Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis

Study of Critical Information Resources Infrastructure Security Strategy

Ahmad Budi Setiawan[1]
[1]*Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi Komunikasi publik*
Jl. Medan Merdeka Barat No.9 Jakarta 10110

INFORMASI ARTIKEL

Naskah diterima 5 Februari 2015
Direvisi 17 Maret 2015
Disetujui 20 Maret 2015

Keywords:
Critical Information Infrastructure Protection
Information Security
Information Security Management System

ABSTRACT

Critical information infrastructure is one of the critical infrastructure that combines telecommunications infrastructure and Internet networks used in the public service. Thus, the critical information infrastructure must operate safely and meet the aspects of information security. This study is a case study on critical information infrastructure as one of the critical national infrastructure used in public service. The critical information infrastructure which is used as a case study is in the field of electricity energy. The purpose of this sudy is to provide input on critical infrastructure security policy based on case studies conducted. This study was conducted with the combined quantitative and qualitative method that combines the results of the risk assessment on the research object with the opinion of policy makers, academics, experts and practitioners. These results are input to the policy framework and securing critical infrastructure, especially the ICT sector.

Kata kunci :
Infrastruktur Informasi Kritis
Proteksi
Keamanan Informasi
Sistem Manajemen Keamanan Informasi

ABSTRAK

Infrastruktur informasi kritis merupakan salah satu infrastruktur kritis yang menggabungkan antara infrastruktur telekomunikasi serta jaringan internet yang digunakan dalam pelayanan publik. Dengan demikian, infrastruktur informasi kritis harus beroperasi dengan aman dan memenuhi aspek keamanan informasi. Kajian ini adalah studi kasus pada infrastruktur informasi kritis sebagai salah satu infrastruktur kritis Nasional yang digunakan dalam pelayanan publik. Adapun infrastruktur informasi kritis yang dijadikan studi kasus adalah pada bidang energi ketenagalistrikan. Tujuan kajian ini adalah memberikan masukan pada kebijakan pengamanan infrastruktur kritis berdasarkan studi kasus yang dilakukan. Kajian ini dilakukan dengan metode gabungan kuantitatif dan kualitatif yang mengkombinasikan hasil penilaian risiko pada obyek riset dengan pendapat pengambil kebijakan, akademisi, pakar dan praktisi. Hasil kajian ini adalah masukan untuk kebijakan dan kerangka kerja pengamanan infrastruktur kritis khususnya sector TIK.

1. Pendahuluan

Perkembangan dan kemajuan Teknologi Komunikasi dan Informasi yang sedemikian pesat telah menyebabkan perubahan pola hidup manusia dalam berbagai bidang secara langsung maupun tidak langsung. Teknologi Internet saat ini telah dimanfaatkan oleh berbagai pihak baik pemerintah, akademisi, industri, institusi dan personal dalam mencari, mendapatkan, mengelola dan mengirimkan informasi. Nilai politik, ekonomi, sosial, budaya, pertahanan dan keamanan dari informasi yang berjalan pada infrastruktur internet saat ini sangat tinggi sehingga meningkatkan potensi ancaman dan gangguan pada pemanfaatan dari teknologi internet itu sendiri (Su, X., 2006).

Pada saat ini di Indonesia terjadi lebih dari satu juta serangan setiap harinya terhadap keamanan informasi, internet, seperti tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain, tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua pihak yang seharusnya berinteraksi, dan tindakan lain yang berpotensi untuk menghancurkan informasi yang berjalan di atas infrastruktur internet. Kasus-kasus terkait insiden terhadap keamanan internet telah marak terjadi di

Email : [1]ahma003@kominfo.go.id

DOI: 10.17933/bpostel.2015.130104

Indonesia dan mengancam langsung pada infrastruktur strategis di Indonesia. Kasus-kasus besar yang terjadi seperti *deface* Situs Pemilu 2004, pencurian identitas dan data (sumber daya informasi) serta pembajakan akun (email, IM, *social network*) yang kebanyakan dilakukan untuk tujuan penipuan, kejahatan *carding* (*credit card fraud*), ATM/EDC *skimming, hacking, cracking, p*hising (*internet banking fraud*), *malware* (virus/worm/trojan/bots), *cybersquatting*, pornografi, perjudian *online*, transnasional *crime*, seperti; perdagangan narkoba, mafia, terorisme, money laundering, *human trafficking*, *underground economy* yang saat ini marak terjadi khususnya di Asia Pasifik. Kasus pencurian data pada CityBank dan Sony Corporation membuka mata kita bahwa serangan semakin terorganisir dan terfokus menyerang sarana ekonomi (DoD, 2012).

Telah diamanatkan dalam Amandemen UUD 1945 bahwa setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia. Dalam melaksanakan amanat tersebut, pemerintah telah mengeluarkan Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi bahwa Penyelenggara Telekomunikasi wajib melakukan pengamanan dan perlindungan terhadap instalasi dalam jaringan telekomunikasi yang digunakan untuk penyelenggaraan telekomunikasi. Sedangkan dalam Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi, mewajibkan bahwa setiap jaringan telekomunikasi, sarana dan prasarana telekomunikasi harus dilengkapi dengan sarana pengamanan dan perlindungan agar terhindar dari gangguan telekomunikasi.

Untuk mendukung pemanfaatan jaringan telekomunikasi berbasis protokol internet yang relatif aman dari ancaman dan gangguan maka dibuatlah Peraturan Menteri Kominfo No. 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet dimana yang telah diubah terakhir dengan Peraturan Menteri Kominfo No. 24/PER/M.KOMINFO/11/2011 menunjuk ID-SIRTII untuk bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.

Keamanan terhadap infrastruktur Internet menjadi tugas dari setiap pihak yang memanfaatkan teknologi tersebut. Keamanan infrastruktur internet di satu pihak tergantung dari keamanan infrastruktur internet di pihak lain. Kerjasama dan koordinasi mutlak diperlukan baik antara penyelenggara telekomunikasi, pengelola dan pengguna dari teknologi itu sendiri untuk bersama-sama meningkatkan keamanan pada infrastruktur internetnya. Pola komunikasi yang baik mutlak diperlukan dalam rangka baik pencegahan terhadap ancaman dan gangguan dan juga penanggulangan terhadap insiden yang terjadi dengan tujuan agar informasi yang berjalan di atas infrastruktur internet dapat terlindungi dengan baik.

Keamanan Infrastruktur Sumber Daya Informasi Kritis Nasional merupakan prasyarat mutlak yang harus diimplementasikan agar dapat menjamin efektivitas keandalan, ketersediaan dan integritas jaringan informasi, baik secara nasional maupun global (Henderson, 2007). Namun demikian, dampak besar dan potensi gangguan serta ancaman terhadap keamanan infrastruktur kritis nasional masih belum disadari sepenuhnya oleh masyarakat. Hal ini tampak dari belum tersedianya kebijakan Proteksi Infarastruktur Informasi Kritis Nasional dan belum dipetakan/diklasifikasikannya Infrastruktur Kritis Nasional, khususnya infrastruktur jaringan informasi.

Secara umum, infrastruktur kritis adalah layanan vital yang jika tidak berfungsi selayaknya akan menimbulkan kelumpuhan ekonomi kerusakan yang amat besar, kekacauan atau huru hara, bahkan kematian. Termasuk diantarnya adalah listrik, air, telekomunikasi, internet, transportasi, keuangan, distribusi minyak, gas dan bahan pangan, pertahanan nasional, layanan pemerintah, dan kesehatan. Fungsi perekonomian dan masyarakat semakin bergantung pada sistem informasi dan jaringan yang saling berhubungan dan saling tergantung, baik di dalam negeri dan lintas batas sektoral. Sejumlah sistem-sistem dan jaringan yang sangat penting nasional dan bahwa perlindungan infrastruktur informasi yang kritis merupakan prioritas bagi kebijakan nasional maupun dalam kerjasama internasional. Perusakan terhadap keamanan informasi pada infrastruktur kritis dapat mengakibatkan dampak besar terhadap perekonomian (Ko & Dorantes, 2006). Dengan demikian permasalahan yang akan dibahas dalam kajian ini adalah;

Bagaimanakah strategi penerapan kebijakan pengamanan Infrastruktur Sumber Daya Informasi kritis di Indonesia?

2. Tinjauan Pustaka

2.1. Proteksi Infrastruktur Informasi Kritis

Infrastruktur kritis atau vital adalah sekumpulan sistem yang menyediakan sumber daya yang menjadi semua fungsi masyarakat bergantung. Contohnya adalah telekomunikasi, informasi penting sebuah negara, transportasi, energi, air bersih, pelayanan kesehatan, pelayanan darurat, manufaktur dan jasa keuangan. Sementara itu, *Organisation for Economic Co-Operation and Development* (OECD) mendefinisikan sebuah Infrastruktur Informasi Kritis atau *Critical Information Infrastructure* adalah sekumpulan sistem informasi yang saling berhubungan dan sistem jaringan informasi/komputerisasi, dimana apabila terjadi gangguan atau kehancuran pada sistem tersebut akan memiliki dampak serius pada kesehatan, keselamatan, keamanan, atau kesejahteraan ekonomi masyarakat, atau pada fungsi efektif pemerintah atau perekonomian (OECD, 2008).

Infrastruktur informasi kritis Nasional dapat diidentifikasi melalui proses penilaian risiko dan biasanya mencakup satu atau lebih hal berikut:

- Komponen Informasi pendukung infrastruktur kritis, dan / atau
- infrastruktur informasi yang mendukung komponen penting dari bisnis pemerintah; dan / atau
- infrastruktur informasi penting untuk perekonomian nasional.

Proteksi terhadap Infrastruktur Informasi Kritis atau dikenal dengan istilah *Critical Information Infrastructure Protection* (CIIP) secara umum dikenal sebagai komponen vital dari sebuah kebijakan keamanan informasi nasional (Suter, 2007). Dalam hal proteksi terhadap infrastruktur kritis, beberapa Negara telah mengembangkan sistem dan organisasi CIIP yang modern dan komprehensif. Kerangka Perlindungan Infrastruktur Informasi Kritis Nasional atau lebih lanjut disepakati dengan istilah CIIP memberikan pandangan terstruktur layanan informasi strategis dan sumber daya infrastruktur untuk negara bangsa. Kerangka kerja ini juga berfungsi sebagai lensa umum dari yang untuk melihat risiko, ancaman, kerentanan, dan kontrol pelindung sumber daya tersebut.

Rencana untuk respon nasional dan perlindungan infrastruktur menentukan proses manajemen risiko dan memiliki potensi untuk menciptakan efek menstabilkan baik domestik maupun internasional. Mengingat berbagai aspek yang berafiliasi dengan CIIP, *International Telecomunication Union* (ITU) memperkenalkan Empat Pilar Model CIIP yang merupakan langkah strategis CIIP (Suter, 2007).

Gambar 1. Empat Pilar Model CIIP

Langkah pertama dalam pengembangan organisasi pengamanan infrastruktur informasi kritis yang efektif dan efisien adalah dengan menentukan prioritas dan tanggung jawab yang penting. Tugas-tugas

penting dari CIIP disusun dalam Empat Pilar-Model CIIP. Empat pilar dari model ini adalah: pencegahan dan peringatan dini (*prevention and early warning*); deteksi (*detection*); reaksi (*reaction*); dan manajemen krisis (*crisis management*).

2.2. NISTIR *Framework for Critical Infrastructure*

National Institute of Standards and Technology – Interagency Report (NSTIR) adalah sebuah pedoman kerangka kerja (*framework*) mengenai *cyber security* untuk membantu pemerintah dan industri dalam memenuhi tanggung jawab yang penting terkait infrasturktur kritis. Laporan terbaru disusun oleh Kelompok Kerja Keamanan Dunia Maya, *Cyber Security Working Group (CSWG)* dari *Smart Grid Interoperability Panel*, sebuah kemitraan publik-swasta yang diluncurkan oleh NIST dengan Departemen Energi, AS. Selanjutnya, pedoman yang dikeluarkan oleh NIST tersebut dikenal dengan NISTIR 7628 (NIST, 2007).

Kerangka kerja NISTIR 7628 merupakan output utama dari koordinasi kelompok kerja pada NIST tersebut, sebagai upaya untuk mengidentifikasi dan mengembangkan standar yang dibutuhkan untuk mengkonversi *smart grid* menjadi infrastruktur kritis, dalam kemajuan teknologi digital dengan kemampuan dua arah untuk mengkomunikasikan informasi, pengendalian peralatan dan mendistribusikan energi (NIST, 2014).

Meskipun dibuat oleh kelompok kerja *Smart Grid*, namun kerangka kerja NISTIR 7628 juga dapat diimplementasikan pada infrastruktur kritis lainnya. Pada panduan tersebut juga menyediakan latar belakang teknis dan detail yang dapat menginformasikan upaya-upaya organisasi untuk aman menerapkan teknologi *smart grid*. Memberikan dasar teknis untuk utilitas, produsen *hardware* dan *software*, penyedia layanan manajemen energi, dan lain-lain untuk membangun implementasi. Setiap organisasi persyaratan keamanan cyber harus berkembang sebagai kemajuan teknologi dan ancaman baru untuk keamanan grid muncul. Laporan ini merekomendasikan pelaksanaan berbagai tingkat keamanan.

2.3. Manajemen Keamanan Informasi

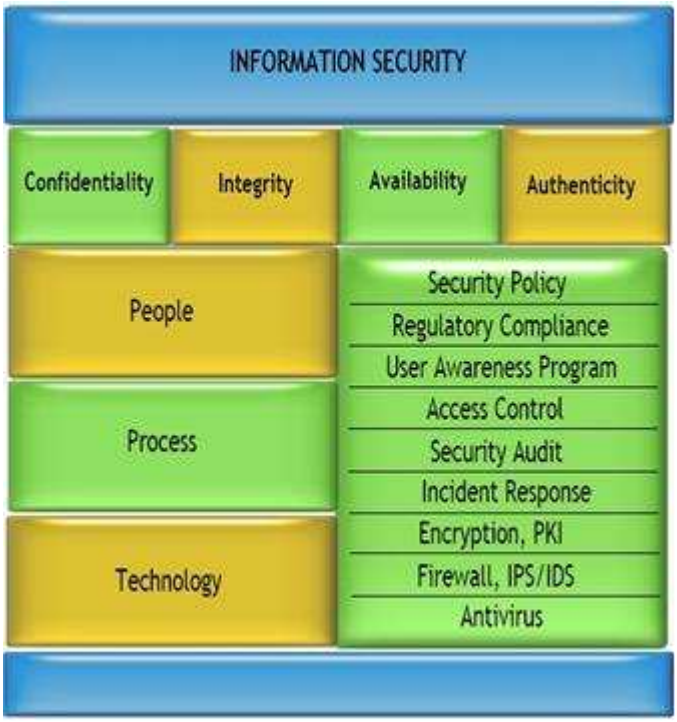
Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur penting. Sebab data/informasi adalah aset bagi perusahaan tersebut. Keamanan data/informasi secara langsung maupun tidak langsung dapat mempertahankan kelangsungan bisnis, mengurangi resiko, mengoptimalkan *return of investment* dan bahkan memberikan peluang bisnis semakin besar. Semakin banyak informasi perusahaan yang disimpan, dikelola dan digunakan secara bersama, akan semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data/informasi ke pihak lain yang tidak berhak.

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

1 *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2 *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3 *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).
4 *Autneticity* (keotentikan) aspek yang menjamin bahwa data atau informasi tidak dapat disangkal (non-repudiation) oleh pihak lain yang tidak memiliki wewenang.

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak. Dalam strategi implementasi, manajemen Keamanan Informasi juga tidak terlepas dari 3

(tiga) ruang lingkup implementasi keamanan informasi, yaitu; Sumber Daya Manusia (*people*), Proses (*process*), dan Teknologi (*technology*). Keempat aspek keamanan informasi dan ruang lingkup keamanan informasi tersebut dijelaskan dalam bagan pada Gambar 2 berikut ini;

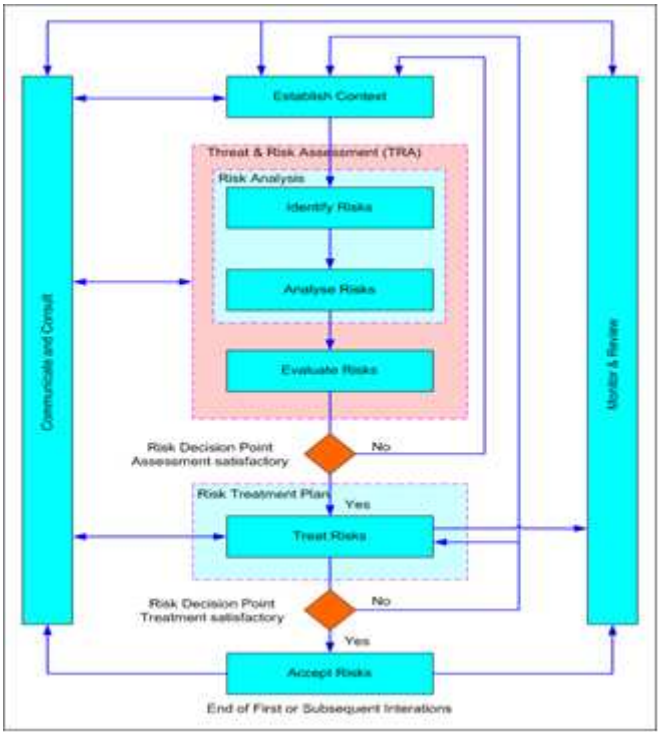


Gambar 2. Manajemen Keamanan Informasi

Secara teknis, Untuk menangkal kejahatan tersebut antara lain dibutuhkan tindakan pengamanan seperti kriptografi, guna melindungi data (enkripsi terhadap database dan storage), *communication protection* (SSL, SSH, dan VPN), *mail protection* (PGP, SMIME), *identity and transaction protection* (CA, PKI, authentification, non repudiation). Untuk memastikan bahwa infrastruktur TI telah aman dari berbagai ancaman dan serangan yang merugikan, maka diperlukan tata kelola keamanan informasi yang baik terkait dengan pemanfaatan TIK. Standard an Tata kelola keamanan informasi secara umum mengadopsi pada kerangka kerja Tata Kelola TI dari COBIT dan ISMS dari ISO/IEC 27001 dan ISO/IEC 27002. ISO/IEC 27001:2005 merupakan standard keamanan informasi yang diterbitkan *International Organization for Standarization* dan *International Electrotecnical Comission* pada bulan Oktober 2005 untuk menggantikan standard BS7799-2. Standard ini 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.

2.4. Kerangka Kerja ISO 31000, ISO 31010

ISO 31000 adalah suatu standar implementasi manajemen risiko yang diterbitkan oleh *International Organization for Standardization* pada tanggal 13 November 2009, merupakan pengembangan standar AS/NZS 4360:2004 yang dikeluarkan oleh *Australian Standards*. Standar ini ditujukan untuk dapat diterapkan dan disesuaikan untuk semua jenis organisasi dengan memberikan struktur dan pedoman yang berlaku generik terhadap semua operasi yang terkait dengan manajemen risiko. Berikut adalah alur proses manajemen risiko yang akan dilakukan dengan mengadaptasi ISO31000:



Gambar 3. Kerangka Kerja Proses Manajemen Risiko

ISO/IEC 31010:2009 *Risk management-Risk assessment techniques* adalah standar pendukung untuk ISO 31000 dan memberikan pedoman untuk pemilihan dan penerapan teknik sistematis untuk menilai/melakukan assessment risiko. Versi pertama standar ini diterbitkan pada bulan November 2009.

ISO 31000 memuat prinsip-prinsip dan kerangka kerja serta proses untuk mengelola segala faktor risiko secara transparan, sistematis dan kredibel. Melalui manajemen risiko berbasis ISO 31000:2009 perusahaan dapat mengembangkan, melaksanakan dan meningkatkan kinerja manajemen risiko perusahaan sebagai bagian integral dari sistem manajemen perusahaan. ISO 31000:2009 dapat diterapkan untuk setiap jenis organisasi, baik publik, swasta, komunitas, asosiasi, kelompok atau perorangan.

2.5. Penelitian yang Pernah Dilakukan

Penelitian yang pernah dilakukan dan relevan sebagai pembanding dalam penelitian ini, yaitu :

1 Penelitian yang dilakukan oleh Sean P. Gorman, Laurie Schintler, Raj Kulkarni, dan Roger Stough dengan judul penelitian "*The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure*", Tahun 2004 (Gorman, schintler, Kulkarni, Stough, 2004). Penelitian tersebut bertujuan untuk menganalisis dampak serangan yang ditujukan terhadap infrastruktur kritis pada sector telekomunikasi seiring adanya peningkatan permasalahan keamanan pada Negara Amerika Serikat paska tragedi 11 September 2011. Analisis dalam penelitian tersebut mencakup perbandingan metode yang digunakan dalam analisis kerentanan dengan metode spasial yang dibangun dengan menggabungkan variabel regional dan jarak. Hasil analisis penelitian tersebut dimanfaatkan dalam konteks mengevaluasi keamanan nasional dan regional dan dampak ekonomi jika terjadinya serangan terhadap CIIP sector telekomunikasi.

2 Penelitian berikutnya adalah yang dilakukan oleh Myriam Dunn (Dunn, 2005). Judul penelitian tesebut adalah "*The socio-political dimensions of critical information infrastructure protection* (CIIP)". Penelitian tersebut membahas mengenai perlindungan infrastruktur kritis dari segi social-polotik dan ekonomi. Dalam penelitian tersebut diperlihatkan perbandingan kebijakan perlindungan infrastruktur kritis di beberapa organisasi dan juga Negara. Hasil penelitian tersebut menyebutkan bahwa

perlindungan yang efektif untuk infrastruktur kritis yang mengancaman secara holistik dan strategis adalah dengan melalui penilaian risiko di tingkat fisik, virtual, dan psikologis sebagai dasar untuk perlindungan dan kelangsungan hidup strategi yang komprehensif. Dengan demikian akan membutuhkan agenda R & D komprehensif dan interdisipliner yang benar-benar meliputi segala bidang ilmu mulai dari teknik, dan ilmu lainnya, seperrti kebijakan, ilmu politik, dan social.

3 Penelitian lainnya adalah yang dilakukan oleh Eugene Nickolov (Nickolov, 2005). Penelitian tersebut memberikan penjelasan singkat mengenai infrastruktur informasi kritis dan menganalisis sejauh mana organisasi dapat tergantung pada berfungsinya infrastruktur kritis tersbeut, seperti pada organisasi perbankan dan jasa keuangan, listrik, bahan bakar dan jaringan pasokan air, serta jaringan informasi dan telekomunikasi. Konsekuensi dari serangan terhadap unsur-unsur tertentu dari infrastruktur tersebut diperiksa, serta inisiatif dan masalah yang timbul dengan perlindungan mereka di tingkat nasional dan internasional.

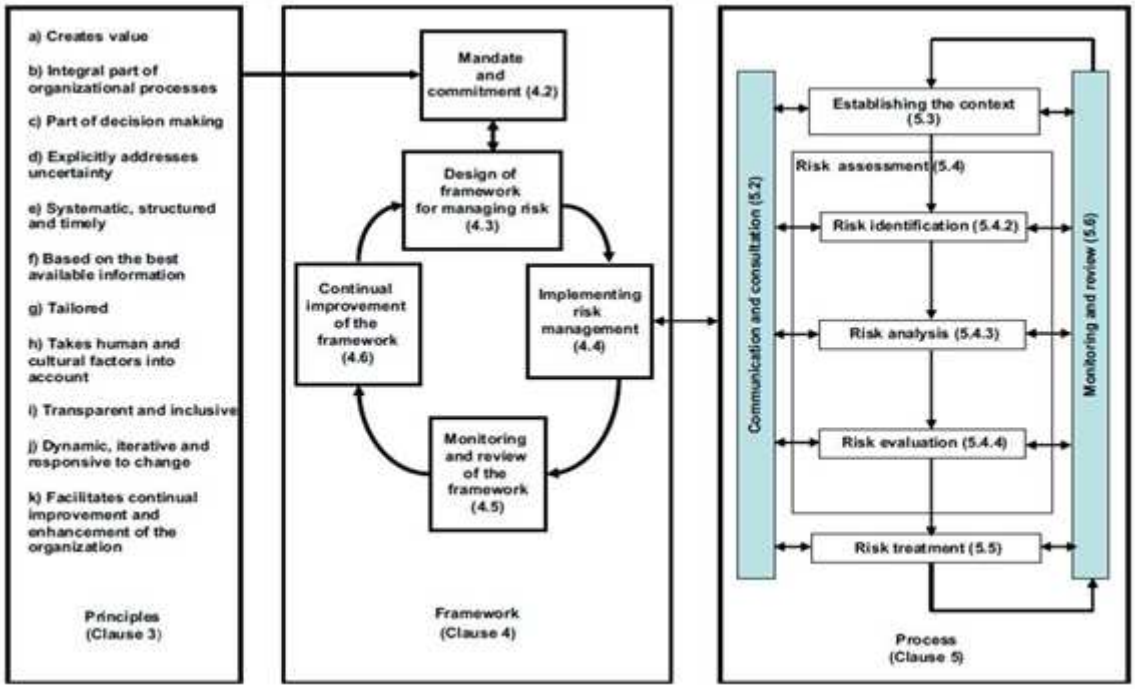
2.6. Kerangka Kerja Penelitian

Kerangka kerja ISO 31000 mencerminkan lingkaran Plan, Do, Check, Act (PDCA), yang biasa dikenal dalam seluruh desain sistem manajemen. Standar menyatakan bahwa "Kerangka kerja tidak ditujukan atau diintensikan untuk menentukan suatu sistem manajemen, tetapi lebih pada suatu usaha atau sarana untuk membantu organisasi untuk mengintegrasikan manajemen risiko kepada keseluruhan sistem manajemen risiko." Pernyataan ini hendak mendorong organisasi untuk lebih fleksibel dalam mengimplementasikan elemen dari kerangka kerja yang dibutuhkan.

Ada dua komponen utama dalam proses manajemen risiko dalam standar ISO 31000, yaitu:

1 Kerangka kerja, yang memandu organisasi untuk memahami keseluruhan struktur dan cara kerja dari manajemen risiko suatu organisasi

2 Proses, yang menjelaskan metode aktual dalam mengidentifikasi, menganalisa, dan mengelola risiko.



Gambar 4. Skema Kerangka Kerja Penelitian berdasarkan Metode Risk Manajemen ISO 31000

Berdasarkan kerangka kerja tersebut, Proses Manajemen Risiko terdiri dari beberapa tahapan, yaitu:

a Tahap I, Penentuan Konteks

Tahap I ini bertujuan untuk melakukan identifikasi permasalahan, menetukan *scope* (ruang lingkup) obyek permasalahan.

b Tahap II, *Risk Assessment*
Tahap II merupakan tahapan identifikasi risiko, baik risiko inherent maupun risiko residual; Analisis risiko, yang mencakup pemetaan risiko, penghitungan *likelihood* untuk melihat risiko mana saja yang *critical* dan *non critical*; dan evaluasi risiko.

c Tahap III, *Risk Treatment*
Tahap ini merupakan proses penentuan respon terhadap risiko yang ada. Selanjutnya respon-respon yang diidentifikasi, di-filter untuk menentukan respon yang tepat sesuai konteks dan penentuan control yang digunakan.

d Tahap IV, *Communication and Consultation*
Tahap ini dilakukan untuk menjaga kesesuaian manajemen proses bisnis dengan tujuan dan sasaran strategic.

e Tahap V*, Monitoring and Review*
Pada tahap ini dirancang mekanisme *monitoring* dalam implementasi manajemen risiko.

3. Metode Penelitian

3.1. Pendekatan Kajian

Kajian ini dilakukan secara kualitatif dan dengan menggunakan pendekatan Manajemen Risiko berdasarkan ISO 31000. Proses pengelolaan risiko menurut ISO 31000 seharusnya merupakan bagian yang terintegrasi, melekat dalam budaya dan praktik manajemen, dan terkustomisasi menurut proses bisnis organisasi. Menurut ISO 31000, asesmen risiko merupakan bagian yang paling penting dan fundamental dalam proses pengelolaan risiko. ISO 31000 menyediakan kerangka kerja sebagai pedoman dalam implementasi manajemen risiko yang efektif.

Tujuan dari kerangka kerja implementasi pengelolaan risiko antara lain:

1. Pemastian bahwa informasi mengenai pengelolaan risiko yang dihasilkan dari proses pengelolaan risiko telah cukup dilaporkan dan digunakan sebagai dasar dalam pengambilan keputusan
2. Pemenuhan akuntabilitas pada setiap tingkatan organisasi yang relevan

Objek yang dijadikan sebagai kajian adalah pengelolaan infrastruktur informasi kritis pada perusahaan pembangkit tenaga listrik, PT. PLN (Persero) Pembangkit Jawa Bali. Dalam pelaksanaan kajian, dilakukan wawancara mendalam dengan pihak pengelola berikut penilaian risiko dan juga dilakukan penilaian pakar (*expert judgement*).

3.2. Tahapan Pengkajian

Mengacu pada kerangka kerja Proses Manajemen Resiko, agar kajian dapat dilakukan dengan sistematis maka disusunlah tahapan pengkajian yang merupakan perwujudan dari alur pemikiran dari tahap definisi masalah, analisa solusi hingga rencana perancangan, secara detail alur pengerjaan kajian dijelaskan di bawah ini.

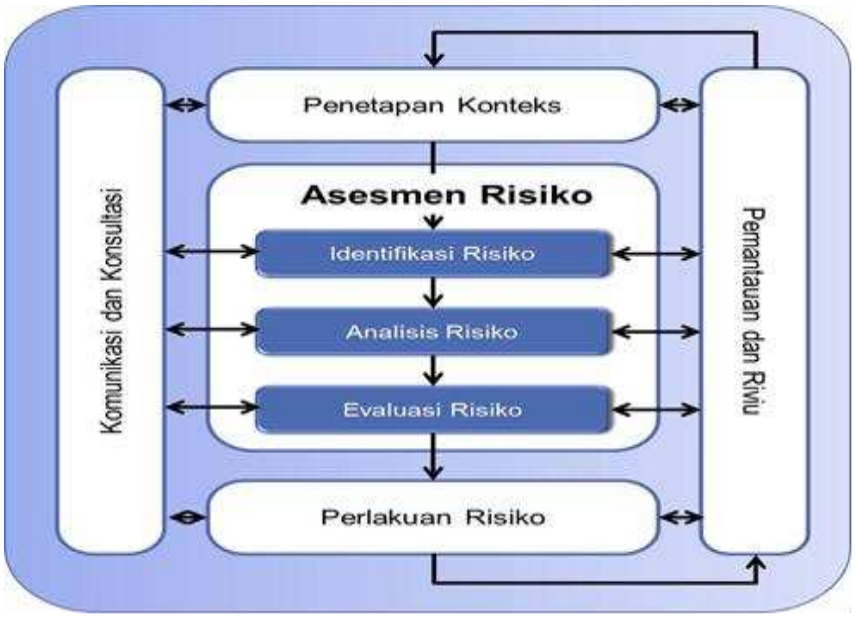
a Penetapan konteks.
Proses tersebut dimulai dengan pendefinisian masalah penelitian, menentukan ruang lingkup dan dapat mencakup pembuatan konsep awal yang melibatkan obyek penelitian.

b Intervensi.
Proses perencanaan, pembangunan dan pengambilan tindakan untuk membuat suatu konstruksi, model, metode, purwarupa (*prototype*) atau sumber daya lainnya.

c Penilaian Risiko .
Proses penilaian risiko dilakukan dengan pengamatan dan pengukuran tingkat tingkatan risiko yang mungkin terjadi pada infrastruktur kritis. Proses ini merupakan validasi model atau rancangan yang dihasilkan dengan cara *deep interview* dan melakukan *Focus Group Discussion* dengan pengambil kebijakan dan pakar.

d *Review* dan Diseminasi.

Proses refleksi dan pembelajaran terhadap keluaran yang dihasilkan. Refleksi dan pembelajaran tersebut bertujuan untuk mengevaluasi hasil penelitian dan mengetahui kontribusinya terhadap hal-hal praktis dan teoretis. Proses ini dilakukan dengan cara penilaian pakar (*expert judgement*) serta akademisi. Tahap selanjutnya adalah mengkomunikasikan hasil riset.



Gambar 5. Skema Metode Kajian

4. Hasil Penelitian dan Pembahasan

4.1. Proses Manajemen Resiko

1. Penentuan konteks

Proses awal dalam sebuah manajemen risiko adalah dengan melakukan penentuan konteks. Proses penentuan konteks dilakukan berdasarkan pengkajian yang dilakukan terhadap dokumen pada organisasi yang memiliki infrastruktur kritis. Aset yang kemungkinan akan terancam sehingga dapat diturunkan dengan mempertimbangkan enabler yang memungkinkan proses diidentifikasi. *Enabler* dapat diturunkan dengan mengidentifikasi orang, tempat, dan produk yang diperlukan untuk memastikan proses dapat dilakukan.Setiap *enabler* ada yang dimiliki. Pemilik adalah otoritas yang bertanggung jawab dalam bagian operasional organisasi untuk memastikan bahwa kontrol mitigasi secara tepat dilaksanakan. Berikut contoh peran struktural dalam organisasi yang memiliki infrastruktur kritis:

Tabel 1 Peran dalam *enterprise*.

Peran	Deskripsi
Chief Executive Officer (CEO)	Pejabat tertinggi yang bertanggung jawab pada keseluruhan manajemen *enterprise*
Chief Financial Officer (CFO)	Pejabat paling senior dari *enterprise* yang bertanggung jawab/*accountable* untuk semua aspek manajemen finansial, termasuk risiko finansial dan kendalinya

Peran	Deskripsi
Chief Operating Officer (COO)	Pejabat paling senior dari *enterprise* yang bertanggung jawab/*accountable* untuk operasional *enterprise*
Komite Pelaksana Strategi	Kumpulan eksekutif senior yang ditunjuk oleh dewan direksi untuk memastikan bahwa dewan direksi terlibat di dalamnya dan tetap diinformasikan mengenai hal-hal dan keputusan terkait TI. Komite ini bertanggung jawab/*accountable* dalam pengelolaan portofolio investasi TI, layanan TI dan aset TI, serta memastikan bahwa nilai tersampaikan dan risiko terkelola. Komite ini umumnya dipimpin oleh anggota dewan direksi, bukan oleh CIO.
Chief Risk Officer(CRO)	Pejabat paling senior dari *enterprise* yang bertanggung jawab/*accountable* pada seluruh aspek manajemen risiko yang ada di dalam *enterprise*. Fungsi petugas risiko TI dapat dibentuk untuk mengawasi risiko terkait TI
CISO	Pejabat paling senior dari *enterprise* yang bertanggung jawab/*accountable* pada seluruh keamanan informasi *enterprise*
Komite *Enterprise Risk Management* (ERM)	Kumpulan eksekutif *enterprise* yang bertanggung jawab/*accountable* pada kolaborasi dan persetujuan tingkat *enterprise* yang diperlukan untuk mendukung aktivitas dan keputusan ERM. Dewan risiko TI dapat dibentuk untuk mempertimbangkan risikoTI lebih detail dan memberikan nasihat kepada komite ERM
Audit	Fungsi dalam *enterprise* yang bertanggung jawab/*responsible* dalam ketentuan audit internal
Chief Information Officer (CIO)	Pejabat paling senior dalam *enterprise* yang bertanggung jawab/*accountable* pada penyelarasan strategi TI dan bisnis dan bertanggung jawab/*accountable* pada perencanaan, pengadaan sumber daya dan pengelolaan dalam pemberian layanan dan solusi TI untuk mendukung sasaran *enterprise*
Manajer Layanan	Pihak yang mengelola pengembangan, implementasi, evaluasi dan manajemen berkelanjutan dari produk dan layanan baru/yang telah ada untuk pelanggan/pengguna atau kelompok pelanggan/pengguna yang spesifik
Manajer Keamanan Informasi	Pihak yang mengelola, merancang, mengawasi dan/atau menilai keamanan informasi *Enterprises*
Manajer BCP	Pihak yang mengelola, merancang, mengawasi dan/atau menilai kemampuan keberlangsungan bisnis *enterprise*, untuk memastikan bahwa fungsi kritis *enterprise* tetap berjalan ketika terjadi kekacauan/gangguan
Privacy Officer	Pihak yang bertanggung jawab/*responsible* dalam pengawasan risiko dan dampak bisnis dari peraturan *privacy* serta pemanduan dan pengkoordinasian implementasi kebijakan dan aktivitas yang akan menjamin bahwa petunjuk *privacy* diikuti. Pihak ini juga biasa disebut sebagai petugas perlindungan data

2. Identitas Risiko

ancaman atau risiko. Sumber risiko yang dihasilkan diturunkan dari masing-masing enabler aset yang telah dijelaskan sebelumnya. Setelah mengidentifikasi aset yang diperlukan untuk memungkinkan pengolahan infrastruktur TI kritis pada instansi/organisasi yang memiliki sistim elektronik kritis serta sumber risiko yang kemungkinan terjadi, kegiatan berikutnya adalah mengidentifikasi kerentanan yang

setiap aset. Kerentanan terhadap aset dapat diidentifikasi melalui pertimbangan potensi ancaman. Proses tersebut ditindak lanjuti dengan mendeskripsikan tingkatan risiko.

3. Analisis Risiko

Tabel 2 Tabel likelihood

Likelihood Descriptor	*Likelihood Description Statements*
Sangat Jarang	Kejadian yang DIHARAPKAN terjadi di sebagian besar keadaan (*The event is EXPECTED to occur in most circumstances*).
Jarang	Kejadian ini ini MUNGKIN akan terjadi di sebagian besar keadaan dan diharapkan pada beberapa waktu (*The event will PROBABLY occur in most circumstances and is expected at some time*).
Kadang-kadang	Kejadian yang MUNGKIN terjadi pada beberapa waktu tetapi tidak diharapkan (*The event MIGHT occur at some time but is not expected*).
Sering	Kejadian BISA terjadi pada beberapa waktu (*The event COULD occur at some time*).
Sangat Sering	Kejadian yang MUNGKIN terjadi dalam keadaan luar biasa (*The event MAY occur in exceptional circumstances*).

Dampak yang dirasakan ketika suatu risiko terjadi dapat berpengaruh dan mengganggu tercapainya tujuan operasional dan organisasi. Pengaruh tersebut dapat bersifat sangat ringan efeknya sampai dengan ekstrem. Penjelasan lengkap mengenai dampak tersebut dapat dilihat pada Tabel 3 berikut ini

Tabel 3 Analisa Dampak Resiko

Konsekuensi/Dampak	Kualitas pelayanan
Tidak signifikan	Pada prinsipnya, defisiensi atau tidak adanya pelayanan rendah, tanpa ada komentar
Kurang signifikan	Pelayanan dianggap memuaskan oleh masyarakat umum, tetapi pegawai instansi mewaspadai adanya defisiensi
Sedang	Pelayanan dianggap kurang memuaskan oleh masyarakat umum dan pegawai organisasi
Signifikan	Masyarakat umum menganggap pelayanan organisasi tidak memuaskan
Sangat signifikan/ berbahaya/Katastropik	Pelayanan turun sangat jauh di bawah standar yang diterima

Berdasarkan tabel analisis kemungkinan dan dampak risiko, dapat dibuat bahan penentuan peringkat risiko yang berlaku dengan menggunakan matriks yang dijelaskan melalui Tabel dibawah ini. Matriks tersebut akan berfungsi untuk menentukan perlakuan/prioritas risiko dari daftar risiko yang ada. Tingkatan risiko terdiri dari 3 (tiga) tingkatan, yaitu; Rendah, Menengah dan Tinggi. Tabel 4 berikut ini menunjukkan pemeringkatan ketiga tingkatan risiko tersebut yang dipetakan berdasarkan kemungkinan frekuensi terjadinya risiko dan konsekuensi dampak terjadinya risiko.

Tabel 4 pemeringkatan risiko

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
	Rare	Rendah	Rendah	Rendah	Rendah	Menengah

Likelihood						
	Unlikely	Rendah	Rendah	Menengah	Menengah	Tinggi
	Possible	Rendah	Menengah	Menengah	Tinggi	Tinggi
	Likely	Rendah	Menengah	Menengah	Tinggi	Tinggi
	Almost Certain	Menengah	Menengah	Tinggi	Tinggi	Tinggi

Berdasarkan tingkatan risiko tersebut, dalam sebuah pengelolaan risiko perlu diklasifikasikan respon terhadap risiko. Bentuk respon ini terkait dengan siapa pejabat yang bertindak sebagai penanggungjawab pada masing-masing level dan apa rekomendasi untuk tindaklanjut berdasarkan kondisi risiko. Hal ini sangat bermanfaat untuk mitigasi terhadap risiko yang terjadi. Berikut ini adalah tabel 5 mengenai respon pemeringkatan risiko.

Tabel 5 Respon Peringkat Risiko

Risk Rating	*Responsibility for Risk Acceptance*	*Action Risiko*	*Rekomendasi*
High	*Risk Manager*	• Akan diharapkan merusak seluruh kemampuan organisasi untuk terus beroperasi dengan keyakinan dari basis pelanggan atau pemilik perusahaan. Risiko yang terjadi dapat mengakibatkan kerusakan sosial atau ekonomi yang serius dan dapat mempengaruhi kemampuan organisasi untuk melanjutkan operasi. • Akan diharapkan untuk memiliki dampak yang signifikan terhadap anggaran perusahaan dan reputasi organisasi.Dapat menyebabkan gangguan layanan diperpanjang dan serius ketidaknyamanan atau memiliki dampak kesehatan pada bagian luas basis pelanggan.	Mitigasi/Transfer
Medium	*Risk Manager* *Senior Manager*	Mungkin mengakibatkan jangka pendek, lokal, gangguan terhadap layanan dan memerlukan eskalasi melalui manajemen garis.Bisa menghasilkan merugikan Media komentar dan moderat hukuman lokal atau biaya dapat ditanggung melalui anggaran operasional normal.	Mitigasi
Low	*Senior Manager*	Tidak mungkin memiliki dampak yang tidak dapat memuaskan ditangani melalui prosedur operasional normal.	*Accept/Avoid*

4. Evaluasi Risiko

Proses evaluasi risiko memiliki tujuan untuk membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Proses dijalankan dengan cara menentukan risiko-risiko yang membutuhkan perlakuan atau prioritas risiko. Evaluasi risiko melibatkan perbandingan level risiko yang ditemukan selama proses analisis risiko dengan menggunakan kriteria risiko. Evaluasi risiko juga mengarahkan pengambilan keputusan terkait risiko mana yang perlu ditangani atau tidak. Tindakan lebih lanjut adalah proses perlakuan risiko. Proses tersebut memiliki tujuan untuk menetukan jenis serta bentuk perlakuan risiko. Pemilihan perlakuan risiko harus mempertimbangkan nilai-nilai dan persepsi *stakeholders*.

5. Communication and Consultation

Bagian ini merupakan identifikasi dan keterlibatan semua pemangku kepentingan yang terlibat dalam pengelolaan risiko pada infrastruktrur informasi kritis. Selain operasi sehari-hari dari sistem, penting untuk

memastikan bahwa informasi risiko dikomunikasikan melalui manajemen organisasi dan dibuat laporan secara singkat kepada forum eksekutif yang bertanggung jawab risiko organisasi secara manajemen keseluruhan.

6. *Monitor and Review*
   Pemantauan dan meninjau komponen yang perlu dilaksanakan untuk memastikan bahwa:

a Eksposur Risiko dimonitor, dievaluasi dan direvisi dari waktu ke waktu;
b Eksposur Risiko diperbarui secara tepat waktu dalam menanggapi peristiwa penting seperti perubahan operasi organisasi dan mempengaruhi peristiwa eksternal;
c Memastikan bahwa kontrol perbaikan diidentifikasi efektif dan efisien baik dalam desain dan operasi;
d Identifikasi risiko yang muncul, dan
e Kerangka manajemen risiko harus beroperasi secara efektif.

komunikasi dan konsultasi terkait mekanisme digunakan untuk mengimplementasikan komponen dari kerangka kerja manajemen risiko sehingga perlu diterapkan dalam manajemen organisasi dengan diiringi proses pemantauan. Tabel 6 berikut menyediakan panduan untuk keberhasilan pelaksanaan dan efektivitas keberlangsungan *Security Risk Management System*.

Tabel 6. Manajemen dan Monitoring untuk Security Risk Management System

ISO 27001 Proses SMKI	Keamanan Sistem Manajemen Risiko
Rencana (*Plan*)	Menetapkan *Security Risk Management Framework*, kebijakan yang berlaku, tujuan, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan untuk memberikan hasil yang sesuai dengan kebijakan dan tujuan keseluruhan organisasi.
Melakukan (*Do*)	Menerapkan dan mengoperasikan kebijakan Kerangka Manajemen Risiko, kontrol, proses dan prosedur.
Memeriksa (*Check*)	Menilai dan, jika memungkinkan, mengukur kinerja proses terhadap kebijakan Kerangka Manajemen Risiko, tujuan dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk diperiksa.
Bertindak (*Act*)	Mengambil tindakan korektif dan preventif, berdasarkan hasil audit internal dan tinjauan manajemen atau informasi lain yang relevan untuk mencapai perbaikan berkesinambungan dari Kerangka Manajemen Risiko.

4.2. Kerangka Kerja Keamanan Informasi

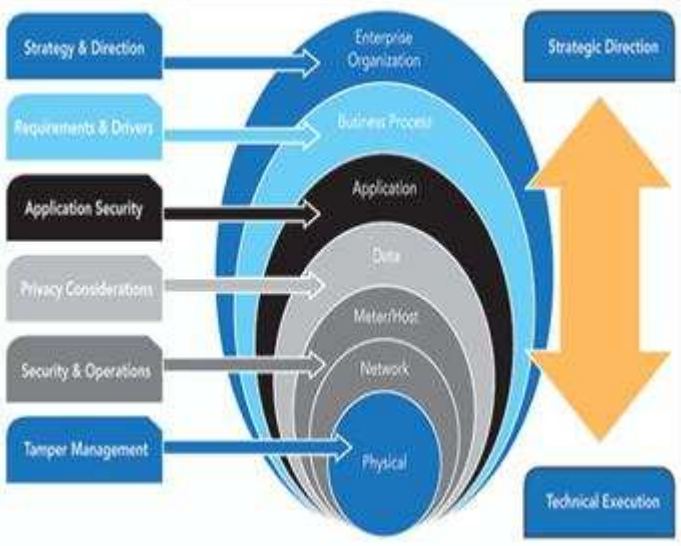
Organisasi membutuhkan kerangka kerja yang mempertimbangkan jenis risiko yang berbeda. Organisasi harus menilai bagaimana keamanan terlibat dengan strategi dan arah organisasi. Arah strategis dan pelaksanaan teknis memandu pendekatan berlapis untuk keamanan *smart grid*. Arah strategis meliputi persyaratan dan *driver* untuk proses bisnis. Pelaksanaan teknis termasuk keamanan aplikasi, data pribadi, integritas data, keamanan fisik, keamanan jaringan, keamanan meter, enkripsi dan proses operasional yang mendukung. Dalam pendekatan ini, setiap lapisan dampak data yang digunakan dan persyaratan keamanan berdasarkan tingkat akuntabilitas dan tanggung jawab dalam organisasi.

Implementasi teknologi dapat mengubah berbagai proses bisnis dan menghasilkan masalah keamanan di seluruh organisasi. Memahami perubahan dan kekhawatiran dapat membantu tim implementasi membuat keputusan keamanan yang tepat. Jika proses bisnis tidak terlibat lebih awal, organisasi mungkin membuat keputusan mengenai teknologi jangka panjang yang lebih mahal untuk merekayasa ulang nanti. Hal ini biasanya lebih murah dan lebih efektif untuk mempertimbangkan hal-hal seperti awal proses.

Peningkatan volume data dari sistem smart grid memperkenalkan pertimbangan manajemen data dan privasi yang terkait dengan pengumpulan data, pengumpulan informasi pribadi, insiden dan perencanaan manajemen pelanggaran, dan kebocoran data pribadi dan pribadi.

Organisasi harus merencanakan skenario keamanan yang berbeda dengan melakukan penilaian kerentanan dan ancaman profiling dan dengan mengembangkan rencana manajemen keamanan. Penilaian

risiko dan mitigasi risiko keamanan yang efektif harus diselesaikan di awal kegiatan. Hal ini sangat penting selama pemilihan vendor atau peralatan.



Gambar 6. Kerangka Kerja Keamanan infrastruktur kritis secara berlapis

- Penilaian kerentanan: Organisasi harus mengidentifikasi dan menilai kerentanan untuk setiap komponen infrastruktur smart grid. Proses harus menyediakan analisis kesenjangan, penilaian risiko, pengamatan dan rekomendasi untuk mengurangi risiko dan memperbaiki infrastruktur keamanan.
- Profil ancaman: Organisasi harus menggunakan perencanaan skenario dan pengujian latihan untuk mengatasi profil ancaman yang berbeda. Profil ancaman termasuk penasaran dan penyadap, pelanggan tidak etis, mengganggu pihak ketiga dan penyerang yang aktif.

Rencana manajemen keamanan: Mengembangkan rencana manajemen keamanan termasuk penggunaan otomatis pemindaian kerentanan, pengujian kerentanan manual dan jasa penilaian konfigurasi teknis.

4.3. Strategi Keamanan Informasi Pada Infrastruktur Kritis Nasional

Keamanan Infrastruktur Informasi Kritis Nasional merupakan prasyarat mutlak yang harus diimplementasikan di Indonesia agar dapat menjamin efektivitas keandalan, ketersediaan, dan integritas jaringan informasi, baik secara nasional maupun global. Namun demikian, dampak besar dan potensi gangguan serta ancaman terhadap keamanan infrastruktur kritis nasional masih belum disadari sepenuhnya oleh masyarakat. kini mengintai kita semua. Hal ini tampak dari belum tersedianya kebijakan Proteksi Infarastruktur Informasi Kritis Nasional dan belum dipetakan / diklasifikasikannya Infrastruktur Kritis Nasional, khususnya infrastruktur jaringan informasi.

Ancaman terhadap Keamanan Infrastruktur Informasi Kritis Nasional dapat menimbulkan suatu kerugian yang tidak dapat ternilai terhadap stabilitas, perekonomian bahkan kedaulatan Negara. Pemerintah perlu mengambil langkah-langkah dan upaya preventif untuk menjamin agar setiap upaya yang dapat mengancam stabilitas negara tersebut dapat dicegah dan bagi pelakunya dapat disidik secara hukum dan dikenai ancaman pidana yang berat.

Terkait hal tersebut, seorang praktisi telekomunikasi dan juga Ketua *Indonesia Telecommunication Users Group (IDTUG)*, Ari Sutedja K dalam sebuah wawancara mendalam, menyebutkan beberapa langkah yang dapat ditempuh oleh pengambil kebijakan terkait proteksi infrastruktur informasi kritis. Langkah pertama di dalam melindungi Infrastruktur Informasi Kritis mencakup pengenalan terhadap potensi ancaman-ancaman yang ada (*threat profiling*) dan potensi- potensi kelemahan infrastruktur (*infrastructure*

weaknesses profiling) agar dapat menekan resiko timbulnya ancaman dan gangguan yang dapat terjadi. Kedua, menekan kerugian yang telah terjadi dan waktu pemulihannya bilamana terjadi sebuah gangguan. Langkah ketiga, adalah mencari dan mengenali penyebab atau sumber dari gangguan tersebut agar kemudian dapat diteliti dan dianalisis secara forensik (*e-forensic*) oleh para ahli dan penyidik dari kalangan aparat penegak hukum.

Keempat, diperlukannya koordinasi, komunikasi (keterbukaan), dan kerja sama secara nasional dan internasional dari para stakeholder, termasuk di dalamnya Badan Perlindungan Jaringan Infrastruktur Kritis Nasional (bilamana ada), kepolisian dan aparat intelijen. Upaya-upaya kerja sama tersebut harus tetap mengacu kepada peraturan yang melindungi keamanan informasi dan aturan-aturan hukum yang terkait dengan bantuan hukum dan perlindungan atas hak-hak pribadi (*privacy law*).

Lebih lanjut disampaikan bahwa, pemerintah hendaknya juga dapat menerapkan Sebelas Prinsip Dasar tentang *Critical Information Infrastructure Protection* yang diusulkan oleh beberapa negara yang tergabung di dalam negara-negara G8 pada bulan Mei 2003, memuat strategi-strategi dalam menekan resiko terhadap potensi ancaman dan gangguan terhadap infrastruktur informasi kritis Nasional yang antara lain;

1. Prinsip pertama; menekankan, pemerintah hendaknya memiliki jaringan peringatan dini (*emergency early warning networks*) untuk memantau kelemahan, ancaman dan kejadian terhadap infrastruktur informasi kritis Nasional.
2. Prinsip kedua; pemerintah berkewajiban meningkatkan kepekaan dalam memfasilitasi pemahaman para stakeholder mengenai sifat dan keadaan infrastruktur informasi kritis yang dimilikinya, dan peran apa yang harus dimainkan oleh mereka.
3. Prinsip ketig; pemerintah harus dapat dan mampu menguji serta mengenali sifat ketergantungan satu sama lain berbagai infrastruktur kritis yang dimilikinya agar dapat meningkatkan perlindungan terhadap infrastruktur tersebut.
4. Prinsip keempat; pemerintah hendaknya mendorong program kemitraan dengan para *stakeholder*, baik sektor public maupun swasta, dalam membagi dan menganalisis informasi infrastruktur kritis dalam rangka penanggulangan, penyidikan, dan tindakan kerugian ataupun gangguan yang telah terjadi terhadap infrastruktur tersebut.
5. Prinsip kelima; pemerintah berkewajiban membentuk dan memelihara pusat jaringan informasi krisis (*Crisis Information Network*) serta menguji dan melindungi keandalannya dalam keadaan darurat.
6. Prinsip keenam; pemerintah hendaknya dapat menjamin bahwa kebijakan tentang keterbukaan informasi juga harus dapat mengacu kepada kebutuhan akan perlindungan terhadap infrastruktur informasi kritis Nasional.
7. Prinsip ketujuh; pemerintah harus memfasilitasi penyidikan terhadap gangguan terhadap infrastruktur informasi kritis Nasional, dan bila memungkinkan berbagi informasi hasil penyidikannya dengan negara- negara lain.
8. Prinsip kedelapan;, pemerintah hendaknya harus dapat memfasilitasi berbagai bentuk pelatihan untuk meningkatkan kemampuan bereaksi serta menguji kesiapan dan rencana cadangan bilamana terjadi gangguan terhadap infrastruktur informasi kritis Nasional dan berkewajiban mendorong para stakeholder untuk melakukan kegiatan yang serupa.
9. Prinsip kesembilan; pemerintah harus dapat menjamin ketersediaan produk-produk hukum yang memayungi berbagai kegiatan di atas, aparat yang terlatih dan mampu melakukan penyidikan dan penindakan atas gangguan yang terjadi, dan mengoordinasikan penyidikan tersebut dengan pihak lain, termasuk negara-negara yang terkait dengan gangguan tersebut.
10. Prinsip kesepuluh; pemerintah harus aktif menjembatani kerja sama internasional untuk memperoleh berbagai informasi kritis, termasuk di dalamnya mengembangkan dan mengoordinasikan sistem peringatan darurat, berbagi dan menganalisis informasi kelemahan-kelemahan, ancaman dan kejadian terhadap infrastruktur kritis, serta melakukan koordinasi penyidikan itu dengan mengacu kepada ketentuan-ketentuan hukum yang berlaku.

11. Prinsip kesebelas; pemerintah hendaknya menjembatani berbagai kegiatan penelitian, baik secara nasional maupun internasional, serta mendorong penggunaan berbagai aplikasi pengamanan yang telah disertifikasi berdasarkan standar- standar internasional yang berlaku.

Hal yang lebih penting selain sebelas prinsip tersebut adalah perlu adanya koordinasi antara pemangku kebijakan, baik regulator maupun operator terkait infrastruktur informasi kritis agar terciptanya harmonisasi. Disamping itu, upaya lainnya adalah dengan membangun *culture of cyber s*ecurity itu sendiri yang harus dimulai dari kalangan pemerintah (*regulator*) agar masyarakat secara luas dapat juga mengikuti dan mencontoh budaya tersebut.

4.4. Kebijakan Keamanan Informasi Pada Infrastruktur Kritis

Keamanan Infrastruktur Informasi Kritis Nasional merupakan prasyarat mutlak yang harus diimplementasikan di Indonesia agar dapat menjamin efektivitas keandalan, ketersediaan, dan integritas jaringan informasi, baik secara nasional maupun global. Namun demikian, dampak besar dan potensi gangguan serta ancaman terhadap keamanan infrastruktur kritis nasional masih belum disadari sepenuhnya oleh masyarakat kini mengintai kita semua. Hal ini tampak dari belum tersedianya kebijakan Proteksi Infarastruktur Informasi Kritis Nasional dan belum dipetakan/diklasifikasikannya Infrastruktur Kritis Nasional, khususnya infrastruktur jaringan informasi.

Berdasarkan hasil analisis kasus smart grid ketenagalistrikan sebagai salah satu infrastruktur informasi yang kritis, kerentanan (*vulnerability*) sistem jaringan smart grid akan berdampak pada aspek Keamanan Informasi. Dalam kerangka kerja pengamanan berlapis pada sistem *smart gri*d, perlu dipastikan bahwa seluruh aktivitas yang sudah dilakukan pengamanan. Proses pengamanan bukan hanya di *real sp*ace tapi juga pada *cyber space* dilingkungan smart grid sebagai infrastruktur kritis. Proses pengamanan *cyber space* dapat dilakukan dengan mengunakan Sertifikasi Keamanan Informasi untuk memastikan bahwa seluruh aktivitas yang diperlukan untuk pengamanan sudah dilakukan.

Dalam terminologi UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan juga pada Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), Transaksi Elektronik didefinisikan sebagai sebuah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya. Sementara itu, Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan elektronik. Adapun Penyelenggara Sistem elektronik adalah setiap orang, penyelenggaran negra, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain. Dengan demikian, *smart gr*id dapat dikategorikan sebagai sistem elektronik yang kritis dan pengguna *smart g*rid dapat dikategorikan sebagai Penyelenggara Sistem Elektronik yang kritis.

Dalam rangka pengamanan *cyber space* pada Penyelenggara Sistem Elektronik, tujuan utamanya adalah agar dapat memenuhi aspek keamanan informasi, yaitu *Confidentiality, Integrity,* dan *Availability*. Lebih lanjut lagi, dalam Pasal 15 UU ITE disebutkan bahwa Penyelenggara Sistem Elektronik memiliki kewajiban untuk menyelenggarakan sistem elektronik yang andal, aman dan bertanggungjawab. Selain itu, regulasi juga mengatur agar Penyelenggara Sistem Elektronik wajib menggunakan sertifikat elektronik dan dapat disertifikasi oleh Lembaga Sertifikasi Keandalan (Pasal 10 UU ITE). Dalam Pasal 41 PP PSTE juga dijelaskan bahwa Penyelenggaraan Transaksi Elektronik dalam lingkup publik atau privat yang menggunakan Sistem Elektronik untuk kepentingan pelayanan publik wajib menggunakan Sertifikat Keandalan dan/atau Sertifikat Elektronik.

Disamping itu, mengingat Informasi adalah aset yang rawan terhadap pencurian dan modifikasi, maka penerapan sertifikasi SNI 27001 sebagai sistem manajemen keamanan informasi sangat penting karena menyangkut informasi yang digunakan. Standar keamanan informasi yang dikeluarkan oleh SNI berlaku

bagi semua jenis organisasi, terutama bagi organisasi Penyelenggara Sistem Elektronik yang memiliki infrastruktur sistem elektronik dengan kategori infrastruktur kritis. Dalam standar itu ditetapkan persyaratan untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, peningkatan dan pemeliharaan Sistem Manajemen Keamanan Informasi (SMKI) yang terdokumentasi dalam konteks resiko bisnis organisasi secara keseluruhan.

5. Simpulan dan Saran

5.1. Kesimpulan

Berdasarkan hasil pembahasan dalam kajian ini, dapat disimpulkan sebagai berikut:

Penerapan manajemen risiko pada infrastruktur informasi kritis dapat menggunakan RMF yang mengacu pada ISO31000:2009 (*Risk management — Principles and guidelines*). Proses yang dilakukan terdiri atas penentuan konteks, penilaian risiko dan perlakuan risiko. Komponen lain yang tidak dapat dipisahkan dalam proses manajemen risiko adalah komunikasi, konsultasi, monitoring dan *review*.

Penentuan konteks risiko dapat diturunkan dari aset yang dimiliki oleh organisasi dan terkait dengan proses bisnis penyelenggara system elektronik yang memiliki infrastruktur informasi kritis. Penilaian risiko dilakukan bertujuan untuk menghasilkan daftar risiko, analisis dan evaluasi risiko yang ada. Perlakuan risiko ditentukan sebagai langkah terakhir yang diambil untuk menangani dampak dan kemungkinan terjadinya risiko yang telah diidentifikasi sebelumnya. Proses-proses tersebut merupakan langkah-langkah terstruktur dan berkelanjutan dalam penerapan manajemen risiko untuk infrastruktur informasi kritis.

5.2. Saran

Berdasarkan hasil kajian dan kesimpulan yang telah diuraikan, disampaikan beberapa saran sebagai berikut :

Sebagai salahsatu pemangku kepentingan (*stakeholder*) dan juga regulator, Pemerintah yang terkait pada sector pemanfaatan infrastruktur informasi kritis dan sector Keamanan Informasi perlu saling berkoordinasi dalam hal pengklasifikasian infrastruktur kritis. Disamping itu perlu juga dibuatkan regulasi dan standar terkait pengamanan infrastruktur informasi kritis, serta mitigasinya.

Terkait kebijakan pengamanan infrastruktur system elektronik dengan kategori kritis (*critical information infrastructure*), perlu dibuatkan kebijakan Pengamanan Infrastruktur system Elektronik yang merujuk pada ISO IEC 31000. Dalam hal pemanfaatan Sertifikat Elektonik, perlu mereview (kaji ulang) terhadap Peraturan Menteri mengenai Sertifikat Berinduk (*root CA*), agar dapat memperhatikan pola *root CA* untuk Infrastruktur Kritis. Sertifikasi Manajemen Keamanan Informasi diperlukan untuk memastikan bahwa seluruh aktivitas pada infrastruktur/sistem informasi kritis telah dilakukan pengamanan. Dengan demikian SE MenKominfo tentang penggunaan SNI 27001 perlu perlu direvisi mengingat ISO terkait yang sudah berkembang.

Daftar Pustaka

M. Henderson. (2007). "Protecting Critical Infrastructure from Cyber Attacks," Department of Homeland Security-USA, 2007.

J. W. Cresswell. (2008). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Third Edition, SAGE Publications, Inc, 2008.

ISO/IEC, ISO/IEC 27002:2013, ISO/IEC, 2013.

ISO/IEC, ISO/IEC 27001:2013, ISO/IEC, 2013

ISO/IEC, ISO/IEC 27000:2014, ISO/IEC, 2014

Department of Defense. (2012) DoD Policy and Responsibilities for Critical Infrastructure, Department of Defense USA.

Federal Energy Regulatory Commission. (2013). "Critical Infrastructure Protection Reliability Standards," Federal Energy Regulatory Commission-USA.

Ko, M. dan Dorantes, C. (2006), *The Impact of Information Security Breaches on Financial Performance of The Breached Firms: an Empirical Investigation*, Journal of Information Technology Management, vol. XVII, pp. 13-22.

Nickolov, Eugene. (2005), *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations,* INFORMATION & SECURITY. An International Journal, Vol.17, pp. 105-119

Su, X. (2006), *An Overview of Economic Approaches to Information Security Management*, University of Twente, Information Systems Group, Enschede, The Netherlands.

Suter, Manuel. (2007), *A Generic National Framework For Critical Information Infrastructure Protection (CIIP)*, Center for Security Studies, ETH Zurich.

National Institute of Standard dan Technology (NIST), (2007), *NISTIR 7628 Guidelines for Smart Grid Cyber Security*, Smart Grid Interoperable Panel (SGIP) Cyber Security Working Group, NIST, US Depertement of Commerce.

National Institute of Standard dan Technology (NIST), (2007), *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, US Depertement of Commerce, v. 1.0

OECD, (2006), *Recomendation of The Council on The Protection of Critical Information Infrastructure, OECD Ministerial Meeting on The Future of Internet Economy*, Seoul, South Korea

Whitman, M. E. (2004), *In defense of the realm: understanding the threats to information security*, International Journal of Information Management,vol. 24, no. 1.

Cashell, B., Jackson, W. D., Jickling, M. dan Webel, B. (2004), *The Economic Impact of Cyber-Attacks*, CISCO.

Dey, M. (2007), Information security management - a practical approach, *AFRICON 2007*.

Norman, A. dan Yasin, N. (2009), *An analysis of Information Systems Security Management (ISSM): The hierarchical organizations vs. emergent organization*, ICITST International Conference on Internet Technology and Secured Transactions.

Chang, H., Kwon, H., Lee, C. dan Kang, J. (2010), *The Weighted Industrial Security Management System for SMBs*, 5th International Conference on Future Information Technology (FutureTech).

Gorman, Sean P. and Schintler, Laurie and Kulkarni, Rajendra and Stough, Roger R., (2004), *The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure*. Journal of Contingencies and Crisis Management, Vol. 12, No. 2, pp. 48-63, June 2004. Available at SSRN: http://ssrn.com/abstract=549768