PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA *INFORMATION CAPITAL READINESS* PT PJB UP GRESIK

Nur Fatimatuz Zuhroh [1] **Haryanto Tanuwijaya** [2]**Erwin Sutomo** [3]
Program Studi/Jurusan Sistem Informasi
Institut Teknologi dan Informatika Stikom Surabaya
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1)Arfafafa@gmail.com , 2)Haryanto@stikom.edu, 3)Erwin@stikom.edu

Abstract: *Information Capital Readliness (ICR) is one of bound performance in technology and information sector at PT Pembangkit Jawa Bali Unit Pembangkit Gresik which is functioned in supporting company's strategy. Information security is an important thing of ICR's performance, because the information resulted must have confidentially, integrity, and availability to support the business process. In ICR, there is assessment of bound performance which supports directness of the business process.*

Nowadays, ICR cannot fulfill the requirements of bound performance yet because there is no good processing yet in planning information security. A solution to figure out that issue is making a good management in planning information security management system or SMKI based on standard ISO/IEC 27001:2005 which will result management in planning information security of ICR. Scope of the information security management system in the ICR include infrastructure and application.

The result of this planning information security management system can be concluded into document of planning information security management system which contains risk assessment report with server's high value of risk level is 35.52 and asset fyber optic cable's low value of risk level is 11.2, policy, procedure, work instruction and other related documents. Those documents are used in handling planning process of ICR's information security, so the requirements of bound performance can be fulfilled.

Keywords*: Assessment of Bound Performance, Information Security Management System, ISO/IEC 27001:2005*

Information Capital Readiness (ICR) merupakan indikator penilaian kinerja dalam mendukung strategi perusahaan yang dilakukan oleh tim assessor dan terdiri dari tiga proses utama yang menilai tentang *Infrastructure* dan *Application*. PT PJB menetapkan *Assesment* Kontrak Kinerja dalam mendukung kelangsungan proses bisnis teknologi informasi khususnya untuk keamanan informasi. Penilaian kontrak kinerja pada ICR berfungsi sebagai landasan penilaian setiap unit yang diperoleh dari dokumen kriteria ICR dan *Opportunity For Improvement* (OFI). OFI merupakan rekomendasi yang dibuat untuk kelangsungan kualitas dari teknologi informasi yang diberikan kepada *user*, sedangkan kriteria ICR terdiri dari kriteria-kriteria dalam ICR yang harus dipenuhi dalam mencapai nilai target kinerja.

Untuk mencapai nilai target kinerja yang sudah ditetapkan pada *Assesment* Kontrak Kinerja memerlukan kriteria-kriteria yang harus dipenuhi oleh ICR dalam menghasilkan nilai *maturity level* pada ICR. Di dalam dokumen kriteria ICR menjelaskan poin-poin target yang perlu dicapai dan dipenuhi dalam hal keamanan informasi. SINFO mengalami kesulitan dalam memenuhi kriteria tersebut karena tidak terdapat pengolahan keamanan informasi yang sesuai standar agar kriteria tersebut dapat terpenuhi. Dampak yang ditimbulkan apabila tidak terdapat pengolahan mengenai keamanan sistem informasi dapat membuat ICR mengalami hambatan pada layanan keamanan informasi dan kondisi kualitas dari teknologi informasi khususnya keamanan informasi pada PT PJB Unit Pembangkit Gresik. Pemenuhan kriteria ICR dan OFI sangat diperlukan dalam menentukan nilai target unit sebagai dasar dari *Assesment* Kontrak Kinerja.

Pemecahan masalah keamanan informasi ICR pada PT PJB Unit Pembangkit Gresik, SINFO membutuhkan sebuah

perencanaan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001:2005 untuk mengelola keamanan informasi yang sesuai standar. Proses ini memiliki tujuan untuk memberikan pedoman pengolahan untuk mengantisipasi keamanan informasi pada ICR. Luaran dari perencanaan sistem manajemen keamanan informasi adalah dibuatnya dokumen perencanaan SMKI yang meliputi dokumen prosedur, instruksi kerja, dan dokumen lain terkait pada tahap perencanaan sistem manajemen keamanan informasi. Dokumen tersebut berfungsi untuk mengelola teknologi keamanan informasi dalam proses perlindungan aspek keamanan informasi yaitu kerahasiaan, keutuhan, dan ketersedian untuk memenuhi kriteria ICR sehingga ICR dapat menentukan nilai untuk target unit pada *Assesment* Kontrak Kinerja. Dalam pembuatan perencanaan sistem manajemen keamanan informasi ini akan menggunakan *standard* ISO/IEC 27001:2005 *Information Security Management System Requirments* dan ISO/IEC 27002:2005 *Code Of Practice For ISMS*. Alasan pemilihan kedua *standard* ini yaitu mendefinisikan persyaratan dalam membangun SMKI berdasarkan ISO/IEC27001:2005, sedang pada ISO/IEC 27002:2005 bertujuan untuk menentukan kontrol objektif dan kontrol yang dibutuhkan dalam perencanaan dan persyaratan SMKI yang ada dalam ISO/IEC 27001:2005.

METODE

Sistem manajemen keamanan informasi (SMKI) atau yang disebut *juga Information Management Security System* (ISMS) merupakan suatu proses yang disusun berdasarkan pendekatan resiko bisnis untuk merencanakan (*Plan*), mengimplementasikan (*Do*), memonitor adan meninjau ulang (*Check*), dan memelihara (*Act*) terhadap keamanan informasi perusahaan. SMKI berdasarkan ISO/IEC 27001:2005 menjelaskan persyaratan dalam menerapkan, melaksanakan, memonitor, menganalisa, memelihara sampai mendokumentasikan sistem manajemen keamanan informasi (SMKI). Pada tahapan perencaan sistem manajemen keamanan informasi dilakukan melalui 3 tahapan yaitu tahap awal, pengembangan, dan tahap akhir. Pada tahap awal memerlukan tiga proses utama yaitu dengan cara wawancara, observasi, dan studi literatur. Wawancara yang dilakukan meliputi proses bisnis pada ICR dan layanan yang terdapat pada ICR. Observasi yang dibutuhkan yaitu mengenai permasalahan yang terdapat pada ICR. Studi literatur dilakukan untuk menggali informasi dan pengetahuan dari proses tugas akhir.

Tahap pengembangan merupakan tahapan inti dari perencanaan sistem manajemen keamanan informasi yang dilakukan melalui 8 tahapan antara lain :

1. Menentukan pendekatan penilaian risiko yang dilakukan dengen mengidentifikasikan metode penilaian risiko yang kriteria penerimaan risiko.
2. Identifikasi risiko yang dilakukan dengan cara melakukan identifikasi aset, menghitung nilai ancaman atau kelemahan, dan mengidemtifikasi dampak keamanan informasi bagi aset.
3. Analisa dan evaluasi risiko yang dilakukan dengan cara menghitung nilai analisa dampak bisnis (BIA) serta mengidentfikasi level risiko, menentukan apakah risiko diterima atau tidak.
4. Analisa dan penanganan risiko yang bertujuan untuk menentukan langkah apa yang harus diambil dalam penanganan risiko dengan menggunakan kriteria penerimaan risiko yang telah ditetapkan.
5. Penetapan kontrol objektif dan kontrol dipilih berdasarkan ancaman dan kelemahan pada aset yang membutuhkan penanganan risiko.
6. Pembuatan kebijakan dan prosedur dilakukan sesuai dengan pemilihan kontrol objektif dan kontrol yang dipilih dari klausul-klausul yang ada pada ISO/IEC 27002:2010. Penulisan kebijakan dan prosedur dilakukan sesuai format yang telah ditentukan oleh perusahaan.

Tahap akhir adalah tahapan yang menjelaskan hasil dari output atau keluaran dari perencanaan sistem manajemen keamanan informasi.

HASIL DAN PEMBAHASAN

Hasil dari proses perencanaan sistem manajemen keamanan informasi ini meliputi :

A. Tahap awal

Tahap awal dilakukan dengan wawancara yang menghasilkan proses bisnis dan layanan yang terdapat pada ICR, observasi yang dilakukan untuk menentukan permasalahan pada ICR, sedangkan studi literatur yang dibutuhkan meliputi studi literatur penilaian risiko, pembuatan

kebijakan dan prosedur, dan pembuatan instruksi kerja dan rekam kerja.

B. Tahap pengembangan

Tahap pengembangan yang dilakukan melalui 6 tahapan yaitu :

1. Menentukan pendekatan penilaian risiko

Metode penilain risiko yang dilakukan pada ICR menggunakan metode kualitatif berdasarkan pada SK Direksi no 128. K/D10/DIR/2014, sedangkan kriteria penerimaan risiko yang ditetapkan pada ICR anatar lain : 1. *Risk acceptance*, 2. *Risk reduction*, 3. *Risk avoid*, dan 4. *Risk transfer*.

2. Identifikasi risiko

Dari hasil identifikasi risiko dilakukan melalui beberapa tahapan yaitu :

a. Identifikasi aset yang dilakukan menghasilkan beberapa jenis aset pada ICR pada Tabel 1.

Tabel 1. Identifikasi Aset

No	Jenis Aset	Aset
1	Perangkat Keras	Server
2	Jaringan	*Wide Area Network* (WAN)
		Local Area Network (LAN)
4	Aplikasi	App. Ellipse
		App. *Helpdesk*
5	Tools	Oracle
6	Infrastruktur	*Cooling System*
		Kabel *Fyber Optic*

b. Nilai aset yang dihasilkan dijelaskan pada Tabel 2.

Tabel 2. Nilai Ancaman

No	Aset	Kriteria			Nilai Aset
		NC	NI	NA	
1.	Server	4	4	4	12
2.	WAN	2	3	3	8
3.	*LAN*	1	2	2	5
4.	*App.Ellipse*	3	2	3	8
5.	App.*Helpdesk*	2	1	1	4
6.	Oracle	3	4	4	11
7	*Cooling System*	1	0	2	3
8	Kabel FO	3	3	2	8

c. Nilai ancaman pada aset dapat dilihat pada Tabel 3.

Tabel 3. Nilai Ancaman

No	Aset	Nilai Ancaman
1	Server	0,74
2	WAN	0,53
3	*LAN*	0,325
4	App. Ellipse	0,6
5	App.*Helpdesk*	0,3
6	Oracle	0,63
7	*Cooling System*	0,15
8	kabel FO	0,7

d. Dampak keamanan informasi pada aset pada salah satu aset server dapat ditunjukkan pada Tabel 4.

Tabel 4. Dampak Keamanan Server

Kategori	Dampak
Kerahasiaan	Jika data server tidak memiliki *access control*, maka akan menimbulkan dampak kerugian finansial yang sangat besar bagi unit PJB dan PT PJB internal akibat pencurian data, kerusakan data, kehilangan data, data data yang terdapat pada server disalahgunakan oleh pihak yang tidak bertanggung jawab.
Keutuhan	Data dan informasi yang ada pada serer harus selalu akurat dan utuh, apabila informasi yang diberikan oleh server tidak akurat dan valid dapat menimbulkan kerugian bagi staf, organisasi, dan general manajer PT PJB UP gresik serta akan menggangu kelancaran proses bisnis *coorporate* PT PJB.
Ketersediaan	Data dan informasi yang disediakan oleh server harus selalu tersedia kapanpun ketika diakses oleh pengguna PT PJB UP Gresik karena apabila data tersebut tidak dapat diakses akan menggangu kelancaran proses bisnis bagi organisasi (divisi) dan pimpinan PT PJB UP Gresik akibatnya aplikasi *core business* tidak dapat diakses oleh semua unit PT PJB.

3. Analisa dan evaluasi risiko

Dari hasil analisa dan evaluasi risiko dilakukan dengan beberapa tahapan antara lain :

a. Analisa Dampak Bisnis (BIA) pada aset dapat dilihat selengkapnya pada Tabel 5.

Tabel 5. Nilai BIA

No	Aset	Dampak	Nilai BIA
1	Server	Operasi layanan aplikasi pusat dan unit terhenti	4
2	WAN	Komunikasi antar PT PJB terhenti dan dapat menggangu pelayanan antar unit PJB.	4
3	*LAN*	Komunikasi dalam unit terhenti dan dapat	2

		menggangu pelayanan terhadap *user*.	
4	App. Ellipse	Sistem informasi manajamen aset menjadi terhambat	3
5	App.*Help desk*	Modul-modul dalam aplikasi helpdek menjadi terhambat	1
6	Oracle	*Database* aplikasi pusat tidak dapat beroperasi	4
7	*Cooling System*	Server tidak dapat berjalan dengan maksimal karena panas dan tidak sesuai standar keamanan.	2
8	kabel FO	Transfer data dan koneksi jaringan tidak dapat digunakan untuk mengakses aplikasi pusat dan unit	2

b. Mengidentifikasi level risiko dilakukan untuk memnetukan skala dari masing-masing aset yang nantinya digunakan dalam penanganan risiko. Matriks level risiko ditunjukkan pada Gambar 1.

Probabilitas Ancaman	**Dampak Bisnis**			
	Not Critical 20	**Low Critical 40**	**Medium Critical 60**	**High Critical 80**
Low 0,1	Low 2	Low 4	Low 6	Low 8
Medium 0,5	Low 10	Medium 20	Medium 30	Medium 40
High 1,0	Medium 20	Medium 40	High 60	High 80

Gambar 1. Matriks Level Risiko

c. Menentukan apakah risiko diterima atau tidak berfungsi dalam penanganan risiko. Risiko diterima apabila memiliki nilai risiko dengan tingkat low namun risiko perlu dilakukan penanganan apabila level risiko bernilai medium atau high. Nilai risiko akan ditunjukkan pada Tabel6.

Tabel 6. Nilai Risiko

No	**Aset**	**Nilai Risiko**	**Level Risiko**
1	Server	35,52	**MEDIUM**
2	WAN	16,96	**MEDIUM**
3	LAN	3,25	LOW
4	App.Ellipse	14,4	**MEDIUM**
5	App.*Helpdesk*	1,2	LOW
6	Oracle	27,72	**MEDIUM**
7	*Cooling System*	0,9	LOW
8	Kabel FO	11,2	**MEDIUM**

4. Analisa penanganan risiko bertujuan untuk menentukan pilihan penanganan risiko pada aset yang memiliki level risiko paling tinggi yaitu server, WAN, app.ellipse, oracle, dn kabel FO sesuai dengan kriteria penerimaan risiko yang telah ditetapkan. Pilihan penanganan risiko ditunjukkan pada Tabel 7.

Tabel 7. Pilihan penanganan Risiko

No	**Aset**	**Pilihan Penanganan Risiko**
1.	Server	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002
2.	*Wide Area Network* (WAN)	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002
3.	App. Ellipse	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002
4.	Oracle	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002
5.	Kabel *Fyber Optic*	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002

5. Penetapan kontrol objektif dan kontrol
Kontrol objektif dan kontrol dipilih berdasarkan pada ancaman dan kelemahan pada aset server, WAN,app.ellipse, oracle, dan kabel FO yaitu sebagai berikut.

a. Server

Kategori Keamanan Utama A.10.5 Back-up Kontrol Objektif: untuk memelihara integritas , ketersediaan informasi, dan fasilitas pengolahan informasi. Organisasi		
A.10.5.1	Back-up informasi	Pengendalian : Salinan back-up informasi dan perangkat lunak harus diuji secara regular sesuai kebijakan *back-up*.
Kategori Keamanan Utama A.11.1 Persyaratan bisnis untuk pengendalian akses Kontrol Objektif: untuk mengendalikan akses kepada informasi.		
A.11.1.1	Kebijakan pengendalian akses	Pengendalian : Kebijakan pengendalian akses harus ditetapkan dan didokumentasikan berdasarkan persyaratan bisnis dan keamanan akses.
Kategori Keamanan Utama A.13.2 Manajemen insiden keamanan informasi dan perbaikan Kontrol Objektif: untuk memastikan pendekatan yang konsisten dan efektif diterapkan untuk		

manajemen insiden keamanan informasi.		
A.13.2.1	Tanggung jawab dan prosedur	Pengendalian : Insiden keamanan informasi harus ditetapkan tanggung jawabdan prosedur untuk memastikan tanggapan yang cepat dan efisien pada insiden keamanan informasi.

b. WAN

Kategori Keamanan Utama A.11.4 Pengendalian akses jaringan Kontrol Objektif: mencegah akses layanan jaringan oleh pengguna yang tidak sah		
A.11.4.1	Kebijakan penggunaan layanan jaringan	Pengendalian : Layanan hanya dapat diberikan kepada pengguna akses yang berwenang secara spesifik.
A.11.4.6	Pengendalian koneksi jaringan	Pengendalian : Jaringan yang digunakan secara bersama khususnya dalam perluasan jaringan harus dibatasi dan sejalan dengan kebijakan pengendalian akses dalam aplikasi.

c. App. Ellipse

Kategori Keamanan Utama A.11.2 Manajemen akses pengguna Kontrol Objektif: memastikan akses sistem informasi oleh pengguna yang sah dan mencegah akses oleh pihak yang tidak sah		
A.11.2.1	Pendaftaran pengguna	Pengendalian : Harus ada prosedur pendaftaran dan penghapusan/pembatalan pendaftaran pengguna dalam pengendalian akses terhadap seluruh layanan dan sistem informasi.
A.11.2.3	Manajemen password pengguna	Pengendalian : Alokasi password harus dikendalikan dengan proses manajemen formal.
A.11.2.4	Tinjauan terhadap hak akses Pengguna	Pengendalian : Manajemen harus selalu melakukan peninajuan ulang terhadap akses pengguna secara rutin.

d. Oracle

Kategori Keamanan Utama A.11.6 Pengendalian akses aplikasi dan informasi Kontrol Objektif: untuk mencegah akses yang tidak sah terhadap informasi pada sistem aplikasi		
A.11.6.1	Pembatasan akses informasi	Pengendalian : Akses terhadap informasi dan fungsi sistem aplikasi oleh pengguna harus dibatasi sesuai dengan kebijakan pengendalian akses yang disetujui.

e. Kabel *Fyber Optic*

Kategori Keamanan Utama A.9.2 Keamanan peralatan Kontrol Objektif: untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi		
A.9.2.3	Keamanan kabel	Pengendalian : Kabel daya dan telekomunikasi yang membawa data atau jasa informasi pendukung harus dilindungi dari ancaman bahaya terhadap kerusakan.

f. Pembuatan kebijakan dan prosedur

Pembuatan kebijakan dan prosedur dihasilkan dari kontrol objektif dan kontrol yang telah ditetapkan diatas. Prosedur juga bisa dihasilkan dari lingkup poin kebijakan. Proses yang membutuhkan penjelasan lebih rinci dapat dibuat instruksi kerja terkait dari proseur tersebut. Sedangkan didalamprosedur atau instruksi kerja yang membutuhkan dokumentasi langsung dapat dibuat rekam kerja terkait. Berikut adalah kebijakan, prosedur, instruksi kerja yang dihasilkan dalam perencanaan sistem manajemen keamanan informasi yaitu :

1. Kebijakan *Backup*
2. Kebijakan Pengendalian Akses
3. Kebijakan Penggunaan Layanan Jaringan
4. Prosedur *Backup Database*
5. Prosedur Pengendalian Hak Akses
6. Prosedur Manajamen Insiden Keamanan Informasi
7. Instruksi Kerja Pelaporan Insiden
8. Instruksi Kerja Penanganan Insiden
9. Instruksi Kerja Analisis dan Investigasi Insiden
10. Instruksi Kerja DRP

11. Instruksi Kerja Pembuatan Tiket *Helpdesk*
12. Form Pelaksanaan *Backup Database*
13. Form Pelaporan Insiden
14. Form Penanganan Insiden
15. Form Penghapusan/ Pembatalan Hak Akses
16. *Checklist* Kelengkapan DRP
17. *Checklis*t Kegiatan DRP

C. Tahap akhir

Tahap akhir merupakan hasil atau luaran dari dokumen perencanaan sistem manajemen keamanan informasi yaitu menghasilkan laporan asesmen risiko (pendekatan penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, analisa penanganan risiko, dan menetapkan kontrol objektif dan kontrol), kebijakan, prosedur, instruksi kerja, dan rekam kerja.

SIMPULAN

Kesimpulan dari perencanaan sistem manajemen keamanan informasi pada ICR PT PJB UP Gresik adalah sebagai berikut.

1. Perencanaan sistem manajemen keamanan informasi telah berhasil dilakukan pada ICR dan menghasilkan dokumen perencanaan sistem keamanan informasi meliputi laporan asesmen risiko, kebijakan, prosedur, instruksi kerja, dan rekam kerja.
2. Laporan asesmen risiko yang dilakukan pada ICR menghasilkan nilai level risiko dari masing-masing aset yang memiliki nilai paling tinggi dalam kategori Medium yaitu aset Server, *Wide Area Network* (WAN), App. Ellipse , Oracle, dan Kabel *Fyber Optic* yang memiliki penanganan risiko yang lebih utama dibanding dengan aset-aset lainnya karena risiko pada aset tersebut menimbulkan dapat yang berdampak besar bagi kelancaran proses bisnis PT PJB UP Gresik.
3. Level risiko yang dihasilkan pada laporan asesmen risiko yang memiliki nilai paling tinggi dengan tingkat medium terletak pada aset server sebesar 35,52 dan nilai terendah pada level risiko terletak pada aset kabel *fyber optic* sebesar 11,2.

SARAN

Saran yang diberikan dalam pengembangan sistem manajemen keamanan informasi pada ICR PT PJB UP Gresik yaitu untuk melanjutkan pelaksanaan sistem manajemen keamanan informasi sampai ke dalam tahap implementasi, pemantauan, dan pemelihaaran berdasarkan ISO 27001:2005.

RUJUKAN

ISO/IEC. (2005). International Standard ISO/IEC 27001 Information security management system - Requirements. ISO/IEC.

ISO/IEC. (2005). International Standard ISO/IEC 27002 – Code Of Practice For Information Security Management System. ISO/IEC.

Riyanarto Sarno, I. I. (2009). Sistem Manajemen Keamanan Informasi berbasis ISO 27001. Surabaya: ITSPress.

Informasi, T. D. (2011). Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Jakarta: KOMINFO .