KAJIAN KESIAPAN KEAMANAN INFORMASI INSTANSI PEMERINTAH DALAM PENERAPAN *E-GOVERNMENT*

STUDY OF GOVERNMENT INFORMATION SECURITY READINESS IN IMPLEMENTING OF E-GOVERNMENT

Ahmad Budi Setiawan

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

Naskah diterima tanggal 4 Oktober 2013, direvisi tanggal 23 Oktober 2013, disetujui tanggal 18 November 2013

Abstract

This study aims to observe the readiness of Implementation Information Security Governance either in government agencies or regional ministerial level for the implementation of e-government. The analysis in this study was done by mapping the information security aspects of Indonesian e-Government Ranking index (index PeGI). The results of this study had concluded that using a framework of information security aspects index that is mapped to the Indonesian e-Govenment Ranking index is helpful to see the readiness of government information security.

***Keywords**: Information Security Governence, Readiness, Indexes KAMI, Indexes PeGI*

Abstrak

Kajian ini bertujuan untuk melihat tentang kesiapan penerapan Tata Kelola Keamanan Informasi pada instansi Pemerintah baik tingkat kementerian atau daerah dalam rangka implementasi *e-government*. Analisis dalam kajian ini dilakukan dengan memetakan aspek keamanan informasi terhadap indeks Pemeringkatan *e-Government* Indonesia. Hasil dari studi ini menyimpulkan bahwa dengan menggunakan kerangka kerja aspek pada indeks keamanan informasi yang dipetakan terhadap indeks Pemeringkatan *e-Government* Indonesia sangat membantu untuk melihat kondisi kesiapan keamanan informasi pada instansi pemerintah.

Kata Kunci: Tata Kelola Keamanan Informasi, Kesiapan, Indeks KAMI, Indeks PeGI

PENDAHULUAN

Latar Belakang

Internet merupakan sebuah media pertukaran informasi dan data yang terbuka, artinya internet dapat diakses oleh siapa saja, kapan saja dan darimana saja. Dengan berbagai kecanggihan sarana komunikasi modern tersebut, internet sangat rentan terhadap serangan sistem informasi. Tanpa adanya sistem keamanan terhadap informasi membuat sistem informasi yang dimiliki individu, organisasi bahkan instansi pemerintahan menjadi sangat rentan terhadap adanya upaya-upaya penyerangan sistem informasi[1].

Semakin tingginya nilai (*value*) internet bagi masyarakat, maka semakin tinggi juga resiko, ancaman serta gangguan terhadap sumber daya informasi maupun interaksi yang dilakukan antar pengguna. Ancaman terhadap sumber daya informasi dan interaksi antar pengguna pada dasarnya diakibatkan oleh berbagai kelemahan yang dieksploitasi oleh pelaku dengan tujuan menguasai/ mengambil alih aset yang bernilai tersebut. Kelemahan (*vulnerability*) dapat berupa *force majeur* (bencana alam dan kerusuhan) maupun kekurangan pada sistem dan kelalaian manusia di dalam mata rantai keamanan.

Saat ini, penggunaan TIK di lingkungan Penyelenggara Pelayanan Publik terus mengalami pertumbuhan, sejalan dengan kebutuhan penyediaan pelayanan publik yang cepat, andal dan aman. Penggunaan TIK yang makin kompleks dapat menyebabkan kerawanan dan ancaman Keamanan Informasi, yang meliputi aspek kerahasiaan, keutuhan, dan ketersediaan layanan, sehingga dapat mengganggu kinerja Penyelenggara Pelayanan Publik. Peran sumber daya informasi dan TIK semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi tata kelola pemerintahan yang baik (*Good Corporate Governence*)[2].

Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah berupa gangguan dan ancaman yang menyangkut aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*)[3]. Adanya ancaman terhadap sumber daya informasi tersebut membutuhkan adanya sebuah tata kelola keamanan informasi di setiap organisasi/ instansi tidak terkecuali instansi penyelenggara pelayanan publik milik pemerintah. Dengan demikian perlu ditingkatkan kesiapan dan kewaspadaan terhadap ancaman serangan keamanan informasi pada instansi pemerintah terutama pada infrastrutur kritis milik pemerintah.

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika telah menghimbau kepada seluruh instansi pemerintah terutama instansi pemerintah penyelenggara pelayanan publik dan instansi pemerintah yang memiliki infrastruktur vital untuk meningkatkan kesadaran akan pentingnya keamanan informasi. Himbauan kepada instansi pemerintah penyelenggara pelayanan publik, baik di lingkungan pusat maupun daerah dilakukan melalui berbagai cara, mulai dari sosialiasasi maupun bimbingan teknis (bimtek). Di samping itu, pemerintah juga telah mengeluarkan regulasi atau kebijakan yang terkait dengan penerapan tata kelola keamanan informasi dilingkungan instansi pemerintah. Regulasi atau kebijakan yang telah dikeluarkan tersebut baik berupa Undang-Undang, Surat Keputusan Menteri Komunikasi dan Informatika, Peraturan Menteri Komunikasi dan Informatika hingga Surat Edaran Menteri Komunikasi dan Informatika.

Sasaran regulasi, kebijakan dan upaya yang dilakukan pemerintah melalui Kementerian Komunikasi dan Informatika

tersebut adalah untuk terwujudnya penerapan tata kelola keamanan informasi di lingkungan instansi pemerintah baik tingkat pusat maupun daerah. Dalam menerapkan tata kelola keamanan informasi di lingkungan instansi pemerintah dibutuhkan kesiapan baik yang mencakup beberapa aspek, di antaranya; infrastruktur, perencanaan, dana/finansial dan kesiapan sumber daya manusia. Dengan demikian, kajian ini ditujukan untuk menggali dan mengevaluasi sejauh mana kesiapan instansi pemerintah untuk menerapkan tata kelola keamanan informasi. Adapun permasalahan dalam kajian ini adalah; *Bagaimana kesiapan keamanan informasi pada instansi pemerintah.*

Tinjauan Pustaka

Jumlah pengguna internet di Indonesia menempati urutan ke-4 terbesar di wiliyah Asia (*Internet World Stats*, 2011). Bergesernya kebutuhan masyarakat dari tradisional ke layanan data, mendorong meningkatnya jumlah pengguna internet. Tingginya penggunaan internet dan makin maraknya keterkaitan internet dengan kehidupan sehari-hari mengakibatkan frekuensi serangan serta kejahatan *Cyber* semakin meningkat. Kejahatan-kejahatan *Cyber,* atau yang dikenal dengan istilah *cybercrime,* dapat berupa pencurian data identitas (Sumber Daya Informasi), pembajakan *account* (*email*, IM, *social network*), penyebaran *malware* dan *malicious code*, *fraud,* s*pionase* industri, penyanderaan sumber daya informasi kritis, serta *cyberwarfare* atau perang dalam dunia maya. Sistem informasi yang terakses melalui internet sangat rentan terhadap adanya upaya-upaya penyerangan keamanan sistem informasi, seperti *Malicious Ware (Virus, Worm, Spyware, Key logger, Trojan, BotNet, etc), DOS, DDOS, Account Hijack, Spam, Phishing, Identity Theft, Web Defaced, Data Leakage/Theft, Web Transaction Attack, Misuse of IT Resources, Hacktivist, Cyber Espionage, Attack Control System, Cyber War, Country National Security*

Perspektif masyarakat tentang Teknologi Informasi dan Komunikasi telah bergeser dari Nilai Aset Bersih (NAB)[4] ke Nilai Aset Informasi. Dalam konteks keamanan informasi, informasi diartikan sebagai sebuah aset yang sangat bernilai dan harus dilindungi. Hal ini dapat bermakna bahwa informasi dalam sebuah perangkat PC atau infrastruktur TIK bahkan menjadi lebih berharga dari pada infrastruktur TIK tersebut secara fisik. Dengan demikian, hilang atau rusaknya sebuah informasi berharga dapat menyebabkan kerugian besar. Seiring dengan meningkatnya nilai aset informasi, maka semakin besar keinginan orang untuk mendapatkan akses ke informasi dan mengendalikannya. Maka muncullah individu atau kelompok yang menggunakan aset informasi demi berbagai tujuan dan mengerahkan segala upaya untuk mendapatkan aset informasi dengan berbagai cara.

Strategi keamanan informasi menentukan arah semua kegiatan keamanan informasi. Komponen regulasi dan kebijakan keamanan informasi adalah dokumen rencana tingkat tinggi dari keamanan informasi seluruh organisasi. Kebijakan berisi kerangka kerja untuk membuat keputusan spesifik, seperti rencana keamanan fisik dan administratif. ini merupakan rumusan untuk mengatasi permasalah Keamanan Informasi Nasional. Dengan adanya peraturan dan strategi maka akan mempertegas serta memperjelas cara untuk mengatasi permasalahan keamanan informasi.

Dalam penerapan TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Tujuan utama dari Tata Kelola keamanan informasi pada organisasi/ instansi pemerintah adalah untuk mengurangi dampak

yang merugikan instansi sampai pada tingkatan yang bisa diterima oleh instansi. Keamanan informasi mencakup semua jenis informasi, baik fisik dan elektronik. Pada implementasi sehari-hari dalam instansi, keamanan informasi melindungi semua aset informasi terhadap resiko kehilangan, pemutusan operasional, salah pemakaian, pemakai yang tidak berhak ataupun kerusakan informasi.

Tata Kelola Keamanan Informasi dalam sebuah korporasi atau organisasi apapun di aplikasikan dalam wujud sebuah sistem, yaitu ISMS (*information security management system*) atau Sistem Manajemen Keamanan Informasi. Konsep utama ISMS untuk suatu organisasi adalah untuk merancang, menerapkan, dan memelihara suatu rangkaian terpadu proses dan sistem untuk secara efektif mengelola keamanan informasi dan menjamin kerahasiaan, integritas, serta ketersediaan aset-aset informasi serta meminimalkan risiko keamanan informasi.

Komponen Kebijakan keamanan informasi yang tercakup dalam tata kelola keamanan informasi adalah arahan startegis dalam pelaksanaan manajemen risiko keamanan informasi pada sebuah organisasi. Kebijakan berisi kerangka kerja untuk membuat keputusan spesifik, seperti rencana keamanan fisik dan administratif. Strategi keamanan informasi akan menentukan arah semua kegiatan keamanan informasi. Dengan adanya peraturan dan strategi maka akan mempertegas serta memperjelas cara untuk mengatasi permasalahan keamanan informasi. Setiap elemen dalam mewujudkan kemanan informasi harus mengacu pada standar keamanan yang telah ditetapkan.

Setiap elemen harus mengacu pada standar keamanan yang telah ditetapkan dalam mewujudkan kemanan informasi. Standar keamanan informasi harus khusus dan spesifik sehingga mereka dapat diterapkan ke semua bidang keamanan informasi. Setiap negara perlu mengembangkan standar sesudah menganalisis standar keamanan administratif, fisik dan teknis yang banyak digunakan di dunia. Standar haruslah sesuai dengan lingkungan TIK yang umum.

Standar keamanan informasi harus khusus dan spesifik sehingga dapat diterapkan ke semua bidang keamanan informasi. Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang *Information Security Management Systems (ISMS)* atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan. Standar ISMS yang paling terkenal adalah ISO/IEC 27001 dan ISO/IEC 27002 serta standar-standar terkait yang diterbitkan bersama oleh ISO dan IEC. *Information Security Forum* juga menerbitkan suatu ISMS lain yang disebut *Standard of Good Practice* (SOGP) yang lebih berdasarkan praktik dari pengalaman mereka. Kerangka Manajemen Teknologi Informasi (TI) lain seperti COBIT dan ITIL juga menyentuh masalah-masalah keamanan walaupun lebih terarah pada kerangka Tata Kelola secara umum. Dari standar seri ISO 27000 hingga September 2011, standar ISO/IEC 27001: 2005 telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001: 2009. Pada struktur keseluruhan proses SMKI diterapkan model PLAN-DO-CHECK-ACT (PDCA).

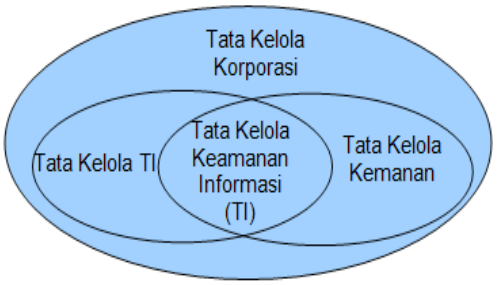
Dalam sebuah pelayanan publik yang diselenggarakan oleh pemerintah, TIK merupakan sebagai pendukung layanan agar layanan dapat disampaikan dengan efektif dan efisien. Hal ini dikemukakan dalam penelitian yang dilakukan oleh Saheer Al-Jaghoub, Hussein Al-Yaseen and Mouath Al-Hourani (Saheer, Hussein & Mouath, 2010) yang menyimpulkan bahwa TIK adalah instrument yang bermanfaat dan mampu meningkatkan efektivitas dan efisiensi layanan pemerintah. Meskipun demikian, dalam peneltian tersebut juga disampaikan mengenai munculnya isu-isu, seperti keamanan, privasi dan penerimaan menjadi hambatan dalam adopsi layanan *e-government*. Dengan demikian dibutuhkan

perhatian khusus mengenai hal tersebut dalam pengembangan *e-government*.

Terkait dengan kajian tentang kebijakan Tata Kelola Keamanan Informasi, dalam penelitian berikutnya yang dilakukan oleh Rossouw Von Solms, Kerry-Lynn Thomson, dan Prosecutor Mvikeli Maninjwa (Solms, Thomson, & Maninjwa, 2011), menyebutkan bahwa; Praktik Tata Kelola Keamanan Informasi yang komprehensif harus dilakukan oleh organisasi. Tata Kelola Keamanan Informasi terdiri dari kegiatan langsung dan kontrol yang harus dilakukan pada semua tingkat (level) manajemen, yaitu: tingkat strategis, taktis, dan operasional. Kebijakan yang berada di masing-masing tingkatan harus terwakili di Arsitektur Kebijakan Tata Kelola Keamanan Informasi atau yang dikenal dengan istilah *Information Security Policy Architecture (ISPA)* pada sebuah organisasi. Namun dalam banyak kasus, kebijakan tata kelola keamanan informasi tidak termasuk dalam kebijakan yang berada di tingkat operasional.

IT *Governance Institute* (ITGI, 2003) menunjukkan bahwa tata kelola TI berkaitan dengan penyampaian nilai TI bagi bisnis dan mitigasi risiko TI. Nilai TI didorong oleh keselarasan strategis TI dengan tujuan bisnis, mitigasi risiko TI disampaikan dengan menanamkan akuntabilitas ke dalam organisasi. Lebih lanjut lagi, menurut Tenver A. Zia (Zia, 2010), hal ini menyebabkan lima area fokus utama tata kelola TI. Dua di antaranya adalah hasil, yaitu: penyampaian nilai TI dan manajemen risiko. Tiga fokus lainnya adalah pendorong, antara lain: keselarasan strategis, manajemen sumber daya, dan manajemen kinerja. Dalam rangka untuk memberikan keamanan di layanan manajemen TI dan tata kelola TI, keselarasan strategis TI dan manajemen risiko harus ditangani dengan baik.

Meskipun ada banyak karakteristik untuk tata kelola keamanan TI, namun sulit untuk dikontekstualisasikan. *Best Practice* menyatakan bahwa tata kelola keamanan TI mendefinisikan inti prinsip-prinsip keamanan TI, akuntabilitas dan tindakan organisasi, untuk memastikan pencapaian tujuan. *Departement of Broadband, Communications and the Digital Economy*, Australia mendefinisikan Tata Kelola Keamanan Informasi sebagai penetapan dan penegakan budaya keamanan TI untuk memberikan jaminan bahwa tujuan bisnis dan persyaratan para *stakeholder* (pemangku kepentingan) akan perlindungan informasi terus dipenuhi (*Department of Broadband Communications, and the Digital Economy*- Australia, 2009).



Gambar 1. Konsep IT *Security Government*

Secara sederhana, tata kelola keamanan TI digunakan untuk memastikan bahwa semua fungsi keamanan manajemen TI dirancang, diimplementasikan dan beroperasi secara efektif. Seperti semua mekanisme tata kelola, tata kelola keamanan TI harus didorong oleh tingkat risiko untuk organisasi. Tata Kelola TI dan tata kelola keamanan mengandung sejumlah atribut yang sama dengan Tata Kelola Keamanan TI. Perbedaan fokus pada Tata Kelola TI dan Tata Kelola Keamanan menghasilkan kegiatan/aktivitas yang saling tumpang tindih, dan dengan perbedaan ini diyakini bahwa kerangka kerja Tata Kelola Keamanan TI tidak hanya didorong dari sudut pandang TI.

Penelitian lainnya yang dilakukan oleh Yi Han, Yoshiaki Hori, Kouichi Sakurai (Han, Hori, & Sakurai, 2008) menyebutkan bahwa evaluasi pra-Kebijakan keamanan Informasi berfokus pada evaluasi kebijakan keamanan sebelum kebijakan ditegakkan. Evaluasi kebijakan keamanan sebelum

penegakan bertujuan untuk menganalisis adanya kesenjangan. Dengan demikian, untuk mengisi kesenjangan tersebut, dilakukanlah evaluasi pra- kebijakan keamanan yang berfokus pada evaluasi kebijakan keamanan sebelum penegakan kebijakan. Sebagian besar penelitian berfokus pada evaluasi setelah kebijakan keamanan informasi. Evaluasi setelah kebijakan diterapkan memang sangat penting. Namun jika evaluasi pra-kebijakan diterapkan juga dilakukan, maka kinerja keamanan pasti akan terarah dan lebih baik.

Hal ini sejalan dengan penelitian yang dilakukan oleh Jean-Christophe Carbonel, CISA (Carbonel, 2008), yang menyebutkan bahwa untuk mengevaluasi dan mengukur tata kelola keamanan TI, sebuah evaluasi dengan *maturity* model (CMMI) adalah alat perbaikan yang baik, karena mengkristal ke dalam istilah yang mudah dipahami dan mudah untuk dilakukan tindakan praktis. Oleh karena itu, *maturity* model membantu untuk memahami dan menyebarluaskan konsep tersebut dengan memberi materi, dan menempatkan dalam jangkauan setiap manajer.

Metode Penelitian

Penelitian ini adalah penelitian evaluatif mengenai kesiapan penerapan tata kelola keamanan informasi dengan metode penelitian kualitatif. Tujuan penelitian ini adalah untuk menghasilkan sebuah rekomendasi terkait dengan keamanan informasi pada instansi pemerintah. Data yang digunakan untuk melihat kondisi keamanan informasi pemerintah saat ini adalah data hasil *assesment* indeks PeGI (Pemeringkatan *E-Government* Indonesia). Data pelengkap lainnya adalah data laporan insiden keamanan informasi dari ID-CERT dan data laporan monitoring insiden keamanan informasi dari Id-SIRTII. Adapun penjelasan masing-masing tahapan penelitian secara sistematis dijelaskan pada penjelasan berikut:

- Tahap 1, pendefinisian masalah dan tinjauan literatur. Pada tahap ini dilakukan untuk mempelajari berbagai teori yang relevan mencakup teori untuk mengkaji kesiapan keamanan informasi pemerintah.
- Tahap 2, pengumpulan dan analisis data. Setelah diperoleh model pengkajian yang cocok, dilakukan pengumpulan data berikut analisis data untuk mengetahui kondisi kesiapan keamanan informasi pada instansi pemerintah. Data lainnya yang dibutuhkan adalah data hasil assesment indeks PeGI (Pemeringkatan *E-Government* Indonesia). Data pelengkap lainnya adalah data laporan insiden keamanan informasi dari ID-CERT dan data laporan monitoring insiden keamanan informasi dari Id-SIRTII.
- Tahap 3, rekomendasi strategi peningkatan kesiapan keamanan informasi pada instansi pemerintah. Berdasarkan data kondisi tersebut dilakukan *gap analysis* dengan kondisi ideal, selanjutnya akan disusun strategi dan alternatif kebijakan peningkatan kesiapan keamanan informasi pemerintah.

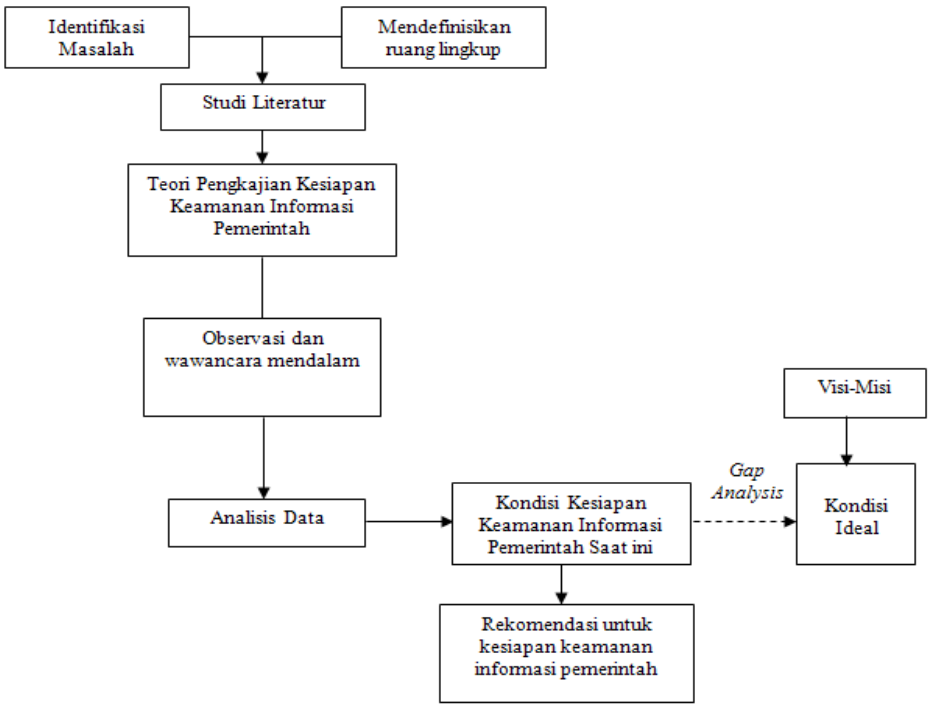
Dalam melakukan penelitian ini, data dikumpulkan dengan cara:

- Studi Literatur

  Studi literatur dilakukan untuk mempelajari berbagai dokumen/ referensi yang terkait dengan tema penelitian untuk dijadikan acuan.
- Wawancara pejabat pengelola dan *document review*

  Proses ini dilakukan untuk mendapatkan gambaran terkini/kondisi mengenai objek penelitian. Dalam penelitian ini, proses ini dilakukan juga untuk mengetahui visi-misi, strategi serta tujuan jangka panjang keamanan informasi pemerintah.
- Wawancara mendalam dengan pakar

Wawancara dengan pakar bertujuan untuk mendapatkan pandangan dari pakar secara teknis mengenai kondisi kesiapan keamanan informasi.



Gambar 2. Bagan Metodologi Penelitian

Analisis dan interpetasi data menggunakan metode analisis kualitatif. Teknik analisis ini dilakukan 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 mensintesanya (Bogdan & Biklen, 1982). Kemudian berdasarkan proses tersebut, ditemukan apa yang penting dan apa yang dapat dipelajari untuk menunjang keputusan. Survei pada Penelitian ini dilakukan di Kota Jakarta, Bandung dan Surabaya. Sebagai sumber data, Penelitian dilakukan dengan melibatkan instansi pusat, yaitu Direrktorat Keamanan Informasi dan Id-SIRTII. Adapun instansi daerah yang dilibatkan adalah Dinas Kominfo Prov. Jawa Barat dan Dinas Kominfo Prov. Jawa Timur.

HASIL DAN PEMBAHASAN

Tata Kelola Keamanan Informasi

Pemerintah Indonesia telah mengeluarkan Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik yang berisikan juga aspek keamanan informasi. Panduan ini mengacu pada SNI ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005. Standar tersebut berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI).

Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini dikembangkan dengan pendekatan

proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan peningkatan suatu SMKI. Pendekatan proses mendorong pengguna menekankan pentingnya:

1. Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
2. Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
3. Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
4. Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran

Indeks KAMI merupakan implementasi Kebijakan Penerapan Tata Kelola/ Sistem Manajemen Keamanan Informasi (SMKI) bagi Penyelenggara Sistem Elektronik untuk pelayanan publik. SMKI diterapkan dengan tujuan untuk manajemen resiko demi terciptanya tata kelola IT yang baik (*good IT Governence*). Indeks KAMI mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 11 area pengamanan sebagai berikut:

- Kebijakan keamanan informasi
- Organisasi keamanan informasi
- Manajemen aset
- Sumber daya manusia menyangkut keamanan informasi
- Keamanan fisik dan lingkungan
- Komunikasi dan manajemen operasi
- Akses kontrol
- Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
- Pengelolaan insiden keamanan informasi
- Manajemen kelangsungan usaha (*business continuity management*)
- Kepatuhan

Tabel 1. Cakupan Dokumen Kerangka Kerja Keamanan Informasi

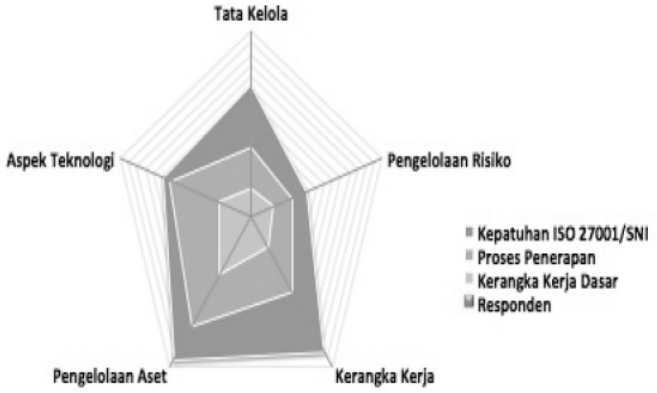
No	Nama Dokumen	Cakupan Dokumen
1	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal.
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggung jawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah
3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara intenal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.
4	Kebijakan Manajemen Risiko TIK	Berisi metodologi / ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.
5	Kerangka Kerja Manajemen kelangsungan Usaha (Business Continuity Management)	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana/k darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (*desktop/laptop/modem* atau email dan internet).

Dalam Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik yang dikeluarkan oleh Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika kontrol yang meliputi 11 area pengamanan tersebut disederhanakan untuk dijadikan cakupan dokumen yang pada umumnya dibangun sebagai kelengkapan kerangka kerja keamanan informasi. Cakupan tersebut antara lain dijelaskan pada Tabel 1.

Lebih lanjut, kondisi keamanan yang dievaluasi pada indeks KAMI meliputi 5 (lima) area berikut:

1. Tata Kelola Keamanan Informasi
2. Manajemen Risiko Keamanan Informasi
3. Kerangka Kerja Pengelolaan Keamanan Informasi
4. Pengelolaan Aset Informasi
5. Teknologi Keamanan Informasi

Indeks Keamanan Informasi (Indeks KAMI) merupakan sebuah test penjembatan untuk kepatuhan terhadap SNI ISO IEC 27001-2009. Indeks KAMI dimulai pada tahun 2011. Pelaksanaan pemeringkatan keamanan informasi pemerintah dengan Indeks KAMI pada tahun tersebut diutamakan untuk pemerintah pusat. Lima area evaluasi ini merupakan rangkuman kontrol-kontrol keamanan sebagaimana dijelaskan dalam ISO/ ISO 27001:2005 dengan mempertimbangkan karakteristik kondisi penerapan sistem manajemen keamanan informasi, khususnya instansi/lembaga penyelenggara pelayanan publik di Indonesia. Area evaluasi ini akan terus disempurnakan sesuai peningkatan kepedulian dan kematangan penerapan tata kelola keamanan informasi di lingkungan penyelenggara pelayanan publik.



Gambar 3. Diagram *Chart* Indeks KAMI

Pemetaan Aspek Keamanan Informasi ke Indeks PEGI

Hasil evaluasi indeks KAMI merupakan dokumen rahasia Negara yang tidak dapat disebar luaskan. Objek yang dievaluasi dalam indeks KAMI tidak menggambarkan keseluruhan kondisi keamanan informasi pada sebuah instansi Pemerintah baik pusat maupun daerah. Hal ini disebabkan oleh karena evaluasi diterapkan pada unit sebuah instansi yang memiliki Pelayanan Publik dengan memanfaatkan sistem infomasi. Dengan demikian, evaluasi indeks KAMI tidak dilakukan sepenuhnya pada instansi pemerintah.

Dalam kajian ini, untuk mendapatkan data mengenai kondisi kesiapan keamanan informasi pada pemerintah, digunakan data mentah yang diambil dari hasil Pemeringkatan *e-Government* Indonesia (PeGI). Data

pemeringkatan yang digunakan adalah data PeGI termutakhir, yaitu data PeGI tahun 2011. Hal ini didasarkan bahwa tata kelola keamanan informasi merupakan bagian dari tata kelola teknologi informasi secara keseluruhan.

Penilaian PeGI mengacu kepada Inpres 3/2003. Pada Inpres 3/2003, kebijakan merupakan pilar dari Kerangka Arsitektur *e-Government*, selain penataan sistem manajemen dan proses kerja, pemahaman tentang kebutuhan publik, dan pemapanan peraturan dan perundang-undangan. Indeks PeGI terdiri dari 5 (lima) dimensi dalam menilai penerapan *e-Government* pada instansi pemerintah dan dalam pemeringkatannya. Adapun kelima dimensi Pemeringkatan *e-Government* Indonesia (PeGI), adalah sebagai berikut

1. Kebijakan, aspek kebijakan dalam PeGI;
   - Proses Kebijakan: Pengelolaan kebijakan TIK yang baik
   - Visi dan Misi: Kebijakan yang memuat visi dan misi TIK
   - Strategi Penerapan: Strategi penerapan kebijakan TIK
   - Pedoman: Acuan-acuan untuk penerapan kebijakan TIK
   - Prosedur: Prosedur untuk menjalankan kebijakan TIK
   - Keputusan: Kebijakan terkait TI ditetapkan dengan keputusan menteri/ pimpinan lembaga/ kepala daerah
   - Skala Prioritas: Kebijakan TIK memuat prioritas implementasi TIK
   - Manajemen Risiko/ Evaluasi: Kebijakan untuk menerapkan manajemen risiko/evaluasi, baik oleh internal maupun pihak yang independen.
2. Kelembagaan, Peran-peran dalam Pengorganisasian Informasi dalam Kerangka Penyediaan Layanan terkait dengan keamanan informasi (manajemen risiko) menurut ITIL v3 yang diadopsi dalam PeGI;
   a. Pengelola Risiko; mengenali, menilai dan mengendalikan risiko termasuk melakukan analisis nilai dari aset, besaran ancaman terhadap aset-aset dan tingkat kerawanan setiap aset terhadap ancaman
   b. Pengelola Keamanan TI (*IT Security Manager*); memastikan terjaganya kerahasiaan, integritas dan ketersediaan dari aset-aset, informasi, data dan layanan TI
   c. Tim Insiden Besar (*Major Incident Team*); tim yang dibentuk khusus untuk menanggani insiden/ masalah yang besar bisa terdiri dari pimpinan dan tenaga ahli tertentu biasanya di bawah koordinasi dari manajer insiden (*incident manager*)
   d. Pengelola Insiden (*Incident Manager*); bertanggung jawab atas implementasi yang efektif dari keseluruhan proses manajemen insiden atau *incident management* serta bertugas menjalankan prosedur pelaporan melakukan eskalasi dari penangganan insiden, bila tidak dapat teratasi sesuai dengan tingkat layanan yang disepakati
   e. Pengelola Permasalahan (*Problem Manager*); bertanggung jawab pada pengendalian siklus penangganan masalah tujuan utamanya adalah mencegah terjadinya masalah dan meminimalisir dampak dari masalah yang tidak bisa dihindari dan mengumpulkan dan menyediakan informasi mengenai masalah masalah yang dikenal dan cara penangganannya
3. Infrastruktur, aspek yang dievaluasi dalam PeGI terkait dengan dimensi infrastruktur;
   - Ketersediaan infrastruktur (dalam spesifikasi dan jumlah yang sesuai dengan kebutuhan)
   - Kondisi infrastruktur (dalam kesiapan berfungsi sesuai dengan kebutuhan)

- Adanya penerapan tata kelola infrastruktur (inventarisasi, pengawasan, perawatan, tata cara pemanfaatan).

4. Aplikasi, dalam Kerangka Kerja PeGI, terdapat 10 (sepuluh) sub dimensi untuk Dimensi Aplikasi, yaitu: Situs (*home page*), Aplikasi fungsional pelayanan publik, Aplikasi fungsional administrasi dan manajemen umum, Aplikasi fungsional administrasi legislasi, Aplikasi fungsional manajemen pembangunan, Aplikasi fungsional manajemen keuangan, Aplikasi fungsional manajemen kepegawaian, Dokumentasi, Inventarisasi Aplikasi TIK, dan Interoperabilitas aplikasi
5. Perencanaan, aspek penilaian PeGI untuk dimensi perencanaan;
   a. Pengorganisasian/Fungsi, poin yang dievaluasi: Adanya unit/elemen dalam Pemerintah yang bertanggung jawab atas pengembangan Rencana Induk TIK dan Evaluasi terhadap Rencana Induk
   b. Mekanisme perencanaan *Master Plan* TIK, poin yang dievaluasi: Mekanisme penyusunan rencana TIK yang baku baku, kepatuhan terhadap mekanisme, dan keterlibatan stakeholders
   c. Dokumen *Master Plan*, poin yang dievaluasi: Adanya dokumen *Master Plan* yang lengkap, Pelaksanaan *Master Plan*, serta apakah *Master Plan* tersebut digunakan sebagai acuan implementasi TIK
   d. Implementasi *Master Plan* TIK, poin yang dievaluasi: *Master Plan* dijabarkan dalam rencana kerja yang lebih detil, dokumentasi rencana kerja detil dan evaluasi dan revisi rencana kerja *Master Plan*
   e. Pembiayaan, aspeknya yang dievaluasi antara lain: Unsur Pembiayaan dalam Dokumen RPJM atau RKPD, Kesesuaian jumlah pembiayaan dan Penyerapan anggaran pembiayaan

Kesiapan Keamanan Informasi Pemerintah Berdasarkan PeGI

Pelaksanaan PeGI merupakan kegiatan evaluasi terhadap pengembangan dan pemanfaatan TIK pada instansi-instansi pemerintahan pusat maupun daerah. Evaluasi didasarkan pada pelaksanaan dan kesiapan infrastruktur TIK pada instansi pemerintah yang dievaluasi. Evaluasi dilakukan dengan menilai peta kondisi pemanfaatan TIK yang disasarkan pada dimensi kebijakan, kelambagaan, infrastruktur, aplikasi dan perencanaan. Dalam kajian kesiapan keamanan informasi pemerintah ini, data PeGI yang digunakan adalah hasil PeGI termutakhir saat kajian ini dilakukan, yaitu PeGI tahun 2011. Pada Pemeringkatan *e-Government* Indonesia (PeGI), sistem pemberian peringkat (*rating*) untuk instansi pemerintah yang dilakukan *assessment* untuk masing-masing dimensi dan secara keseluruhan adalah sebagai berikut:

3,60 ≤ SANGAT BAIK ≤ 4,00

2,60 ≤ BAIK < 3,60

1,60 ≤ KURANG < 2,60

1,00 ≤ SANGAT KURANG < 1,60

Tabel 2. Data Hasil Evaluasi PeGI Tingkat Kementerian

No.	Departemen	Dimensi					Rata-rata	Kategori
		Kebijakan	Kelembagaan	Infrastruktur	Aplikasi	Perencanaan		
1	DEPDIKNAS	3.41	3.25	3.39	3.25	3.56	3.37	Baik
2	DEPKEU	3.25	3.47	3.57	3.38	2.92	3.32	Baik
3	DEP PU	3.29	3.13	3.05	3.46	3.58	3.30	Baik
4	DEPHAN	2.83	2.84	3.14	2.86	3.50	3.03	Baik
5	DEPPERIN	3.25	3.07	2.67	3.33	2.33	2.93	Baik
6	BAPPENAS	2.71	2.67	2.81	3.08	3.08	2.87	Baik
7	DEPNAKERTRANS	2.84	2.70	2.57	2.59	3.06	2.75	Baik
8	DEPSOS	2.83	2.80	3.05	3.00	1.92	2.72	Baik
9	DEP ESDM	2.46	3.07	2.57	2.92	2.50	2.70	Baik
10	KEMENEGRISTEK	2.54	2.60	2.86	3.42	2.08	2.70	Baik
11	DEPHUB	2.63	2.80	2.43	2.63	2.92	2.68	Baik
12	DEPKOMINFO	2.63	2.67	2.62	3.00	2.42	2.67	Baik
13	DEPKUMHAM	3.02	2.65	2.29	2.56	2.75	2.65	Baik
14	KEMENEG KOP UKM	2.25	2.60	2.62	3.00	2.08	2.51	Kurang
15	DEPTAN	2.42	2.60	2.67	2.56	2.17	2.48	Kurang
16	DEPDAG	1.93	2.08	2.69	2.80	2.40	2.38	Kurang
17	DEPKES	2.44	2.40	2.68	2.72	1.63	2.37	Kurang
18	DEPAG	2.29	2.47	2.33	3.08	1.58	2.35	Kurang
19	KEMENEG BUMN	1.58	2.00	2.24	3.38	1.92	2.22	Kurang
20	KEMENEG PAN	1.63	1.90	2.57	2.57	1.88	2.11	Kurang
21	KEMENEG KLH	1.83	2.13	2.51	1.89	1.83	2.04	Kurang
22	DEPBUDPAR	1.88	1.93	2.43	1.92	1.75	1.98	Kurang
23	DEPDAGRI	1.97	1.85	2.32	2.00	1.56	1.94	Kurang
24	DEPHUT	1.54	2.00	2.14	2.21	1.50	1.88	Kurang
25	KEMENEG PDT	1.50	1.53	1.81	2.15	2.00	1.80	Kurang
26	KEMENPERA	1.38	1.87	2.00	2.38	1.33	1.79	Kurang
27	KEMENPORA	1.54	2.07	1.57	1.88	1.58	1.73	Kurang
	Rata-rata	**2.37**	**2.49**	**2.58**	**2.74**	**2.29**	**2.49**	**Kurang**

Tabel 3. Data Hasil Evaluasi PeGI Tingkat Provinsi

No.	Provinsi	Dimensi					Nilai Rata-rata	Kategori
		Kebijakan	Kelembagaan	Infrastruktur	Aplikasi	Perencanaan		
1	Jawa Barat	2.96	3.40	3.33	2.97	3.20	3.17	Baik
2	Jawa Timur	2.96	3.20	3.00	3.00	3.33	3.10	Baik
3	D.I. Nanggroe Aceh Darusalam	2.96	3.13	2.95	2.87	2.80	2.94	Baik
4	DKI Jakarta	3.29	2.73	2.57	2.67	3.20	2.89	Baik
5	D.I. Yogyakarta	2.88	2.87	2.76	2.93	2.73	2.83	Baik
6	Sumatera Selatan	2.71	2.67	3.05	2.47	3.00	2.78	Baik
7	Jambi	2.63	2.53	2.43	2.47	3.00	2.61	Baik
8	Papua	2.75	2.53	2.81	2.30	2.13	2.50	Kurang
9	Kalimantan Barat	2.42	2.53	2.48	2.50	2.20	2.43	Kurang
10	Riau	2.17	2.33	2.14	2.23	1.93	2.16	Kurang
11	Sumatera Utara	1.88	2.40	2.29	2.13	2.07	2.15	Kurang
12	Jawa Tengah	1.71	2.40	2.38	2.33	1.53	2.07	Kurang
13	Kalimantan Timur	2.00	2.13	2.10	2.03	1.80	2.01	Kurang
14	Nusa Tenggara Barat	2.54	1.87	1.71	1.73	2.00	1.97	Kurang
15	Kalimantan Tengah	2.17	1.67	1.95	1.83	2.20	1.96	Kurang
16	Bali	2.33	2.40	2.00	1.93	1.13	1.96	Kurang
17	Lampung	1.96	2.27	1.67	1.87	1.60	1.87	Kurang
18	Kepulauan Bangka Belitung	2.08	2.13	1.29	1.50	2.20	1.84	Kurang
19	Bengkulu	1.67	2.07	1.43	1.50	1.33	1.60	Kurang
20	Nusa Tenggara Timur	1.67	1.60	1.48	1.70	1.40	1.57	Sangat Kurang
21	Sulawesi Barat	1.04	2.00	1.62	1.37	1.27	1.46	Sangat Kurang
22	Sumatera Barat	1.33	1.20	1.48	1.83	1.00	1.37	Sangat Kurang
23	Kepulauan Riau	1.25	1.67	1.00	1.43	1.40	1.35	Sangat Kurang
24	Sulawesi Tengah	1.08	1.53	1.33	1.03	1.00	1.19	Sangat Kurang
25	Sulawesi Selatan	1.04	1.07	1.00	1.00	1.00	1.02	Sangat Kurang
	RATA-RATA	2.14	2.25	2.09	2.06	2.02	2.11	Kurang

Penilaian Mengenai Kondisi Keamanan Informasi Pemerintah

Secara umum, kesiapan keamanan informasi pada instansi pemerintah baik pusat maupun daerah masih dinilai kurang memenuhi harapan. Walaupun demikian, ada beberapa instansi baik pusat maupun daerah yang sudah memiliki inisiatif yang baik dalam menerapkan tata kelola TI sebagai wujud implementasi tata kelola pemerintahan yang baik (*Good Governance*). Implementasi tersebut juga berdampak pada kesiapan keamaman informasi pemerintah. Penilaian pada instansi pemerintah tersebut antara lain pada aspek; perencanaan, kebijakan, kelembagaan dan infrastruktur.

Untuk aspek perencanaan, dengan melihat total skor kumulatif pada instansi pemerintahan tingkat pusat sebesar 2,29 dan

instansi pemerintahan daerah sebesar 2,02, memperlihatkan bahwa perencanaan sistem pada instansi pemerintah belum memiliki mekanisme perencanaan Master Plan TIK yang baik mencakup mekanisme implementasinya. Hal ini juga mencakup aspek pendanaan terhadap infrastruktur TIK untuk mendukung penerapan tata kelola TIK pada instansi pemerintah. Penilaian terhadap aspek tersebut juga memperlihatkan kurangnya kesiapan dalam perencanaan tata kelola TIK yang juga mencakup kesiapan keamanan informasi pemerintah.

Dalam hal kebijakan, total skor kumulatif pada instansi pemerintahan tingkat pusat sebesar 2,37 dan instansi pemerintahan daerah sebesar 2,14. nilai tersebut masih berada di bawah nilai rata-rata untuk kategori baik. Aspek ini mencakup penilaian yang meliputi adanya pedoman, prosedur dan strategi penerapan tata kelola TIK yang juga mencakup prosedur dan kebijakan untuk menerapkan manajemen risiko. Dengan total nilai rata-rata kumulatif pada aspek kebijakan tersebut, dapat disimpulkan bahwa masih banyak instansi pemerintah yang belum memiliki kesiapan pada aspek kebijakan untuk menerapakan tata kelola TIK yang baik dan tata kelola keamanan informasi.

Aspek kelembagaan mencakup penilaian terhadap adanya kelembagaan yang bertujuan untuk mengorganisir pengelolaan TIK termasuk dalam hal penanganan insiden keamanan informasi pada instansi pemerintah. Penilaian ini juga mencakup ketersediaan sumber daya manusia yang bertanggung jawab untuk mengelola sarana dan prasarana TIK pada instansi pemerintah berikut pengorganisiran tanggungjawab masing-masing pegawai. Hal ini berdampak pada pendelegasian tanggungjawab pengelolaan TIK termasuk dalam hal pengelolaan keamamanan informasi yang mencakup penanganan jika terjadi insiden keamanan informasi. Total nilai rata-rata kumulatif yang dicapai pada instansi pemeritahan pusat adalah sebesar 2,49 dan untuk pemerintah daerah sebesar 2, 25. Hal ini menunjukkan bahwa banyaknya instansi pemerintah pusat dan daerah yang belum menerapkan strategi kelembagaan untuk mengelola TIK termasuk keamanan TIK yang mencakup penanganan insiden keamanan informasi dengan baik.

Untuk aspek infrastruktur, masih banyak instansi pemerintah baik pusat maupun daerah yang perlu memperhatikan penerapan tata kelola infrastruktur TIK yang meliputi; inventarisasi, perawatan dan tata cara pemanfaatan. Ketersediaan infrastruktur, dalam hal spesifikasi dan jumlah yang sesuai dengan kebutuhan untuk menunjang kinerja masih kurang diperhatikan pada banyak instansi pemerintah baik pusat maupun daerah. Hal ini juga meliputi ketersediaan infrastruktur untuk kebutuhan pengamanan informasi yang belum diterapkan secara maksimal. Kondisi kesiapan ini tampak dengan capaian nilai rata-rata kumulatif untuk instansi pemerintah pusat sebesar 2,58 dan untuk pemerintah daerah sebesar 2,09.

Sebagai pelengkap dalam kajian ini, maka dilakukan wawancara mendalam yang melibatkan para pakar dibidang keamanan informasi sebagai proses penilaian pakar (*expert judgement*) untuk menilai kondisi kesiapan keamanan informasi pada instansi pemerintah. Berikut ini adalah rangkuman hasil penilaian pakar dalam menilai kondisi keamanan informasi pada instansi pemerintah;

Ir. Hogan Kusnadi, M.Sc, CISA, CISM, CISSP-ISSAP, SSCP:

- *Awareness* mengenai manajemen resiko/ tata kelola keamanan informasi pada instansi pemerintah umumnya berasal dari tingkat *operational* IT pada instansi pemerintah dan berjalan sudah cukup baik. Namun, dari sisi *governance* (tata pamong) masih besar gap yang ada antara *best practice* dengan yang sudah berjalan. Masalah IT dan *Information Security* pada instansi pemerintah cenderung dilepaskan ke pihak IT *Operational*.

IT masih dianggap sebagai bagian yang terpisah dari upaya pencapaian visi/misi organisasi

- Peran IT harus ditingkatkan baik secara struktur maupun kebijakan. Hal ini diperlukan agar kebijakan yang dikeluarkan dalam bidang TIK khususnya keamanan informasi dapat dijadikan landasan hukum yang kuat bagi instansi pemerintah baik pusat maupun daerah dalam menerapkan tata kelola TI dan tata kelola keamanan informasi. Dengan kelemahan sistem seperti itu, maka kesiapan instansi publik dalam menghadapi insiden keamanan informasi patut dipertanyakan.

Ir. Iwan Sumantri, CEH :

- Penerapan tata kelola keamanan informasi adalah bagian dari penerapan tata kelola TIK. Pemerintah pusat yang terkait dengan regulasi TIK Nasional, dalam hal ini adalah Kementerian Kominfo telah memberikan perhatian khusus terhadap permasalahan keamanan informasi terkait dengan banyaknya insiden keamanan informasi dan mengingat asset informasi pada instansi pemerintah adalah hal yang sangat penting.
- Kementerian Kominfo telah mensosialisasikan tentang kesadaran akan keamanan informasi (*information security awareness*) pada instansi pemerintah baik pusat maupun daerah dan mengeluarkan panduan tata kelola keamanan informasi bagi penyelenggara pelayanan publik.
- Sebagian besar pemerintah pusat maupun daerah sudah menerapkan Tata Kelola TIK, dengan kapasitas yang berbeda, sesuai dengan kondisi SDM dan dukungan Pimpinan**.** Kesiapan keamanan informasi pada instansi pemerintah pusat dan daerah sangat beragam dan terdapat berbagai kendala. Kendala yang umum adalah; SDM, Komitmen Pimpinan dan pendanaan (sistem anggaran yang sangat kaku)

Ir. Rinaldi Munir, MT :

- Keamanan informasi yang disinggung di dalam tata kelola hanya 3 aspek saja yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Menurut William Stalling, layanan keamanan juga meliputi: otentikasi (*authentication*), kontrol akses (*access control*), otorisasi, dan anti-penyangkalan (*non-repudiation*). Seharusnya semua layanan keamanan tercakup di dalam tata kelola itu.
- Keamanan informasi tidak hanya untuk data/informasi dalam bentuk digital, tetapi seharusnya juga mencakup data/ informasi dalam bentuk cetak/ *hard copy.*
- Model penerapan kebijakan keamanan informasi di tingkat nasional maupun daerah seharusnya tidak jauh berbeda karena insiden keamanan informasi dapat terjadi di mana saja. Hanya saja untuk tingkat pusat perlu model yang lebih kuat karena Instansi Pusat menyimpan informasi yang lebih strategis. Setiap instansi daerah yang terhubung dengan instansi pusatnya memiliki protokol keamanan informasi yang unik.
- Insiden keamanan informasi antara lain pencurian data penting (*hard copy* dan *soft copy*), penyadapan, penyalaghunaan *password*, pencurian PIN, *deface*, *phising*, serangan virus dan *worm*, *denial of services* (DOS), *distributed denial of service* (DDOS), penyalahgunaan *email*, pembajakan akun, *hacking*, dan lain-lain**.** Sebagian besar insiden keamanan informasi di dunia, termasuk di Indonesia, jarang dipublikasikan, sebab dapat memberikan "*negative publicity*" bagi instansi yang terkena serangan. Instansi memilih diam atau menyelesaikan sendiri masalah keamanan yang terjadi.

- Dari beberapa laporan insiden keamanan informasi yang dilaporkan ke ID-CERT dan Id-SIRTII, maka dapat disimpulkan bahwa penyedia layanan informasi di instansi pemerintah masih rentan terhadap serangan. Banyak situs web dan sistem *online* ketika dirancang tidak memperhitungkan aspek keamanan yang kuat sehingga sistem mudah dijebol. Masalah menjadi lebih berat karena instansi publik tidak punya standard prosedur *recovery* setiap terjadi insiden keamanan informasi, misalnya apa yang harus dilakukan, kemana dilaporkan, dan sebagainya.
- Dengan kelemahan sistem seperti itu, maka kesiapan instansi publik dalam menghadapi insiden keamanan informasi patut dipertanyakan.

DR. Ronny Wuisan, M.Kom :

- Hal terpenting dalam kaitan penerapan kemanan informasi adalah membangun kesadaran akan keamanan informasi. Selanjutnya adalah membuat prosedur dan kebijakan yang terkait dengan pengelolaan keamanan informasi. Setelah itu membuat kelembagaan kemanan informasi untuk dapat menerapkan tata kelola keamanan informasi.
- Dalam membuat kebijakan dan operasional secara teknis dalam hal penerapan tata kelola kemanan informasi pada instansi pemerintah, diharapkan pemerintah dapat merangkul pihak akademisi karena pihak akademisi memiliki banyak sumber daya manusia yang memahami dan mendalami permasalahan TIK dan keamanan informasi. Pihak akademisi akan memberikan telaahan dan masukan/ rekomenasi teknis serta dapat melakukan riset sebelum dan sesudah penerapan tata kelola keamanan informasi dilakukan.
- Pada tiap-tiap instansi pemerintah baik pusat maupun daerah perlu dibentuk penanggung jawab dalam hal tata kelola TIK, seperti CIO (*Chief Information Officer*) dan juga penanggung jawab yang khusus di bidang keamanan informasi, seperti CISO (*Chief Information Security Officer*)
- Pemerintah perlu membentuk struktur kelembagaan tim respon insiden seperti CERT khusus untuk instansi pemerintahan mulai dari tingkat pusat hingga instansi daerah untuk menangani adanya insiden keamanan informasi dan tim respon yang terbentuk dapat bekerjasama dengan CERT lainnya.

Dengan melihat hasil penilaian kesiapan keamanan informasi pemerintah berdasarkan pemetaan aspek keamanan informasi ke indeks PeGI, baik secara keseluruhan maupun untuk tiap-tiap aspek, secara umum terlihat bahwa umumnya instansi pemerintahan baik pusat maupun daerah kurang memenuhi standar penilaian. Dapat disimpulkan bahwa kondisi kesiapan keamanan informasi pada instansi pemerintah masih kurang memenuhi harapan dan belum siap menghadapi adanya ancaman insiden keamaman informasi. Walaupun demikian, beberapa instansi pemerintah baik pusat maupun daerah yang memiliki skor penilaian dengan kategori baik. Hal ini juga menunjukan instansi tersebut telah menerapkan tata kelola TIK mencakup tata kelola keamanan informasi dengan baik.

PENUTUP

Simpulan

Berdasarkan hasil kajian yang telah dilakukan, maka dapat diambil beberapa kesimpulan aspek tata kelola keamanan informasi adalah bagian dari lingkup tata kelola TIK secara umum. Dalam melihat kondisi kesiapan keamanan informasi pemerintah baik pusat maupun daerah dapat digunakan data PeGI yang dipetakan berdasarkan aspek keamanan informasi.

Sebagian besar instansi pemerintah baik pusat maupun daerah sudah menerapkan Tata Kelola TIK, namun dengan kapasitas yang berbeda dan sesuai dengan kondisi SDM yang tersedia dan adanya dukungan Pimpinan. Kendala yang umum pada penerapan tata kelaola TIK dan tata kelola keamanan informasi di lingkungan pemerintah adalah; SDM, Komitmen Pimpinan dan pendanaan (sistem anggaran yang sangat kaku).

Kebijakan, panduan dan sosialiasi terkait dengan keamanan informasi pada instansi pemerintah yang dilakukan oleh Kementerian Komunikasi dan Informatika melalui Direktorat Keamanan Informasi, Ditjen APTIKA saat ini belum mendatangkan hasil maksimal dengan belum diterapkannya tata kelola kelola keamanan informasi secara maksimal pada instansi pemerintah pusat maupun daerah. Hal ini didasarkan dari hasil evaluasi PeGI yang menyebutkan bahwa nilai total rata-rata PeGI pada instansi pusat maupun daerah adalah pada kategori "KURANG".

Saran

Adapun rekomendasi yang dapat diberikan sebagai hasil penelitian ini adalah dalam menerapkan tata kelola keamanan informasi dibutuhkan sebuah kesadaran, dasar / landasan hukum dan kebijakan yang cukup kuat, kelembagaan dan penanggung jawab, sumber pendanaan, ketersediaan infrastruktur dan teknologi yang digunakan, Sumber Daya Manusia (SDM) yang memahami TIK dan keamanan informasi serta komitmen pimpinan.

Pada setiap instansi pemerintah baik pusat maupun daerah perlu dibuat SK/ keputusan pimpinan instansi tersebut terkait dengan keamanan informasi sebagai dasar dan landasan untuk melakukan penerapan tata kelola keamanan informasi yang mengacu pada panduan dan kebijakan yang dikeluarkan oleh Kementerian Kominfo. Dasar hukum tersebut dapat dijadikan sebagai komitmen penerapan tata kelola keamanan informasi termasuk untuk mengatasi permasalahan/isu mengenai pendanaan.

Dalam hal pemberlakukan kebijakan khusus tentang keamanan informasi, direkomendasikan agar Surat Edaran Menteri Komunikasi dan Informatika Nomor: 5/ SE/M.KOMINFO/07/2011 tentang Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik yang memberikan panduan tentang penerapan tata kelola keamanan informasi bagi penyelenggara pelayanan publik untuk dinaikkan tingkatan hukumnya agar dapat dijadikan landasan/ dasar hukum yang kuat bagi setiap instansi pemerintah pusat maupun daerah.

Pada setiap instansi pemerintah baik pusat maupun daerah perlu memiliki BCP (*Business Continuity Plan*) dan DRP (*Disaster Recovery Plan*) sebagai standard prosedur *recovery* untuk mengantisipasi setiap terjadinya insiden keamanan informasi. Model ststus infrastruktur TIK yang sesuai dengan konsep pengamanan informasi juga perlu meninjau sisi ekonomi dan disesuaikan dengan kebutuhan organisasi karena diperlukan investasi yang besar.

Pada setiap instansi pemerintah baik pusat maupun daerah perlu memiliki mekanisme penanganan insiden keamanan informasi yang ditunjang dengan bentuk kelembagaan yang akan menangani insiden tersebut.

Untuk menunjang program dan kebijakan keamanan informasi, baik pemerintah pusat maupun daerah perlu membentuk peranan GCIO (*Government Chief Information Officer*) dan lebih spesifik lagi membentuk peranan GCISO (*Government Chief Information Security Officer*). Peranan GCISO dapat berada pada peran level koordinatif dan pelaksana.

DAFTAR PUSTAKA

Al-Jaghoub, S, Al-Yaseen, H., & Al-Hourani, M. (2010). "Evaluation of awareness and acceptability of using e- Government services in developing countries: the Case of Jordan" *The Electronic Journal Information Systems Evaluation Volume 13 Issue 1 2010, (pp1 - 8), available online at www.ejise.com*

Carbonel, J.-C. (2008). Assessing IT security governance through a maturity model and the definition of a governance profile. *Information System Control Journal, Vol.2, ISACA* , 4.

Department of Broadband Communications, and the Digital Economy- Australia. (2009). *CIO, CISO and Practitioner Guidance.* Australia: DBCDE Press.

Han, Y., Hori, Y., & Sakurai, K. (2008). Security Policy Pre-evaluation towards Risk Analysis. *International Conference on Information Security and Assurance* (hal. 415). IEEE.

OECD. (2008). *Building an institutional framework for Regulatory Impact Analysis, guidance for policy maker.* Paris: OECD Press.

Solms, R. V., Thomson, K.-L., & Maninjwa, M. (2011). Information security governance control through comprehensive policy architectures. *IEEE* .

Zia, T. A. (2010). An Analytical study of IT security governance and its adoption on Australian Organisations. *Australian information security management conference* (hal. 183). Perth: Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western.

Catatan Kaki:

1. Hogan Kusnadi, Seminar Studi Kelembagaan CERT Nasional, 17/11/2011
2. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kemkominfo. 2011
3. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik
4. Keamanan Jaringan dan Keamanan Informasi dan Privasi, Akademi Esensi TIK untuk Pimpinan Pemerintahan. Ditjen APTIKA, Kemkominfo dan UNESCAP/ APCICT 2009