keamanan Informasi.

Penelitian ini mengusulkan sebuah rencana strategis untuk implementasi sistem informasi pada Pusat Penanganan Keamanan Informasi Pemerintah.

Tinjauan Pustaka

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.

Keamanan Informasi

Informasi secara umum 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, mainpulasi dan pengaturan data yang dapat ditransmisilkan (UNESCAP APCICT, 2009). Sementara definisi informasi menurut standar ISO/ IEC 27001 adalah sebuah ‘aset’ yang memiliki nilai dan harus dilindungi (Badan Standarisasi Nasional, 2008). 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

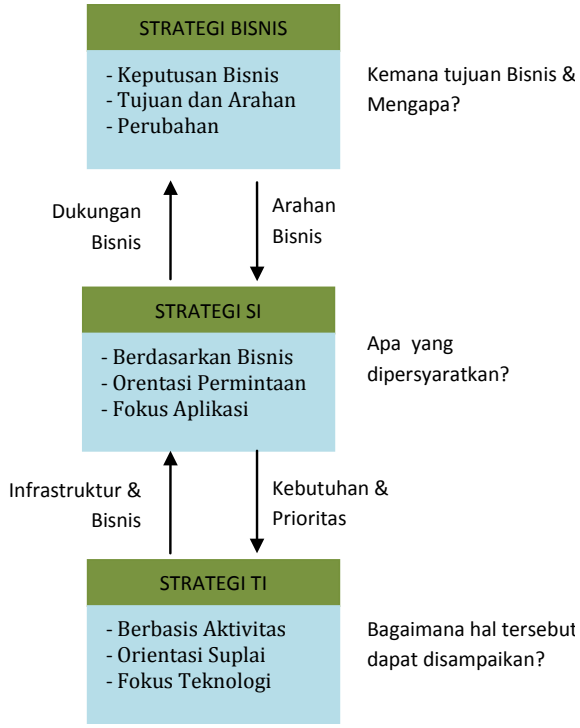
bagi Negara manapun. Keamanan informasi dapat juga disebut sebagai sebuah tindakan menghargai nilai informasi sebagai sebuah aset yang berharga dengan melindungi informasi tersebut dari berbagai ancaman.

Perencanaan Strategis Sistem Informasi

Untuk memahami perancangan strategis sistem informasi, maka harus dipahami pengertian *blue print* atau perencanaan strategis. Definisi perancangan strategis menurut kerangka konseptual Sistem Informasi Nasional (SISFONAS) adalah gambaran desain sistem informasi secara konseptual ideal yang menggambarkan desain secara komprehensif menyangkut arus informasi mulai dari pemasukan, pengolahan hingga presentasi data menjadi suatu informasi (Depertemen Komunikasi dan Informatika, 2002). Merujuk definisi tersebut, perencanaan strategis dapat juga didefinisikan sebagai kerangka kerja terperinci yang digunakan sebagai landasan dalam pembuatan kebijakan, meliputi penetapan tujuan dan sasaran, penyusunan strategi, pelaksanaan program, fokus kegiatan serta langkah-langkah atau implementasi yang harus dilaksanakan setiap unit di lingkungan kerja (Dewan TIK Nasional, 2007).

Perencanaan strategis menurut Ward and Peppard adalah proses identifikasi kebutuhan aplikasi sistem informasi berbasis komputer yang akan mendukung organisasi dalam pelaksanaan rencana bisnis dan merealisasikan tujuan bisnisnya (Wedhasmara, 2009). Dengan demikian, perencanaan strategis pembentukan tim respon insiden keamanan informasi bertujuan untuk menyelaraskan pembentukan tim respon insiden keamanan informasi pemerintah dengan visi-misi, strategi serta tujuan Kementerian Komunikasi dan Informatika, khususnya dalam membentuk tim respon insiden keamanan informasi untuk instansi pemerintah.

Untuk menentukan strategi SI/ TI yang dapat mendukung pencapaian visi dan misi organisasi, diperlukan pemahaman strategi organisasi (Lederer & Gardiner, 1992). Isu utama yang akan dibahas dalam membangun strategi organisasi adalah adanya keselarasan (*alignment)* antara strategi bisnis dengan strategi SI/ TI. Hubungan antara strategi SI/ TI dan strategi bisnis sebagaimana Gambar 1 berikut ini.



Gambar 1. Hubungan antara Strategi Bisnis, SI dan TI
(Sumber : Ward & Peppard, 2002)

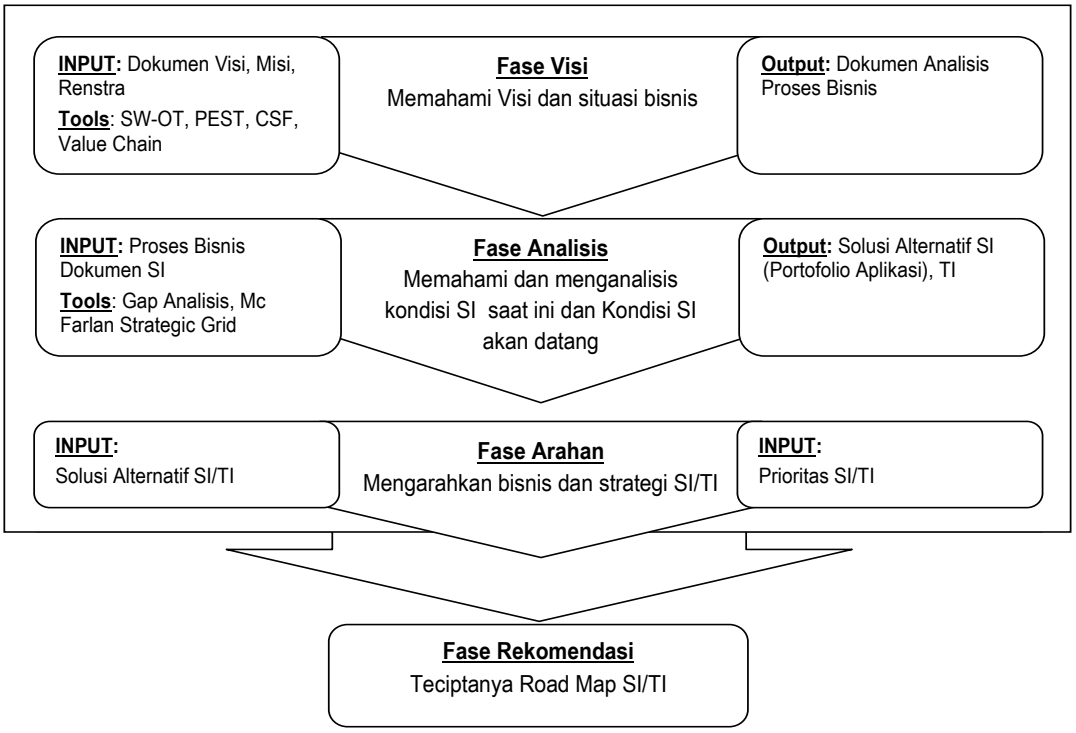
Strategi bisnis merupakan sebuah uraian dan rencana yang sistematik dari tindakan yang mengarah kepada pencapaian tujuan bisnis organisasi. Di dalamnya berisi keputusan bisnis, arah dan tujuan bisnis, serta perubahan yang harus dilakukan. Strategi SI menetapkan kebutuhan dan atau permintaan organisasi akan sistem informasi untuk mendukung keseluruhan strategi dari organisasi. Yaitu, menetapkan dan membuat prioritas investasi yang dibutuhkan untuk mendapatkan portfolio aplikasi yang ideal bagi organisasi. Strategi TI lebih menekankan pada pemilihan teknologi infrastruktur dan keahlian khusus yang dibutuhkan suatu organisasi dalam hal perangkat keras (*hardware*) seperti *server*, teknologi pengembangan aplikasi dan jaringan (Waterhouse, 1996).

Kerangka Kerja (framework) Penelitian Perencanaan Strategis Pusat Penanganan Insiden Keamanan Informasi

Setelah menganalisis beberapa teori, penelitian sebelumnya serta metodologi yang sesuai dengan topik, penulis menggunakan metodologi perencanaan strategis SI/ TI pada Pusat Penanganan Insiden Keamanan Informasi Pemerintah dengan metodologi Perencanaan Strategis SI/ TI versi *Cassidy* dalam membuat perencanaan strategis sistem informasi pada Tim Respon Insiden Keamanan Informasi. Hal ini dikarenakan tahapan pada metodologi *Cassidy* memberikan arahan yang jelas dan sistematis dalam merencanakan SI/ TI pada organisasi (Cassidy, 2006). Kerangka kerja tersebut adalah sebagai berikut :

1. Tahapan Visi
   Pada tahapan ini dilakukan identifikasi strategi bisnis organisasi baik secara internal maupun eksternal untuk mengetahui kebutuhan organisasi akan infrastruktur SI/TI.
2. Tahapan Analisis
   Pada tahapan ini dilakukan analisis kondisi SI/TI organisasi saat ini dan juga dilakukan analisis mengenai tren teknologi yang sedang berkembang. Hal ini ditujukan untuk melihat prospek pemanfaatan SI/TI agar sesuai dengan kebutuhan organisasi.
3. Tahapan Arahan
   Dalam tahapan ini, dilakukan strategi pengelolaan dan operasionalisasi serta prioritasi untuk menentukan pemanfaatan SI/TI yang sesuai dengan kebutuhan organisasi.
4. Tahapan Rekomendasi
   Dalam tahapan ini ditentukan peta jalan (*Road map*) perencanaan SI/TI pada organisasi berdasarkan masukan dan hasil analisis pada tahapan sebelumnya.

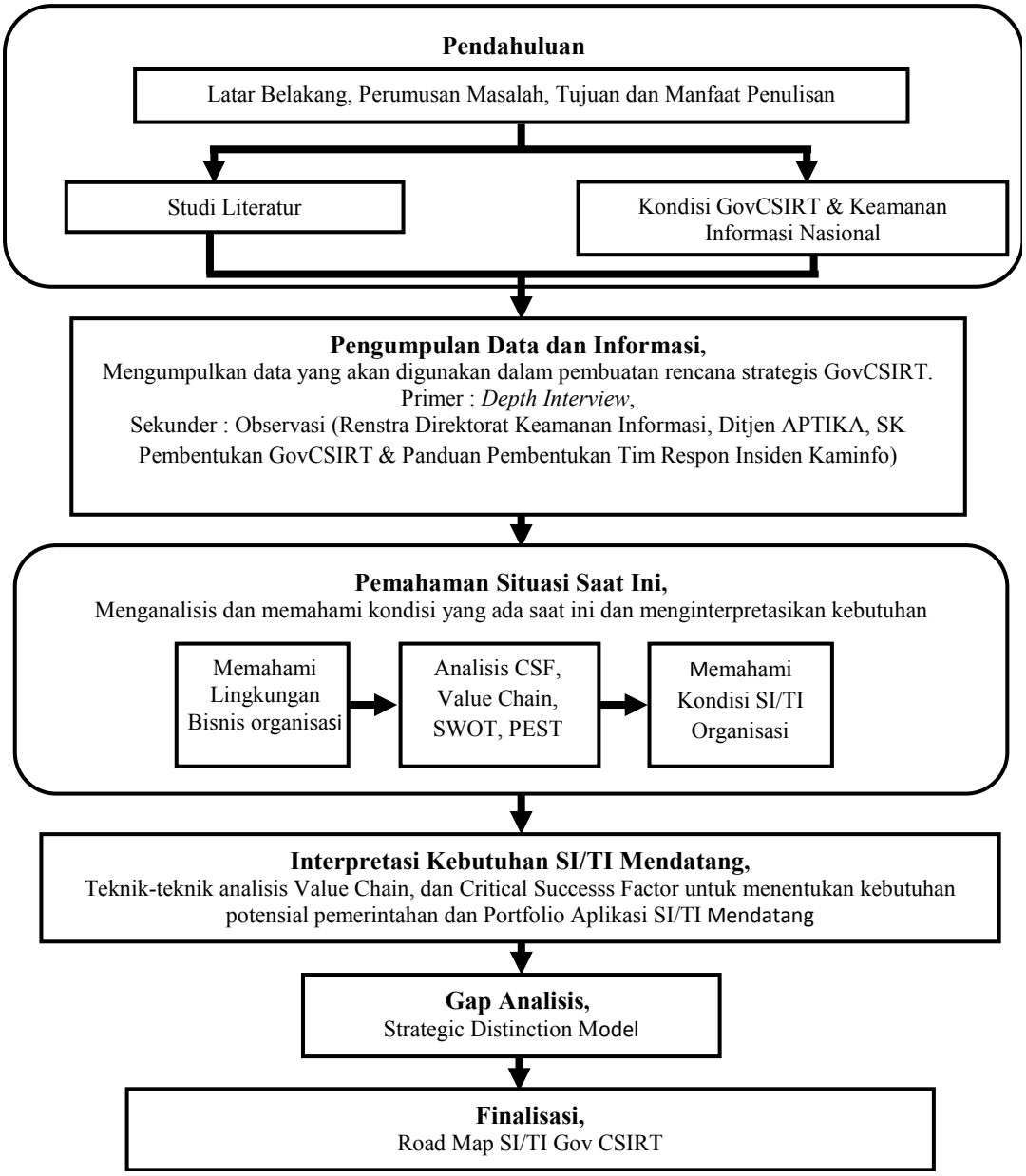
Adapun penjelasan tahapan kerangka penelitian (*Theoretical Framework*) Perencanaan Strategis Sistem Informasi Pusat Penanganan Insiden Keamanan Informasi Pemerintah dijelaskan pada Gambar 2 berikut ini:



Gambar 2. *Framework* Perencanaan Strategis SI/TI pada Pusat Penanganan Insiden Keamanan Informasi Pemerintah

Metode Penelitian

Untuk membahas permasalahan dalam penelitian ini digunakan metodologi yang diturunkan dari kerangka kerja Cassidy untuk implementasi sistem informasi pada Pusat Penanganan Insiden Keamanan Informasi yang disesuaikan dengan karakteristik dan kebutuhan organisasi. Metode yang digunakan dalam penelitian ini adalah metode peneltian kualitatif. Adapun tahapan/ alur metodologi penelitian yang dilakukan, dijelaskan pada Gambar 3. berikut ini:



Gambar 3. Alur Metodologi Penelitian

Analisis dan interpretasi data menggunakan metode analisis kualitatif. Metode analisis ini menggunakan pendekatan logika induktif, di mana 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 mensintesisnya. Kemudian berdasarkan proses tersebut, ditemukan apa yang penting dan apa yang dapat dipelajari untuk menunjang keputusan. Dalam hal analisis, pada penelitian ini digunakan unit analisis *supply chain*, SWOT, dan CSF.

HASIL DAN PEMBAHASAN

Perencanaan strategis pembentukan pusat penanganan insiden keamanan informasi pemerintah dimulai dari tahapan analisis dan dilanjutkan dengan tahapan implementasi rencana strategis.

Analisis Perencanaan Strategis Pembentukan Pusat Penanganan Insiden Keamanan Informasi Pemerintah

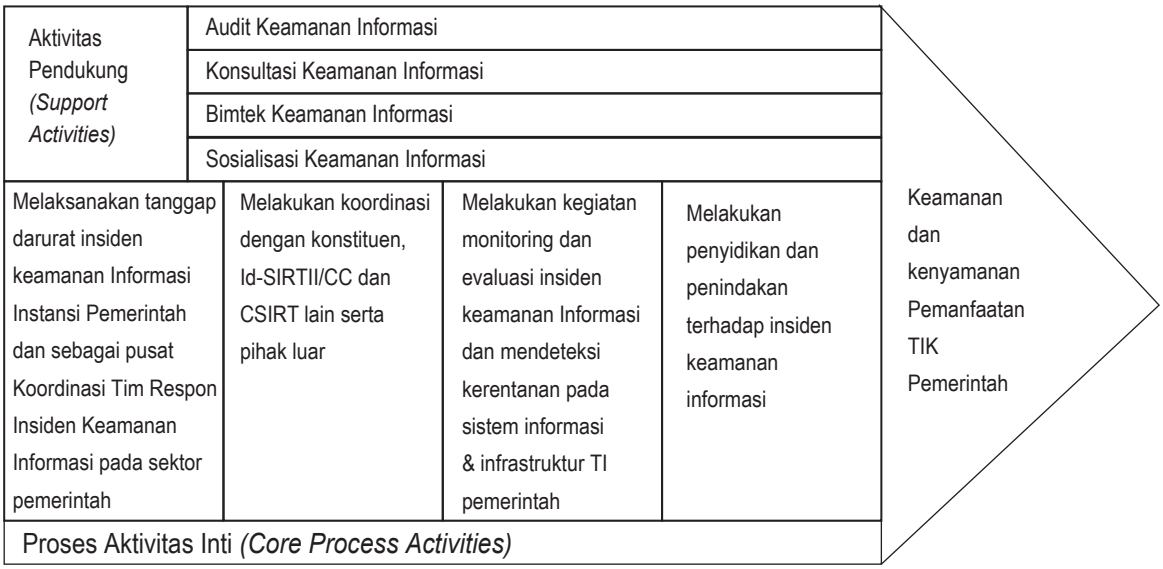
Bagian tahapan perencanaan ini bertujuan mengidentifikasi persyaratan yang dibutuhkan dalam mengembangkan pemanfataan Sistem Informasi pada Pusat Penanganan Insiden Keamanan Informasi Pemerintah (GovCSIRT). Identifikasi dilakukan dengan melibatkan beberapa aktivitas seperti: mengidentifikasi peraturan hukum dan peraturan yang memengaruhi GovCSIRT dan tren insiden saat ini untuk menentukan fokus layanan yang akan diberikan GovCSIRT. Analisis dilakukan menggunakan analisis *value chain*, matriks SWOT (*Strength, Weakness, Opportunity*, *Threats*), TOWS, dan Analisis CSF.

Analisis Value Chain

Pembentukan Pusat Penanganan Insiden Keamanan Informasi Pemerintah bertujuan untuk mendukung pelaksanaan program monitoring, evaluasi dan tanggap darurat keamanan informasi instansi Pemerintah (GovCSIRT) yang mempunyai tanggung jawab sebagai berikut:

1. Memberikan layanan dan melakukan Penanganan Tanggap Darurat Keamanan Informasi Instansi Pemerintah
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
4. Menyusun rancana kerja dan jadwal pelaksanaan untuk pelaksanaan analisis, dan evaluasi serta monitoring terhadap insiden keamanan informasi di instansi pemerintah
5. Mengumpulkan bahan yang berkaitan dengan penanganan insiden Keamanan Informasi Instansi Pemerintah
6. Melakukan koordinasi dengan satuan kerja terkait untuk membahas materi-materi Penanganan Insiden Keamanan Informasi Instansi Pemerintah

Analisis *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. Analisis *Value Chain* pada GovCSIRT dapat dilihat pada Gambar 4 berikut ini.



Gambar 4. Diagram Analisis *Value Chain* GovCSIRT

Analisis Critical Success Factor

Sebagai organisasi yang baru didirikan (2011), GovCSIRT dibebani dengan permasalahan yang sangat besar terkait dengan keamanan informasi. GovCSIRT dituntut untuk memberikan layanan tanggap darurat insiden keamanan informasi pada instansi pemerintah. Secara statistik yang dimiliki baik oleh Id-SIRTII ataupun ID-CERT, 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. Berikut analisis CSF pada bidang keamanan informasi nasional dan GovCSIRT untuk memetakan layanan bisnis yang ada sehingga diperoleh gambaran internal bisnis GovCSIRT.

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 kerjasama 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 kerjasama keamanan informasi;	Tata Kelola keamanan informasi	Tersusunnya kebijakan di bidang strategi dan kerjasama keamanan informasi
Penyusunan kebijakan, standard 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

Tabel 2. Analisis CSF untuk Internal Bisnis GovCSIRT

Strategi	CSF	Kebutuhan SI/TI
Melakukan tanggap darurat insiden keamanan informasi	Respon tanggap darurat insiden keamanan informasi	✓ Saluran komunikasi ✓ Layanan kontak 24 jam ✓ SI Database kontak ✓ SI Aduan Keamanan Informasi ✓ *Digital Signature,* PGP dan PKI
Melakukan monitoring keamanan informasi	Monitoring & evaluasi keamanan informasi Pemerintah	✓ *Tools monitoring on-line* ✓ *e-monitoring*
Melakukan penyidikan dan penindakan terhadap insiden keamanan infomasi	Penyidikan dan penindakan	✓ *Tools* untuk *digital forensic*
Melaksanakan audit dan evaluasi keamanan informasi	Audit Keamanan Informasi	✓ *Web Based Pen-Test Application Aplikasi Risk Management* (APRISMA)
Bimbingan teknis dan konsultasi keamanan informasi	Bimbingan Teknis dan konsultasi	✓ Sistem Informasi yang menyimpan pengetahuan mengenai keamanan informasi / *knowledge management* tentang keamanan informasi ✓ *E-learning* keamanan informasi
Sosialisasi dan edukasi keamanan informasi	Sosialisasi keamanan informasi	✓ *Web content* yang berisi sosialiasi dan kampanye kesadaran keamanan informasi
Koordinasi dengan konstituen dan pihak luar	Kolaborasi dan koordinasi	✓ Saluran komunikasi ✓ Jaringan internet

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 di mana 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.

Tabel 3. Analisis PEST Gov CSIRT

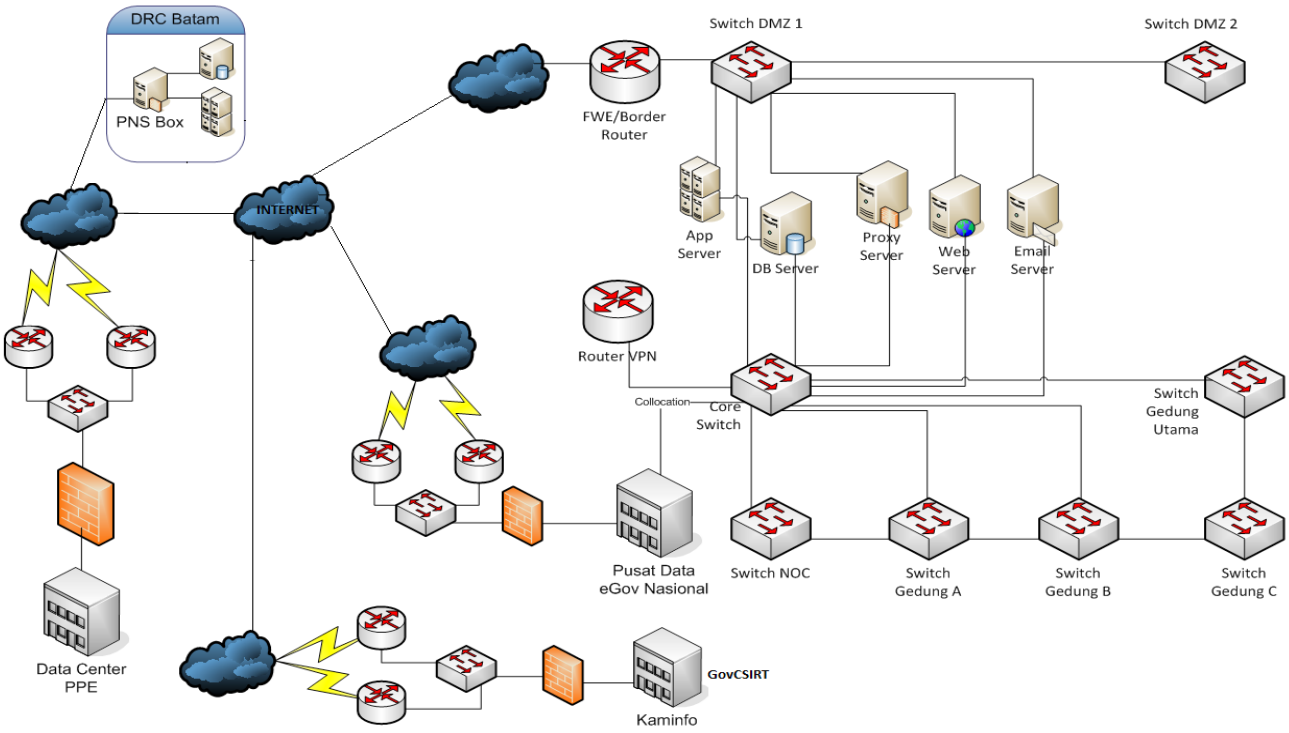
Politik	Ekonomi
1. Pengaruh politik mempunyai dampak yang besar dalam pemanfaatan TIK di Indonesia, dalam hal ini untuk implementasi *e-government* 2. Pemerintah telah menetapkan Peraturan Perundangan di bidang Transaksi Elektronik, yaitu UU ITE 3. Pemerintah juga telah mengeluarkan Surat Edaran No. 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*

Implementasi Perencanaan Strategis Sistem Informasi Pusat Penanganan Insiden Keamanan Informasi Pemerintah

Dalam konteks implementasi Perencanaan Strategis Sistem Informasi (SI)/Teknologi Informasi (TI), akan digali kondisi SI/TI pada saat ini sebagai acuan agar rencana strategis GovCSIRT dapat dicapai. Dengan menggunakan analisis *McFarlan*, ditinjau kondisi eksisting dari aplikasi saat ini. Hal ini bertujuan untuk membuat perencanaan portofolio yang ditargetkan. Analisis Konteks SI/TI Internal, mencakup kondisi SI/TI organisasi dari perspektif bisnis saat ini, bagaimana kontribusi terhadap bisnis, sumber daya dan infrastruktur teknologi, termasuk juga bagaimana portofolio dari SI/TI yang ada saat ini.

Kondisi Situasi SI/TI Saat Ini

GovCSIRT merupakan salah satu program yang dimiliki oleh Direktorat Jenderal Aplikasi Informatika(Ditjen APTIKA) melalui Direktorat Keamanan Informasi. Dengan demikian, infrastruktur SI/TI yang digunakan oleh GovCSIRT seluruhnya disediakan oleh Direktorat Keamanan Informasi, Ditjen APTIKA, Kementerian Kominfo. Berdasarkan data yang dimiliki oleh Ditjen APTIKA, berikut ini adalah topologi Infrastruktur TI di GovCSIRT yang difasilitasi oleh Ditjen Aptika saat ini. Gambar 5 berikut ini adalah ilustrasi topologi Jaringan yang dimiliki Ditjen APTIKA saat ini:



Gambar 5. Topologi Infrastruktur TI pada GovCSIRT Ditjen APTIKA saat ini

Portofolio aplikasi Sistem Informasi yang saat ini digunakan oleh GovCSIRT adalah portofolio yang difasilitasi oleh Direktorat Jenderal Aplikasi Informatika, Kementerian Kominfo. Hal ini disebabkan karena GovCSIRT berada di bawah wewenang Direktorat Keamanan Informasi. Hal tersebut dapat terlihat pada penjelasan Tabel 4 berikut ini.

Tabel 4. Portofolio Aplikasi GovCSIRT-Ditjen APTIKA Saat Ini

STRATEGIC	HIGH POTENTIAL
• *Aplikasi Risk Management* (APRISMA) • e-Aduan Keamanan Informasi • *e-Monitoring* • *Public Key Infrastructure*	• TRUST+ Positif • ASP *Govt Services* • *e-learning* • Manajemen Integrasi Informasi dan Pertukaran Data (Mantra) • *Certficate of Authority*
• Aplikasi Layanan Publik • *Knowledge Management* • PNS Box	• Portal GovCSIRT • Intranet • *e-Office*
KEY OPERATIONAL	**SUPPORTING**

Untuk dapat mengetahui kondisi infrastruktur SI/ TI yang dapat dimanfaatkan oleh GovCSIRT untuk menunjang aktivitasnya, maka seluruh infrastruktur yang dimiliki oleh Kementerian Kominfo dapat dimanfaatkan meskipun dimiliki oleh Satuan Kerja di luar Ditjen APTIKA. Id-SIRTII/CC merupakan salah satu unit layanan Keamanan Informasi dalam hal respon insiden keamanan informasi.

Dalam hal proses pemantauan dan analisis insiden keamanan informasi, Id-SIRTII memiliki sejumlah aplikasi pendukung atau penunjang proses pemantauan serta analisis tren pola trafik yang dipantau tersebut. Secara fungsional, dengan kapabilitas yang dimiliki oleh perangkat aplikasi tersebut, rangkaian proses yang dilakukan oleh Id-SIRTII menyangkut tiga hal (atau yang dikenal sebagai 3D). Istilah 3D ini khusus diperkenalkan dan diperuntukkan untuk perangkat aplikasi *Sourcefire* – pengembangan dari *Snort* – untuk merepresenasikan keunggulan dan kapabilitas perangkat lunaknya yang dikeluarkan pada awal tahun 2007.

1. *Detect*, sebuah proses di mana melalui pemantauan ditemukan suatu pola trafik yang anomali atau tidak biasa dari kondisi normalnya.
2. *Determine*, yaitu sebuah rangkaian proses analisis untuk menentukan apakah pola trafik anomali tersebut berpotensi menjadi sebuah insiden yang dapat mengganggu kerja sistem.
3. *Defend*, yaitu suatu proses reaktif (maupun prefentif) dengan cara memberikan *early warning system* kepada pihak-pihak yang terlibat dan memberitahukan cara paling efekif untuk melakukan perlindungan terhadap insiden tersebut.

Mengingat salah satu karakteristik CSIRT adalah kolaborasi, maka dalam aktivitasnya, GovCSIRT dapat berelaborasi dengan Id-SIRTII dalam hal kinerja dan tentunya dalam hal memanfaatkan sumber daya infrastruktur.

Analisis Tren TI Saat Ini

Analisis Tren SI/ TI yang sedang berkembang saat ini, mencakup tren teknologi dan peluang pemanfaatannya, serta penggunaan SI/ TI yang dapat dimanfaatkan oleh GovCSIRT. Teknologi sangat mendukung dalam penyampaian layanan GovCSIRT. Perkembangan teknologi akan mendatangkan perubahan layanan aplikasi informatika bagi konstituen. Untuk pemahaman lebih lanjut, maka tren teknologi tersebut dapat dijelaskan lebih lanjut pada Tabel 5 berikut ini:

Tabel 5. Analisis Tren Teknologi SI/TI

Tren Teknologi	Contoh Teknologi
Teknologi *Hardware*	RAID, SAN, NAS
Teknologi Jaringan	Open Standard, TCP/IP, DHCP, HighSpeed WLAN, media transmisi
Teknologi Database	*RDBMS, Data Mining, Data WareHouse*
Teknologi Sistem Operasi	*Linux, Open Source, UNIX, Proprietary, Window*
Trend Teknologi Sistem Informasi	SOA, SOAP, SONA
Trend Virtualisasi infrastruktur	*Vmware, Virtual Box*
Trend web 2.0	*LMS, multimedia*
Trend cloud computing	*Infrastucture as Service dan Software as Service*
Trend IPv6	IPv6 teknologi
Trend Konvergensi	IPTV
Trend Security	*Encryption, PKI, firewall, VPN, CA*
Teknologi Terintegrasi	*ERP*

Analisis SWOT Sistem Informasi

Strategi SI bisnis, yang mencakup bagaimana setiap unit/ fungsi bisnis akan memanfaatkan SI/TI untuk mencapai sasaran bisnisnya, portofolio aplikasi dan gambaran arsitektur informasi. Untuk menganalisis strategi bisnis SI dapat menggunakan analisis TOWS sebagai pelengkap analisis SWOT. Analisis TOWS dapat memetakan peluang dan ancaman eksternal dengan kekuatan dan kelemahan internal suatu organisasi kedalam 4 (empat) alternatif strategi bisnis. Analisis SWOT ditunjukkan pada Tabel 6 di bawah ini:

Tabel 6. Analisis SWOT pada GovCSIRT untuk SI/TI

Kekuatan (*Strength*)	**Kelemahan (*Weakness*)**
1. Kementerian Kominfo melalui Direktorat Keamanan Informasi adalah pemegang kebijakan tertinggi di bidang Keamanan Informasi TIK, dan GovCSIRT berada dibawah Direktorat Keamanan Informasi 2. Dukungan sumber daya dan infrastruktur SI/TI yang dimiliki oleh Kementerian Komunikasi dan Informatika 3. Surat Keputusan Dirjen APTIKA berdasarkan SK No. 01/SK/DJAI/ KOMINFO/01/2012. Tentang Pembentukan Tim Respon Insiden Keamanan Informasi Pemerintah	1. Fasilitas yang dimiliki Gov't CSIRT Direktorat Keamanan Informasi masih sangat minim 2. Belum terbentuk kelembagaan dan model koordinasi GovCSIRT yang ideal 3. Belum tersedianya manajemen pengetahuan mengenai keamanan informasi dan insiden serangan 4. Belum tersedianya database kontak insiden keamanan informasi
Peluang (*Opportunity*)	**Ancaman (*Threat*)**
1. Adanya dukungan kuat dari CC-CSIRT Indonesia; Id-SIRTII dan CSIRT berbasis komunitas di Indonesia; ID-CERT 2. Pesatnya perkembangan teknologi keamanan informasi dan saat ini menjadi salah satu tren teknologi dunia. 3. Adanya Kerjasama berupa koordinasi dengan multipihak untuk permasalahan insiden keamanan informasi *4.* Adanya SNI 7512:2008 tentang Teknik keamanan – Pengelolaan insiden keamanan informasi yang diadopsi dari ISO/IEC TR 18044:2004, *Information Technology – security techniques – Information Security Incident Management*	1. Meningkatnya insiden serangan keamanan informasi terhadap infrastruktur milik Pemerintah 2. Monitoring insiden keamanan informasi tidak terpantau dengan baik 3. Respon terhadap insiden keamanan informasi pemerintah belum ditangani secara maksimal 4. Tersebarnya teknik-teknik penyerangan *Cyber warfare*

Tabel 7. Analisis TOWS pada GovCSIRT untuk SI/TI

Strategi Menggunakan Kekuatan untuk Memanfaatkan Peluang (S-O)	• Memperkuat fungsi GovCSIRT sebagai tim respon insiden keamanan informasi di kalangan pemerintah • Memanfaatkan kolaborasi dengan Id-SIRTII untuk pemanfaatan sumber daya infrastruktur SI/TI dalam penanganan insiden keamanan informasi • Mempersiapkan teknologi keamanan infrastruktur TIK pada GovCSIRT dengan teknologi keamanan informasi yang mutakhir
Strategi Meminimalkan Kelemahan dengan Menggunakan Peluang (W-O)	• Melakukan sosialisasi dan koordinasi dengan seluruh instansi Pemerintah dalam hal penanganan insiden keamanan informasi • Memberikan konsultasi dan bimbingan teknis bagi aparatur Pemerintah dalam menerapkan tata kelola keamanan informasi • Melakukan audit kesiapan infrastruktur pengaman dan kondisi keamanan informasi • Membuat strategi dan landasan kebijakan untuk kolaborasi antar instansi Pemerintah dan pihak terkait lainnya dalam hal penanganan insiden keamanan informasi
Strategi Menggunakan Kekuatan untuk Mengatasi Ancaman (S-T)	• Membentuk kelembagaan penanganan insiden keamanan informasi yang *sustainable* • Mengembangkan teknologi dan infrastruktur Keamanan Informasi untuk monitoring dan menghadapi insiden keamanan informasi • Melakukan penyidikan dan penindakan atas terjadinya insiden keamanan informasi • Memberdayakan sumber daya infrastruktur yang dimiliki oleh internal pada Satuan Kerja dilingkungan Kementerian kominfo dalam mendukung GovCSIRT
Strategi Memperkecil Kelemahan untuk Menghindari Ancaman (W-T)	• Meningkatkan pengetahuan dan pemahaman sumber daya manusia aparatur pemerintah akan keamanan informasi dan memaksimalkan penerapan kebijakan keamanan informasi yang telah dikeluarkan bagi setiap instansi Pemerintah • Membuat master plan pemanfaatan SI/TI pada GovCSIRT untuk mendukung strategi bisnis GovCSIRT • Memanfaatkan forum *e-goverment* dalam mengembangkan database kontak konstituen GovCSIRT • Mempersiapkan dan membuat standar prosedur keamanan infrastruktur TIK pada instansi pemerintah serta SOP dalam keamanan informasi

Berdasarkan analisis SWOT tersebut, menggambarkan situasi dan kondisi yang dihadapi oleh Direktorat Jenderal Aplikasi Informatika, maka strategi yang telah dijalankan oleh organisasi adalah:

Tabel 8. Pemetaan Strategi SWOT di GovCSIRT

Strategi SWOT	Pemetaan
Memperkuat fungsi GovCSIRT sebagai tim respon insiden keamanan informasi di kalangan pemerintah	SO1
Memanfaatkan kolaborasi dengan Id-SIRTII untuk pemanfaatan sumber daya infrastruktur SI/TI dalam penanganan insiden keamanan informasi	SO2
Mempersiapkan teknologi keamanan infrastruktur TIK pada GovCSIRT dengan teknologi keamanan informasi yang mutakhir untuk aktivitas seluruh GovCSIRT	SO3
Melakukan sosialisasi dan koordinasi dengan seluruh instansi Pemerintah dalam hal penanganan insiden keamanan informasi	WO1
Memberikan konsultasi dan bimbingan teknis bagi aparatur Pemerintah dalam menerapkan tata kelola keamanan informasi	WO2
Melakukan audit kesiapan infrastruktur pengaman dan kondisi keamanan informasi	WO3
Membuat strategi dan landasan kebijakan untuk kolaborasi antar instansi Pemerintah dan pihak terkait lainnya dalam hal penanganan insiden keamanan informasi	WO4
Membentuk kelembagaan penanganan insiden keamanan informasi yang *sustainable*	ST1
Mengembangkan teknologi dan infrastruktur Keamanan Informasi untuk monitoring dan menghadapi insiden keamanan informasi	ST2
Melakukan penyidikan dan penindakan atas terjadinya insiden keamanan informasi	ST3
Memberdayakan sumber daya yang dimiliki oleh internal pada Satuan Kerja dilingkungan Kementerian kominfo dalam mendukung GovCSIRT	ST4

Strategi SWOT	Pemetaan
Meningkatkan pengetahuan dan pemahaman sumber daya manusia aparatur pemerintah akan keamanan informasi dan memaksimalkan penerapan kebijakan keamanan informasi yang telah dikeluarkan bagi setiap instansi Pemerintah	WT1
Membuat *master plan* pemanfaatan SI/TI pada GovCSIRT untuk mendukung strategi bisnis GovCSIRT	WT2
Memanfaatkan forum *e-goverment* dalam mengembangkan database kontak konstituen GovCSIRT	WT3
Mempersiapkan dan membuat standar prosedur keamanan infrastruktur TIK pada instansi pemerintah serta SOP dalam keamanan informasi	WT4

Berdasarkan analisis *value chain* yang telah dilakukan pada GovCSIRT, maka selanjutnya dapat ditentukan solusi SI yang sesuai dengan karakteristik organisasi, di antaranya adalah sebagai berikut:

Tabel 9. Analisis *Value Chain* untuk Solusi SI GovCSIRT

No	BIDANG KERJA	KEGIATAN	SOLUSI SI
1	Tanggap Darurat Insiden Keamanan Informasi	Melakukan tanggap darurat terhadap insiden keamanan informasi di lingkungan instansi Pemerintah	e-Aduan Keamanan Informasi*, Aplikasi Layanan Publik, Portal GovCSIRT, ASP (*Application Service Provider) Gov't Service*
2	Monitoring dan evaluasi insiden keamanan Informasi	Melakukan monitoring dan evaluasi insiden keamanan informasi, analisis hasil monitoring dan deteksi kerentanan *(vulnerabilities)* sistem informasi dan infrastruktur TI Pemerintah	*Private Network Security Box, PKI, TRUST+ Positive*
3	Penyidikan dan penindakan terhadap insiden keamanan informasi	Melakukan penyidikan melalui digital forensic dan penindakan terhadap adanya insiden keamanan informasi	SIM Hukum*, Aplikasi *Digital Forensic*
4	Audit Keamanan informasi pemerintah	Menilai kondisi kesiapan Keamanan Informasi pada instansi Pemerintah	Aplikasi *Risk Management*
5	Konsultasi dan Bimbingan Teknis Keamanan Informasi	Memberikan jasa konsultasi dan bimbingan secara teknis bagi para pengelola TI di lingkungan instansi Pemerintah	*Knowledge Management,*
6	Sosialisasi dan Edukasi Keamanan Informasi	Memberikan pemahaman dan edukasi untuk para aparatur Pemerintah pengelola TIK untuk meningkatkan kesdaran dan pemahaman mengenai Keamanan Informasi	*e-Learning*, Content Management System (CMS)*
7	Koordinasi dengan konstituen	Menjalin hubungan (*relationship*) dan komunikasi yang baik dengan konstituen dan pihak luar lainnya	Manajemen Integrasi Informasi dan Pertukaran Data (Mantra), PNS Box, ASP *Inter Government*

Analisis CSF dan Strategi SWOT GovCSIRT

Hasil analisis CSF GovCSIRT sebelumnya ditujukan untuk menentukan analisis bisnis internal organisasi. Selanjutnya dilakukan pemetaan CSF dengan Strategi SWOT untuk menghasilkan strategi bisnis SI pada GovCSIRT yaitu sebagai berikut:

Tabel 10. Identifikasi Kebutuhan Informasi GovCSIRT

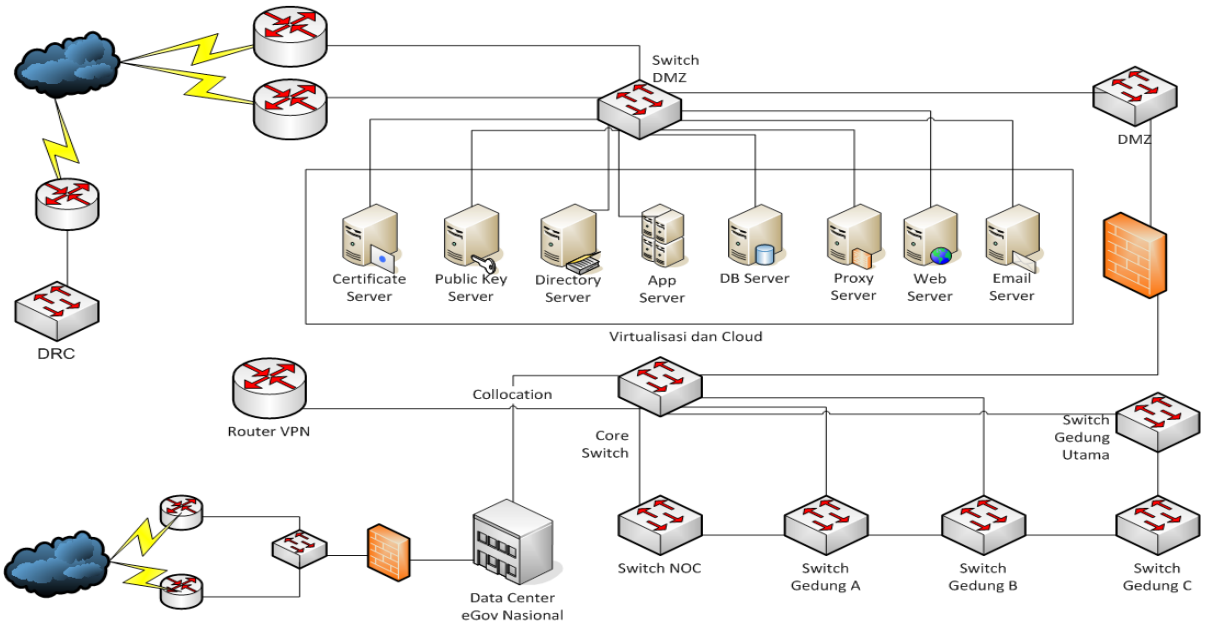
Value Chain	CSF	Prime Measures	Strategi SWOT	Data / informasi	Solusi SI
Tanggap Darurat Insiden Keamanan Informasi	Respon tanggap darurat insiden keamanan informasi	Tertanganinya insiden keamanan infromasi dengan baik dan turunnya jumlah insiden keamanan informasi di lingkungan instansi Pemerintah	SO1, SO3, ST1, WT2, WT4	Data tentang kebijakan di bidang keamanan informasi	e-Aduan Keamanan Informasi*, Aplikasi Layanan Publik, Portal GovCSIRT, ASP (*Application Service Provider*) Gov't Service
Monitoring dan evaluasi insiden keamanan Informasi	Monitoring & evaluasi keamanan informasi Pemerintah	Diketahuinya status kondisi keamanan informasi dan kondisi kerawanan infrastruktur TIK Pemerintah	SO1, SO3, ST3, WT2	Data dan informasi tentang program dan evaluasi kegiatan serta regulasi bidang keamanan informasi	*Private Network Security Box*, PKI, TRUST+ *Positive*
Penyidikan dan penindakan terhadap insiden keamanan informasi	Penyidikan dan penindakan	Tersidik dan tertindaknya setiap insiden keamanan informasi dapat disidik dan ditindak	SO1, SO2, SO3, WT2, ST3	Data tentang teknologi keamanan informasi	SIM Hukum*, Aplikasi Digital Forensic
Audit Keamanan informasi pemerintah	Audit Keamanan Informasi	Diketahuinya kondisi kesiapan Keamanan Informasi pada instansi Pemerintah	SO1, SO2, SO3, WT2, WO3,	Data dan informasi tentang monitoring, evaluasi, dan tanggap darurat keamanan informasi	Aplikasi Risk Management
Konsultasi dan Bimbingan Teknis Keamanan Informasi	Bimbingan Teknis dan konsultasi	Terlayaninya permasalahan mengenai keamanan informasi pada instansi Pemerintah	SO1, SO3, WT2, WO2	Data dan Informasi tentang permasalahan teknis keamanan informasi	*Knowledge Management*,
Sosialisasi dan Edukasi Keamanan Informasi	Sosialisasi keamanan informasi	Meningkatnya tingkat kesadaran aparatur pemerintah akan keamanan informasi	SO1, SO3, WT1, WT2, WO1,	Informasi mengenai keamanan informasi	*e-Learning**, *Content Management System* (CMS)
Koordinasi dengan konstituen	Kolaborasi dan koordinasi	Terjalinnya hubungan baik dan komunikasi antara GovCSIRT dengan konstituen dan pihak luar lainnya	SO1, SO3, WT2, WT3 , WO1, SO2, WO3, WO4	Database kontak konstituen, ISP dan pihak terkait lainnya	Manajemen Integrasi Informasi dan Pertukaran Data (Mantra), PNS Box, ASP Inter Government

Strategi TI, yang mencakup kebijakan dan strategi bagi pengelolaan teknologi dan sumber daya manusia SI/TI. Mengacu pada strategi bisnis utama yang sedang dilakukan, baik jangka pendek maupun jangka panjang, maka disusun strategi SI/ TI-nya. Secara umum, maka strategi SI/ TI yang digunakan organisasi, dijelaskan pada Tabel 11 di bawah ini:

Tabel 11. Strategi TI di GovCSIRT dan Ditjen APTIKA

Teknologi *Hardware*	NAS
Teknologi Jaringan	*Open Standard*, TCP/IP
Teknologi Database	*Open Source*
Teknologi Sistem Operasi	*Open Source*
Trend Teknologi Sistem Informasi	SOA
Trend Virtualisasi infrastruktur	Virtualisasi *Server*
Trend web 2.0	LMS, multimedia
Trend mobile & cloud computing	*Software as a Service*
Trend IPv6	IPv6 teknologi
Trend Konvergensi	*Social computing*
Trend Security	*Encryption, PKI, Redundant firewall, VP, DRC, CA*

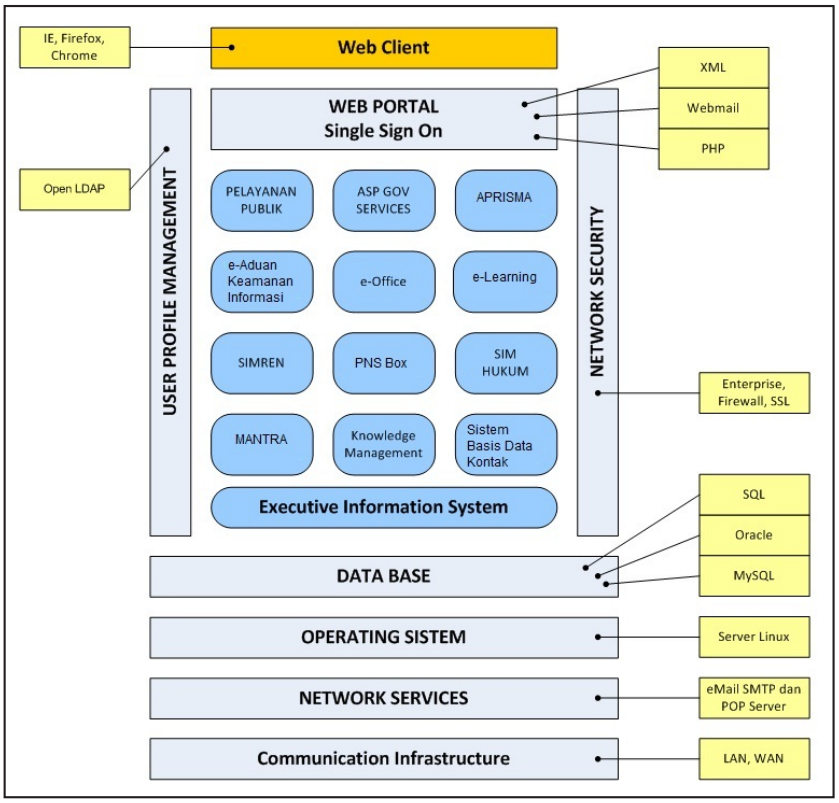
Berdasarkan acuan perkembangan teknologi di atas, maka dapat digambarkan topologi infrastruktur TI untuk GovCSIRT, adalah sebagai berikut:



Gambar 6. Topologi Infrastruktur TI GovCSIRT di Masa Mendatang

Arahan Strategis Manajemen SI/ TI

Arahan untuk manajemen SI/ TI mencakup elemen-elemen umum yang diterapkan melalui organisasi, untuk memastikan konsistensi penerapan kebijakan SI/TI yang dibutuhkan. Konsep rancangan aplikasi tersebut diarahkan untuk membangun aplikasi menjadi dua bagian, yaitu bagian yang menyediakan antarmuka kepada *user* dan bagian yang memroses dan menyimpan data ke dalam *database*. Pada Gambar 7 di bawah ini, dijelaskan arsitektur Sistem Informasi gabungan pada GovCSIRT.



Gambar 7. Arsitektur Sistem Informasi GovCSIRT

Aplikasi yang digunakan untuk menerapkan konsep tersebut adalah aplikasi yang berbasis *web based* sehingga dibutuhkan penggunaan *database* yaitu RDBMS (*Relational Database Management System*). Untuk sistem operasi yang digunakan baik untuk *server* atau untuk *workstation* akan diarahkan pada penggunaan sistem operasi yang *open sources*.

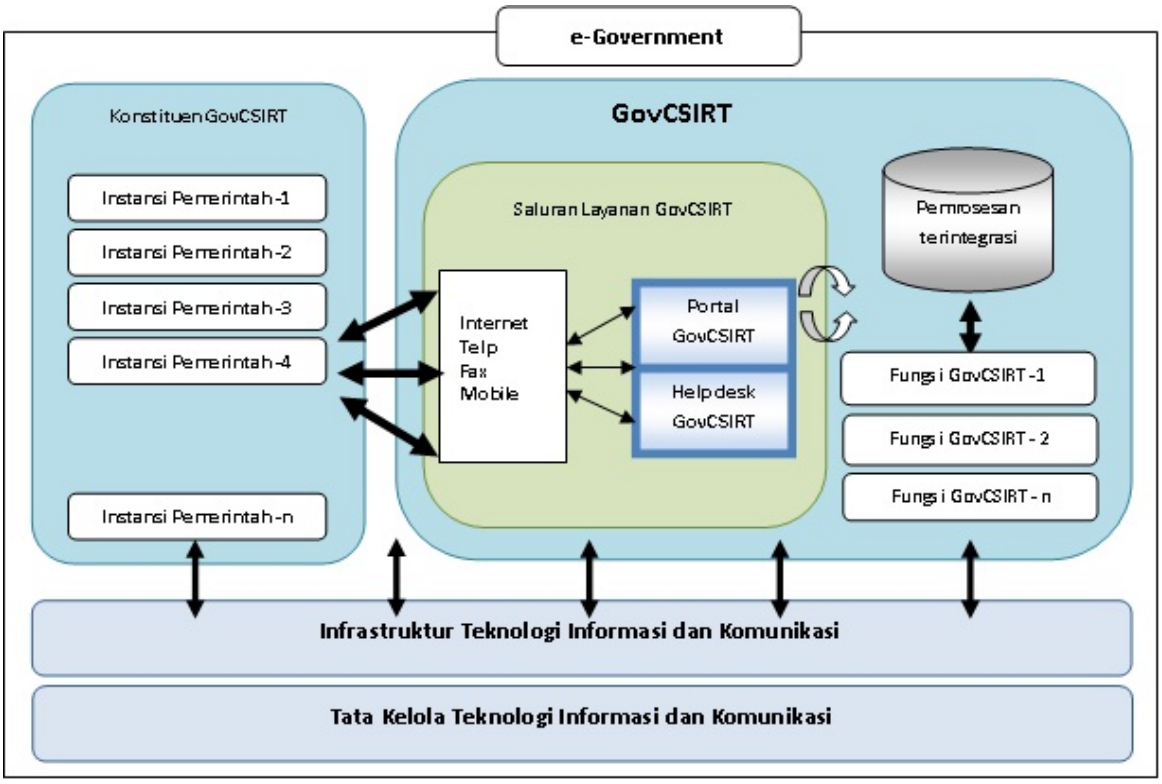
Untuk usulan konfigurasi infrastruktur jaringan komputer di GovCSIRT adalah sistem jaringan yang tidak melupakan faktor keamanan dalam perencanaannya. Dalam melakukan suatu pengamanan infrastruktur SI, digunakan kebijakan keamanan yang di dalamnya berisi aturan-aturan yang akan membantu memastikan setiap kinerja karyawan bekerja sesuai dengan apa yang diinginkan organisasi. Untuk melakukan perencanaan keamanan maka GovCSIRT berpedoman pada Tata Kelola Keamanan Informasi dan mengacu pada Standar ISO 27001:2005.

Strategi Operasionalisasi dan Pengembangan SI/TI dalam Kerangka e-government

Sebagai unit kerja yang memberikan layanan, GovCSIRT juga dituntut harus mampu memberikan *service level agreement* yang sesuai standar organisasi GovCSIRT pada umumnya. Dengan demikian dibutuhkan pengembangan infrastruktur SI/ TI yang memadai sesuai dengan standar yang berlaku umum. Di satu sisi, anggaran yang dikeluarkan untuk memfasilitasi infrastruktur SI/TI GovCSIRT berikut operasionalnya sangat mahal. Untuk terus meningkatkan kualitas layanan, pengembangan tersebut perlu dilakukan berdasarkan rencana strategis sistem informasi yang dirancang.

Biaya pengembangan sebaiknya ditekan serendah mungkin dengan strategi pemanfaatan *software open source* yang sudah terbukti kualitasnya. Di samping itu, strategi kolaborasi sumber daya infrastruktur SI/ TI dapat dilakukan. Mengingat salah satu karakteristik organisasi CSIRT adalah kolaborasi, maka GovCSIRT dapat memanfaatkan kolaborasi dengan Id-SIRTII/CC.

Salah satu bentuk inisiatif yang dapat dilakukan GovCSIRT adalah dengan memainkan peran penting dalam berkolaborasi dengan seluruh konstituen untuk memproteksi keamanan informasi. Untuk itu, Sebagai salah satu komponen pendukung keberhasilan implementasi *e-government* di Indonesia, GovCSIRT dituntut untuk memberikan layanan bagi instansi Pemerintah baik pusat maupun daerah dalam menjaga keamanan informasi dengan memanfaatkan TIK sebagai pemungkin (*enabler*) bagi kesuksesan organisasi. Gambar 8 di bawah ini menjelaskan strategi operasionalisasi GovCSIRT dalam kerangka *e-government.*



Gambar 8. GovCSIRT dalam kerangka *e-government*
(diolah dari konsep layanan *e-government,* Dit. *e-government,* Kominfo)

Dalam konteks pemanfaatan TIK untuk layanan publik, GovCSIRT juga dituntut untuk memanfaatkan teknologi TIK yang handal terutama untuk teknologi keamanan informasi. Organisasi pemerintah yang terus berkembang, menuntut seluruh pihak yang terlibat sebagai komponen *e-government* untuk dapat memanfaatkan infrastruktur TIK dengan baik dan mengelola infrastruktur tersebut dengan baik pula. Hal inilah yang dinamakan tata kelola TIK dan juga tata kelola keamanan TIK.

Portofolio Aplikasi Sistem Informasi

Pada *application portfolio matrix* di bawah ini bisa diperhatikan peran dari masing-masing aplikasi SI pada GovCSIRT. Matrik portofolio berikut ini bertujuan untuk mengategorikan prioritas Aplikasi Sistem Informasi berdasarkan tingkat kepentingan aplikasi tersebut. Strategi prioritas aplikasi Sistem Informasi pada GovCSIRT dijelaskan pada Tabel 12 berikut ini.

Tabel 12. Portofolio Aplikasi di GovCSIRT

STRATEGIC	HIGH POTENTIAL
• Aplikasi *Risk Management***	• ASP *Inter Government*
• e-Aduan Keamanan Informasi*	• TRUST+ Positif
• PNS Box (*Enterprise Security Management*)**	• *Knowledge Management* *
• Aplikasi enkripsi dan *digital signature**	
• Sistem Informasi Basis Data Kontak*	• Intranet
• *E-Learning**	• *e-Office*
• SIM Hukum dan investigasi*	
• Manajemen Integrasi Informasi dan Pertukaran Data (Mantra)	
• *Content Management System**	
• *Certification Authority***	
• *Public Key Infrastructure***	
• Portal GovCSIRT**	
KEY OPERATIONAL	**SUPPORTING**

Keterangan:
(*) Inisiatif Aplikasi Baru
(**) Aplikasi sudah ada namun belum dan perlu diperbaharui disesuaikan dengan kebutuhan

Pembagian kategori tersebut, adalah sebagai berikut:

- *Supporting*: Aplikasi berperan hanya sebagai penunjang dan sangat umum bagi organisasi.
- *High Potential*; Aplikasi yang bersifat inovasi/pengembangan.
- *Key Operational*; Aplikasi digunakan sebagai penunjang operasional organisasi GovCSIRT.
- *Strategic*: aplikasi yang sangat kritis bagi organisasi dan bersifat strategis.

Gap Analysis Sistem Informasi di GovCSIRT

Berdasarkan kondisi sistem informasi yang ada di GovCSIRT dan kebutuhan akan sistem informasi untuk mendukung bisnis organisasi, maka dapat dibuat hasil analisis berupa matriks penggunaan data yang biasanya dikenal dengan CRUD Matrix (*Create, Read, Use,* dan *Delete*). Hal ini dapat dilihat pada Tabel 13 berikut ini:

Tabel 13. *Gap Analysis* Sistem Informasi di GovCSIRT

EXISTING	FUTURE																			ELIMINATED
		Portal GovCSIRT	Intranet	e-Office	ASP Inter Government	TRUST+ Positif	Aplikasi Layanan Publik	PNS Box	Certification Authority	Public Key Infrastructure	Aplikasi Enkripsi dan Digital signature	e-Learning	Knowledge Management	SIM Hukum	Content Management System	e-Aduan Keamanan Informasi	APRISMA	Sistem Informasi Basis Data Kontak	ASP Gov Services	
	Portal GovCSIRT	U										add	add		add					
	Intranet		R												add					
	e-Office			R																
	TRUST+ Positif					R									add					
	Aplikasi Layanan Publik						R													
	ASP Inter Government				R													add		
	PNS Box							U												
	CA								U	add	add									
	Public Key Infrastructure								add	U	add									
	ASP GovServices																		R	
	APRISMA																U			
	New										C	C	C	C	C	C		C		

Gap Analysis Infrastruktur TI di GovCSIRT

Berdasarkan potret kondisi infrastruktur teknologi informasi yang ada di GovCSIRT dan kebutuhan akan infrastruktur teknologi informasi yang sesuai dengan kebutuhan bisnis organisasi, maka dapat dibuat hasil analisis berupa matriks penggunaan data yang biasanya dikenal dengan analisis kesenjangan (*gap analysis*) pada infrastruktur TI GovCSIRT. Hal ini dapat dilihat pada Tabel 14 di bawah ini:

Tabel 14. *Gap Analysis* Infrastruktur TI di GovCSIRT

	GAP ANALYSIS INFRASTRUKTUR TI					
	FUTURE					
	Open Source DataBase	*Open Source Server*	*Redundant Firewall*	*NAS*	*Virtualisasi Server*	*ELIMINATED*
EXISTING						
Proprietary DataBase						*DELETE*
Open Source DataBase	*RETAIN*					
Open Source Server		*RETAIN*				
Proprietary Server						*DELETE*
Single Firewall			*REPLACE*			
Storage				*REPLACE*		
Server Fisik					*REPLACE*	
NEW						

Roadmap SI/TI GovCSIRT dalam Tiga Tahun

Pada bagian ini akan dibahas mengenai *roadmap* inplementasi proyek-proyek sistem informasi. Hal yang menjadi dasar pertimbangan dari *roadmap* ini adalah prioritas Sistem Informasi bagi kebutuhan operasional organisasi. Berdasarkan solusi SI/TI yang didapat dari hasil analisis sebelumnya maka *roadmap* tiga tahun di GovCSIRT dapat dijelaskankan secara rinci pada Tabel 15 di bawah ini:

Tabel 15. *Roadmap* 3 (Tiga) Tahun Implementasi SI/TI GovCSIRT

STRATEGI		Tahap 1				Tahap 2				Tahap 3			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Aplikasi Baru													
1	e-Aduan Keamanan Informasi												
2	Aplikasi enkripsi dan Tandatangan Digital												
3	Sistem Informasi Basis Data Kontak												
4	*e-learning*												
5	SIM Hukum												
6	*Knowledge Management*												
7	*Content Management System*												
Pengembangan Aplikasi Lama													
1	PNS Box												
2	APRISMA												
3	Portal GovCSIRT												
Infrastruktur TI													
1	Integrasi Infrastruktur												
2	*Server Farm* (Virtualisasi Cloud)												
3	*Data Recovery Center* (DRC)												
Manajemen													
1	Kebijakan dan Prosedur SI/TI												
2	Melakukan Evaluasi Tata Kelola SI/TI di govCSIRT												

Berdasarkan peta jalan (*roadmap*) SI/ TI GovCSIRT tersebut, dapat dijelaskan prioritas pada masing-masing strategi yang dapat dilakukan oleh pihak manajemen GovCSIRT sebagai berikut:

Strategi Aplikasi Baru

- Untuk tahun pertama, fokus pengembangan adalah pada sistem informasi yang berada di bagian *strategic* dan *key operational*, karena sistem informasi dalam bagian ini sangat vital untuk menjalankan aktivitas GovCSIRT. Sistem Informasi tersebut, yaitu: e-Aduan Keamanan Informasi yang dibutuhkan oleh konstituen untuk melaporkan terjadinya insiden kemanan informasi, Aplikasi Enkripsi dan Tanda tangan Digital dan Sistem Informasi Basis Data Kontak yang dibutuhkan oleh GovCSIRT dalam melakukan komunikasi, koordinasi dan kolaborasi.
- Selanjutnya pada tahun kedua, pengembangan sistem informasi *key operational* yang menjadi fokus pengembangan adalah *e-learning* dan SIM Hukum dan Investigasi. Hal ini disebabkan karena fungsi kedua aplikasi tersebut memiliki peran penting dan dibutuhkan dalam aktivitas organisasi. *E-learning* berfungsi sebagai acuan untuk edukasi mengenai keamanan informasi bagi konstituen GovCSIRT dan SIM Hukum dan Investigasi dibutuhkan GovCSIRT dalam melakukan fungsi penyidikan dan penindakan dari hasil analisis ancaman dan gangguan insiden keamanan informasi. Sementara itu, aplikasi sistem informasi yang bersifat *high potential*, yaitu *Knowledge Management* dikembangkan mulai pada kuartal keempat pada tahun kedua hingga memasuki tahun ketiga, karena prioritas aplikasi tersebut lebih rendah (kebutuhannya tidak mendesak) dibandingkan kedua aplikasi kategori *key operational* sebelumnya, namun aplikasi *knowledge management* memiliki kontribusi yang baik dan sangat berpotensi untuk mendukung dan menunjang kesuksesan kinerja GovCSIRT untuk mengelola informasi yang berasal dari serangkaian aktivitas-aktivitas GovCSIRT yang dapat dijadikan sebagai sumber pengetahuan untuk pembelajaran bagi GovCSIRT.
- Pada tahun ketiga, fokus pengembangan adalah pada sistem informasi yang berada di bagian *support,* yaitu *Content Management System*, karena prioritas aplikasi yang berada di bagian ini tergolong rendah. *Content Management System* berfungsi untuk mengelola konten data dan informasi pada Portal GovCSIRT guna mendukung fungsi GovCSIRT dalam mengedukasi konstituen dan menyosialisasikan keamanan informasi.

Strategi Pengembangan Aplikasi Lama

- Pada pengembangan Aplikasi Sistem Informasi lama, terdapat dua Sistem Informasi kategori strategis, yaitu PNS Box dan APRISMA, dan satu sistem informasi dengan kategori support. Ketiga sistem informasi tersebut merupakan sistem informasi yang telah lama dikembangkan oleh Direktorat Jenderal Aplikasi Informatika dan saat ini ketiga sistem informasi tersebut diperbaharui sesuai dengan kebutuhan GovCSIRT. Seperti halnya Portal GovCSIRT adalah pengembangan dari Portal APTIKA yang telah lama dikembangkan sebelum GovCSIRT dibentuk.
- Prioritas pengembangan sistem informasi untuk diperbaharui adalah pada kedua sistem informasi berkategori strategis, yaitu: APRISMA dan PNS Box. Hal ini disebabkan karena fungsi sistem informasi dinilai sangat vital bagi aktivitas GovCSIRT. Prioritas pengembangan selanjutnya adalah

pembaharuan Portal GovCSIRT. Sistem informasi yang sekarang ada masih sangat kaku dan belum berbasis layanan.

Strategi Infrastruktur TI

Pengembangan infrastruktur TI dimulai dengan mengintegrasikan infrastruktur TI yang digunakan GovCSIRT dengan infrastruktur Kementerian Kominfo secara keseluruhan. Sementara itu, kebijakan untuk menerapkan strategi *cloud computing* sudah merupakan komitmen Kementerian Kominfo untuk menerapkan kebijakan teknologi *cloud government*. Dalam hal ini, GovCSIRT dilibatkan mengingat GovCSIRT berwenang untuk mengawasi keamanan informasi Pemerintah. Prioritas strategi berikutnya adalah mengembangkan *Data Recovery Center* (DRC). Hal ini dipilih sebagai prioritas terakhir setelah kedua strategi sebelumnya dikarenakan DRC yang akan dikembangkan perlu menyesuaikan dengan strategi teknologi *cloud computing* yang dikembangkan.

Strategi Manajemen SI/ TI

Manajemen SI/ TI diterapkan dengan membuat kebijakan dan prosedur pemanfaatan SI/ TI. Hal ini dilakukan secara berkelanjutan mengingat kondisi SI/ TI yang selalu berkembang. Kebijakan dan prosedur tersebut dikembangkan oleh pihak manajemen menyesuaikan dengan standar yang berlaku pada organisasi. Kebijakan evaluasi tata kelola SI/ TI dilakukan secara berkesinambungan dengan penerapan kebijakan dan prosedur SI/ TI yang berlaku. Strategi menerapkan kebijakan dan prosedur serta melakukan evaluasi merupakan bagian dari strategi tata kelola SI/ TI pada GovCSIRT.

PENUTUP

Simpulan

Berdasarkan hasil analisis dan pembahasan mengenai perencanaan strategis Pusat Penanganan Insiden Keamanan Informasi Pemerintah yang telah dilakukan pada GovCSIRT, Direktorat Keamanan Informasi, Kementerian Kominfo, maka dapat diambil simpulan yaitu:

Penelitian ini memberikan usulan perencanaan strategis pembentukan Pusat Penanganan 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 infrastrutur 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.

Solusi kebutuhan sistem informasi berdasarkan hasil analisis terdapat tujuh sistem informasi baru yang harus dibangun yaitu *e-Aduan Keamanan Informasi, e-Monitoring, Content Management System, Knowledge Management, e-learning, Sistem Informasi Basis Data Kontak* dan *SIM Hukum*. Selain itu juga ada beberapa sistem yang perlu di modifikasi menyesuaikan dengan kebutuhan bisnis organisasi.

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.

Saran

Berdasarkan pembahasan pada Bab-bab sebelumnya, maka saran untuk penelitian selanjutnya, antara lain:

1. GovCSIRT Direktorat Keamanan Untuk memudahkan kinerja GovCSIRT, Direktorat Jenderal Aplikasi Informatika perlu mengeluarkan kebijakan/regulasi mengenai pembentukan tim khusus yang menangani insiden keamanan informasi pada masing-masing instansi Pemerintah baik Kementerian tingkat pusat maupun Pemerintahan Daerah.
2. GovCSIRT perlu menyusun standar prosedur operasi yang sesuai dengan penggunaan SI/TI sehingga visi dan misi perusahaan dapat dicapai.
3. 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. (2008). SNI 7512:2008. *Teknik keamanan - Pengelolaan insiden keamanan informasi*. Indonesia

Cassidy, A. (2006). *A Practical I Guide to information System Strategic Planning.* New York: Averbach Publication.

Depertemen Komunikasi dan Informatika. (2002). *Kerangka Konseptual Sistem Informasi Nasional.* Jakarta: Depkominfo.

Dewan TIK Nasional. (2007). *Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional.* Jakarta, Indonesia: Departemen Komunikasi & Informatika.

Kilcrece, G., Kossakowski, K. P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, USA: CMU Publisher.

Lederer, A. L., & Gardiner, V. (1992). *Strategic Information System Planning: The Method Approach. Information system Management*. (p. 13-20).

Puslitbang APTIKA & IKP. (2012). *Kajian Kesiapan Keamanan Informasi Pemerintah.* Jakarta: Balitbang SDM.

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

Ward, J., & Peppard, J. (2002). *Strategic Planning for Information system.* John Wiley.

Waterhouse, Price. (1996). *System Management Methodology: Strategic Information System Planning (SISP), Overview and Baseline version 2.1.* Price Waterhouse World Firm Services BV, Inc.

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

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