BAB IV

HASIL DAN PEMBAHASAN

Pada Bab IV ini akan membahas hasil analisis dalam pembuatan perencanaan sistem manajemen keamanan informasi pada *Information Capital Readiness* PT PJB UP Gresik. Hasil yang didapatkan dari masing-masing metode dari tahap awal, tahap pengembangan, dan tahap akhir adalah sebagai berikut.

4.1 Tahap Awal

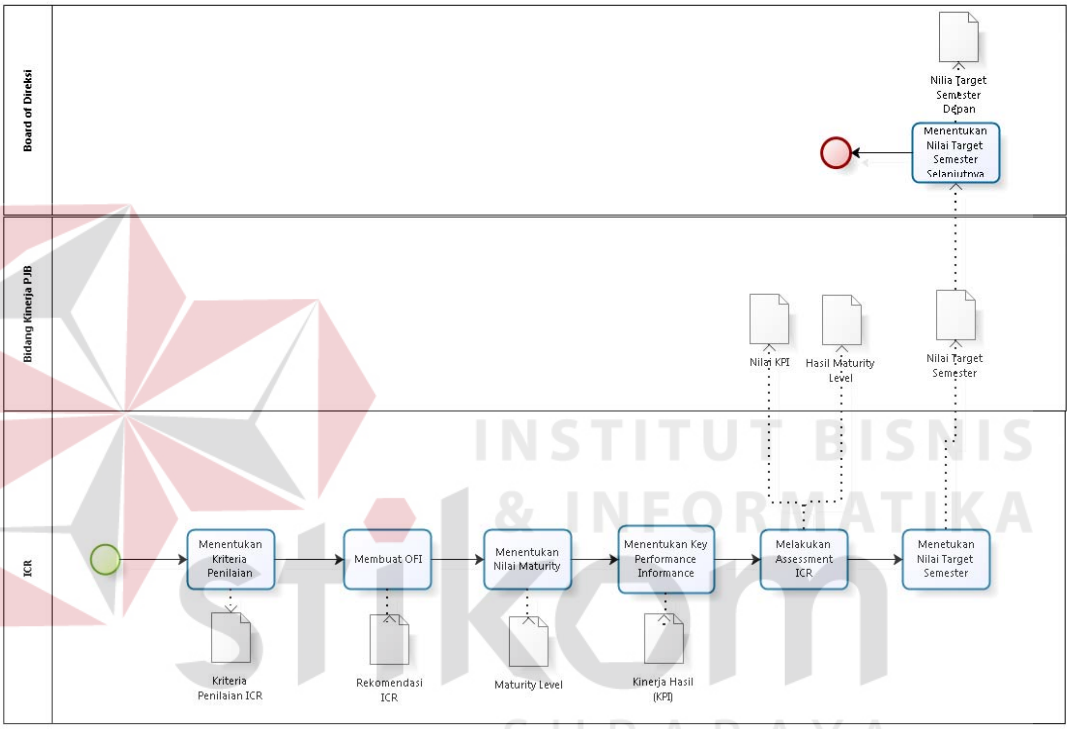
Tahap awal dilakukan dengan cara melakukan wawancara, studi literatur, dan observasi. Dari hasil tahap awal tersebut menghasilkan output pada wawancara berupa layanan pada ICR dan permasalahan pada ICR, sedangkan pada observasi berupa proses bisnis pada ICR. Studi literatur yang dibutuhkan meliputi studi literatur sistem manajemen keamanan informasi, ISO/IEC 27001:2005, ISO/IEC 27002:2010, dan cara pembuatan prosedur.

4.1.1 Wawancara

a. Proses Bisnis ICR

Dalam proses bisnis pada ICR yaitu menentukan nilai target semester yang dilakukan oleh *assesor* dengan melakukan *asessment* ICR. *Asessment* ICR terdiri dari penilaian kinerja hasil dan kinerja proses. Hasil dari *assessment* ICR tetrsebut nantinya akan diberikan kepada pihak bidang kinerja PJB kemudian diserahkan kepada direksi utama PT PJB. Hasil asessment tersebut dapat dijadikan rekomendasi dalam strategi pengembangan sistem dalam jangka waktu panjang. Nilai target yang terdapat dalam *asessment* ICR akan dijadikan acuan dalam perbaikan sistem untuk ke depannya. ICR memiliki dua bagian utama

yaitu *infrastructure* dan *application*. Pada infrastruktur mencakup beberapa area terdiri dari standarisasi *network*, kesiapan data center, kesiapan pengamanan informasi, dan *toolsmonitoring* dan *troubleshooting*. Aplikasi memiliki beberapa area diantaranya aplikasi *core business*, aplikasi *helpdesk*, dan pelatihan *key user*. Gambaran proses bisnis pada ICR dapat dilihat pada Gambar 4.1.



Gambar 4.1. Proses Bisnis ICR

b. Layanan ICR

Pada hasil wawancara pada Lampiran 1 mengenai layanan pada ICR dapat disimpulkan bahwa layanan IT yang mencakup area-area yang terdapat di dalamnya yaitu infrastruktur dan aplikasi. Detil layanan pada ICR akan dijelaskan pada Tabel 4.1

Tabel 4.1 Layanan ICR

No	Bagian	Area	Layanan
1.	Infrastruktur	Standarisasi *Network*	a. Kelengkapan *Patch* Panel
			b. Manajemen *user*
			c. Manajemen *hardware*
		Kesiapan Data Center	*a. Access control*
			b. Security monitoring
			c. Cable management
		Kesiapan Pengamanan Informasi	a. Autentifikasi user
			b. Ketersediaan antivirus dan *firewall*
		Ketersediaan *toolsmonitoring* dan *troubleshooting*	Aplikasi Toolsmonitoring (Aplikasi *Whatsup*, Aplikasi IP Centry, dan *Network Analyzer*)
2.	Aplikasi	Aplikasi *Core Business*	a. Ellipse (MIMS)
			b. Navitas (Energi Management)
			c. Sistem Manajemen Perusahaan (E-SMP)
			d. Portal Knowledge Management
			e. Aplikasi Monitoring Pengadaan (AMP)
		Aplikasi *Helpdesk*	a. Aplikasi Corvu
			b. Aplikasi *Helpdesk*

4.1.2 Observasi

a. Permasalahan pada ICR

Permasalahan yang terdapat pada ICR yaitu dalam melakukan asesmen kontrak kinerja, ICR membutuhkan kriteria-kriteria yang dapat mendukung peningkatan target untuk asesmen di tiap semesternya. Salah satu kriteria yang

belum terpenuhi pada ICR yaitu kriteria tentang pengamanan informasi. ICR belum dapat mengelola bagaimana merencanakan sebuah sistem keamanan informasi yang baik dan sesuai standar sehingga ICR membutuhkan panduan sebuah perencanaan sistem manajemen keamanan informasi agar kriteria dapat terpenuhi serta sistem keamanan informasi yang ada pada ICR dapat dikelola dan dikembangkan dengan baik. Detil hasil wawancara masalah ICR dapat dilihat pada Lampiran 2.

4.1.3 Studi Literatur

a. Penilaian Risiko berdasarkan ISO 27001:2005

Penilaian risiko yang dilakukan menurut ISO 27001:2005 memiliki beberapa tahapan yang harus dilakukan yaitu melakukan identifikasi risiko (identifikasi aset, menghitung nilai aset, menghitung nilai ancaman dan kelemahan aset, dan mengidentifikasi dampak keamanan informasi sesuai dengan kerahasiaan, keutuhan, dan ketersediaan), melakukan analisa dan evaluasi risiko (analisa dampak bisnis (BIA), mengidentifikasi level risiko, dan menetapkan apakah risiko diterima atau tidak), melakukan analisa dan penanganan risiko, serta menetapkan kontrol objektif dan kontrol berdasarkan ISO 27002:2010 bagi aset yang memiliki level risiko lebih tinggi.

b. Pembuatan Kebijakan dan Prosedur Keamanan Informasi

Kebijakan dan prosedur keamanan informasi dibuat berdasarkan pemilihan kontrol objektif dan kontrol pada salah satu aset yang memiliki level risiko lebih tinggi. Kontrol objektif dan kontrol pada ISO 27002:2010 dipilih sesuai dengan ancaman dan kelemahan yang ada pada aset. Penulisan kebijakan dan prosedur dibuat sesuai dengan ketentuan format yang ada perusahaan, jika

perusahaan tidak memiliki format tertentu maka dapat menggunakan format bebas.

c. Pembuatan Instruksi Kerja dan Rekam Kerja

Instruksi kerja dibuat apabila dalam proses prosedur membutuhkan langkah pengerjaan yang lebih rinci dan jelas, maka instruksi kerja dapat dibuat mengacu pada prosedur terkait. Rekam kerja dibuat apabila prosedur atau instruksi kerja membutuhkan dokumentasi langsung dalam setiap kegiatan yang dilakukan, maka rekam kerja akan dibutuhkan dan menjadi lampiran terkait dari prosedur atau instruksi kerja.

4.2 Tahap Pengembangan

Tahap pengembangan merupakan tahapan inti yang dilakukan pada penelitian tugas akhir ini. Pada subbab 3.3 telah menjelaskan proses dari tahap pengembangan yaitu mendapatkan persetujuan manajemen, menentukan ruang lingkup SMKI, melakukan pendekatan penilaian risiko, identifikasi risiko, analisa dan evalusi risiko, identifikasi dan penanganan risiko, menetapkan kontrol objektif dan kontrol, dan membuat prosedur keamanan informasi. Tahap pengembangan dalam prosesnya akan menghasilkan output berupa dokumen perencanaan sistem manajemen keamanan informasi.

4.2.1 Persetujuan Manajemen

Persetujuan manajemen dilakukan dengan cara melakukan wawancara dengan bagian SINFO yaitu manajer IT mengenai komitmen manajemen pada PT PJB. Hasil dari wawancara dapat dilihat pada Lampiran 3 dan kesimpulan hasil wawancara yang didapat yaitu PT PJB memiliki sebuah komitmen manajemen yang telah tertuang dalam pernyataan lampiran kebijakan manajemen nomor

063.K/020/DIR/2015 yang telah ditandatangani oleh top manajemen PT PJB mengenai visi misi, tujuan dan kompetensi inti dari organisasi dalam mengimplementasikan PJB *Integrated Management System* untuk menjalankan seluruh proses manajemen yang sesuai dengan standar nasional maupun standar internasional dari tiap unit. Kebijakan manajemen PT PJB dapat dilihat pada Lampiran 4. Dalam kebijakan manajmen tersebut PT PJB memberikan kewenangannya melalui kebijakan sistem manajemen yang tertuang ke dalam beberapa poin yaitu :

1. Menerapkan PJB-IMS secara konsisten, serta menyediakan informasi, sumber daya dan kerangka kerja dalam penyusunan dan peninjauan terhadap tujuan dan sasaran untuk meningkatkan kinerja secara berkelanjutan.
2. Mematuhi peraturan perundangan dan ketentuan lain yang berlaku terkait dengan PJB-IMS.
3. Menggunakan sumberdaya energi dan sumberdaya alam lainnya secara efisien dan bijaksana melalui pengembangan kompetensi sumber Daya Manusia dalam pengendalian operasi dan pemeliharan yang optimal guna mendukung peningkatan kinerja PJB mencapai "*Bussiness Excellence*".
4. Mengelola proses bisnis sesuai prinsip-prinsip *Good Corporate Governance* (GCG) secara sistemantis untuk mencapai optimalisasi *life cycle activity* dan *life cycle cost* dalam peningkatan ketersediaan, kehandahalan, dan efisensi pembangkit serta mendukung *Supply Chain Management* yang terkait dengan persyaratan standar guna menjamin kepuasan pelanggan dan stakeholder lainnya.

5. Mencegah terjadinya pencemaran lingkungan, kecelakaan kerja dan penyakit akibat kerja dengan mengendalikan aspek dan dampak lingkungan serta bahaya potensial keselamatan dan kesehatan kerja pada tiap kegiatan.

Dari poin-poin yang tertulis diatas keamanan informasi terletak pada poin pertama dan keempat yaitu dalam menyediakan informasi dan sumber daya yang dapat mendukung proses kinerja secara berkelanjutan serta mengelola proses bisnis sesuai dengan prinsip *Good Corporate Governance* (GCG) dalam peningkatan ketersediaan dan kehandahalan pembangkit (unit). Dalam pernyataan tersebut terlihat bahwa informasi merupakan hal yang penting terutama dalam hal keamanan yang bertujuan untuk melindungi aset, fasilitas, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab yang merupakan salah satu Sistem Manajemen Keamanan dan prinsip dari *Good Corporate Governance* (GCG) dalam meningkatkan proses bisnis PT PJB.

4.2.2 Menentukan Ruang Lingkup SMKI

Menentukan ruang lingkup SMKI dilakukan dari hasil wawancara yang dilakukan oleh staf SINFO pada Lampiran 5 diperoleh suatu informasi bahwa dalam buku pedoman kontrak kinerja unit lingkup teknologi informasi PT PJB berada pada sub direktorat sumber daya manusia teknologi informasi yaitu berada pada bagian *Information Capital Readiness* (ICR). ICR mengatur semua tentang penyediaan layanan yang menangani teknologi informasi PT PJB UP Gresik termasuk dalam hal pengamanan informasi karena pengamanan informasi merupakan salah satu kriteria utama dalam melakukan *asessment* pada ICR. Dalam menentukan ruang lingkup SMKI membutuhkan kebutuhan yang dimiliki oleh ICR dan aset-aset yang terdapat pada ICR sebagai berikut.

A. Kebutuhan ICR

Kebutuhan yang ada pada ICR yaitu dapat dibedakan menjadi dua area yaitu dari segi infrastruktur dan aplikasi yang akan ditunjukkan pada Tabel 4.2.

Tabel 4.2 Kebutuhan ICR

Area	Bagian
Infrastruktur	Keamanan *network* yang meliputi kelengkapan *patch* panel, kelengkapan kabel, manajemen *user*, dan manajemen *hardware*
	Keamanan data center meliputi *rack system*, *centralized UPS*, *cooling system*, *access control*, pemadam kebakaran, *security monitoring*, dan segmentasi *network*
	Keamanan informasi yang meliputi autentifikasi *user*, kesediaan DNS lokal, antivirus & *firewall,* dan IPS
Aplikasi	Pelatihan aplikasi *core business* bagi *key user*.
	Mencatat permasalahan IT ke dalam aplikasi *helpdesk*

B. Aset pada ICR

Aset yang dimiliki pada ICR terdiri dari beberapa bagian yaitu aset perangkat keras, aset perangkat lunak, aplikasi, aset infrastruktur, dan aset data atau informasi yang dapat dilihat pada Tabel 4.3.

Tabel 4.3. Aset ICR

Jenis Aset	Aset
Perangkat Komputer	PC
	Server
	Server Farm
Perangkat Jaringan	*Storage Area Network*
Sistem Operasi	*Network Devices*
	Windows Server
Jaringan	Windows
	Wide Area Network (WAN)

Jenis Aset	Aset
	Local Area Network (LAN
	Wireless-LAN
Aplikasi	Aplikasi Core Business
	Aplikasi Helpdesk
	Aplikasi *Toolsmonitoring*
Tools	Antivirus dan Firewall
Database	Oracle
Fasilitas	*Rack System*
	Cooling System
	Raised Floor
Jaringan	kabel FO
	Patch Panel
Listrik	*Centralized UPS*
Keamanan	*Backup* Genset
	Pemadam kebakaran
	IPS

Ruang lingkup kegiatan ICR terdiri dari dua bagian yaitu *Infrastructure* dan *Application*. Berikut ini akan dijelaskan bagian-bagian yang terdapat di dalam ICR yaitu *Infrastructure* dan *Application* :

1. *Infrastucture*

Sasaran utama bidang infrastruktur TI yaitu menyediakan infrastruktur TI yang handal dalam rangka menjamin ketersediaan *(availibility) & performance* layanan teknologi informasi, sehingga dapat beroperasi secara optimal dalam mendukung proses bisnis PT. PJB. Infrastruktur merupakan hal yang sangat penting dan berfungsi sebagai serangkaian sistem TI yang saling terkait dalam rangka menjalankan layanan teknologi informasi. Infrastuktur pada aspek ICR yang terdiri atas beberapa bagian yaitu :

a. Standarisasi *Network*

Standarisasi *network* dalam infrastruktur ICR menangani cakupan area beberapa jaringan yang ada pada PT PJB UP Gresik meliputi kelengkapan *Patch* Panel, standar terminasi, kelengkapan kabel, manajemen user, diagram topologi (dokumen topologi), dan manajemen hardware.

b. Kesiapan Data Center

Kesiapan data center dalam ICR mencakup beberapa area yaitu rak *system*, *centralized* UPS, *cooling system, access control,* pemadam kebakaran, *security monitoring, raised floor,* dan segmentasi *network.*

c. Kesiapan Pengamanan Informasi

Kesiapan pengamanan informasi pada ICR mencakup area dari autentifikasi *user*, kesediaan DNS lokal, antivirus & *firewall*, dan IPS

d. Ketersediaan *Tools Monitoring* dan *Troubleshooting*

Ketersediaan *tools monitoring* dan *troubleshooting* ini mengamati pendokumentasian dari *tools monitoring* dan *troubleshooting.*

2. *Application*

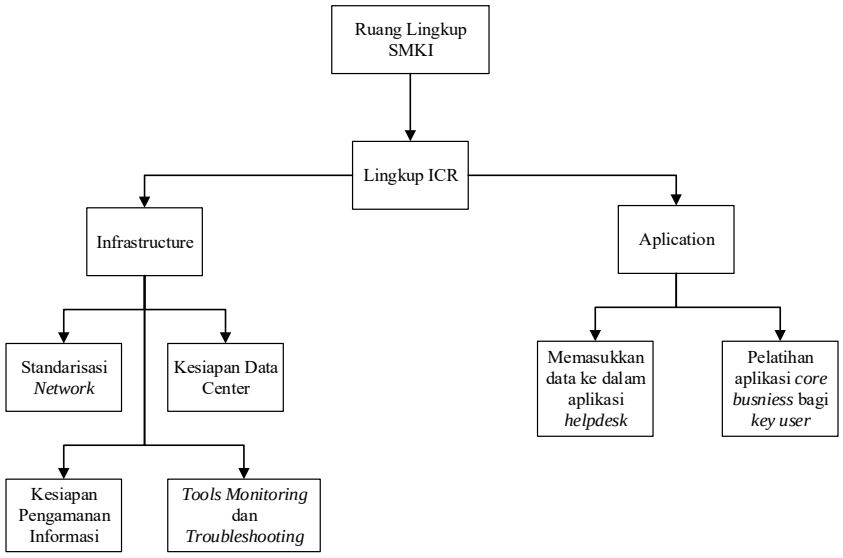
Aplikasi merupakan alat penyelarasan secara efisien suatu organisasi dengan keinginan dan kebutuhan organisasi dan berupaya untuk melakukan perbaikan proses secara berkelanjutan. Penggunaan IT dalam proses bisnis akan mempercepat proses dan efisiensi biaya. Peningkatan konsistensi penggunaan aplikasi TI bertujuan untuk meningkatkan budaya penggunaan TI dalam proses bisnis perusahaan dengan cara menjamin setiap transaksi TI dilakukan dengan benar sesuai dengan prosedur yang berlaku, sehingga data yang masuk ke dalam sistem benar dan akurat. Dalam aplikasi terdapat tiga hal yang di *assesment* yaitu :

a) Pelatihan aplikasi *core business* bagi *key user.*

b) Terdapat aplikasi *tools monitoring.*

c) Mencatat permasalahan IT ke dalam aplikasi *helpdesk.*

Dari penjelasan *assessment* aplikasi diatas dapat ditarik kesimpulan bahwa aplikasi membutuhkan pelatihan aplikasi *core business* bagi *key user* dan memasukkan data ke dalam aplikasi *helpdesk*. Aplikasi *core business* dalam PT PJB diantaranya adalah Aplikasi Ellipse (MIMS), Navitas (Energi Management), Sistem Manajemen Perusahaan (E-SMP), *Portal Knowledge Management*, Aplikasi *Monitoring* Pengadaan (AMP), dan Aplikasi PBViews. Aplikasi Ellipse digunakan untuk manajemen asset dengan mengintegrasikan modul – modul aplikasi. Aplikasi Navitas digunakan untuk memanajemen *informasi operasi* unit pembangkit. Aplikasi E-SMP digunakan sebagai alat bantu pengadministrasian dan persetujuan dalam proses pengaturan dokumen-dokumen ISO. Aplikasi Portal *Knowledge management* digunakan untuk pintu gerbang menuju informasi yang terbaru selain akses untuk aplikasi internal PJB. Aplikasi AMP digunakan untuk *monitoring* pengadaan. Aplikasi Portal *Knowledge management* digunakan untuk pintu gerbang menuju informasi yang terbaru selain akses untuk aplikasi internal PJB. Aplikasi PBViews digunakan untuk pengukuran kinerja yang difokuskan pada pengukuran kegiatan yang berkontribusi untuk mencapai tujuan organisasi. Sedangkan aplikasi *helpdesk* terdiri dari dua aplikasi pendukung yaitu aplikasi Corvu dan aplikasi *Helpdsk*. Aplikasi untuk *toolsmonitoring* yaitu aplikasi Whatsup, aplikasi IP Centry, dan *Network Analyzer*. Ruang lingkup SMKI dapat dilihat pada Gambar 4.2.



Gambar 4.2. Ruang Lingkup SMKI

4.2.3 Menentukan Pendekatan Penilaian Risiko

A. Metode *Risk Asessment*

Metode yang digunakan dalam penilaian risiko pada ICR PT PJB UP Gresik yaitu menggunakan metode kualitatif dengan cara melakukan brainstroming, wawancara, analisis dan historis, pengamatan, survei, teknik delphi, dan *checkslist.* Metode kualitatif dipilih berdasarkan dengan Surat Keputusan Direksi no 128. K/D10/DIR/2014 tentang Penerapan Manajemen Risiko di Lingkungan PT PJB yang mengarah kepada standar COSO dan ISO 31000 tentang Manajemen Risiko. Detil wawancara dalam melakukan pendektan penilaian risiko dapat dilihat pada Lampiran 6 dan SK Direksi no 128. K/D10/DIR/2014 dapat dilihat pada Lampiran 7.

Metode kualitatif pada penilaian risiko di lingkungan PT PJB dipilih karena mempunyai keuntungan diantaranya :

a) Relatif lebih mudah untuk dilakukan
b) Mudah dikomunikasikan kepada organisasi

c) Tidak membutuhkan perhitungan analisis data yang besar.

B. Kriteria Penerimaan Risiko

Kriteria dalam penerimaan risiko PT PJB telah ditetapkan berdasarkan Surat Keputusan Direksi no 128. K/D10/DIR/2014 tentang Penerapan Manajemen Risiko di Lingkungan PT PJB. SK Direksi tersebut dibuat bedasarkan referensi dari standar COSO dan ISO 31000. Kriteria penerimaan risiko dalam PT PJB dibagi menjadi 4 bagian diantaranya yaitu :

1. Risiko diterima (*Risk Acceptance*) yaitu risiko diterima dengan segala dampaknya dan risiko tersebut tidak menggangu proses bisnis dalam organisasi.
2. Risiko direduksi (*Risk Reduction*) yaitu risiko direduksi atau dikontrol apabila risiko yang dihasilkan masih dapat ditanggulangi dengan menggunakan kontrol-kontrol yang ada.
3. Risiko dihindari atau Ditolak (*Risk Avoid*) yaitu risiko ditolak atau dihindari yaitu memutuskan untuk tidak melakukan aktivitas yang mengandung risiko sama sekali. Dalam memutuskan untuk melakukannya, maka harus dipertimbangkan potensial keuntungan dan potensial kerugian yang dihasilkan oleh suatu aktivitas.
4. Risiko dialihkan kepada pihak ketiga (*Risk Transfer*) yaitu berbagi risiko dengan pihak lain atau pihak (termasuk kontrak dan pembiayaan risiko) .

Perkiraan penerimaan risiko yaitu ditentukan apabila level risiko yang dihasilkan bernilai *Low*, maka risiko tersebut diterima (*Risk Acceptance*) dan tidak memerlukan pengolahan risiko lebih lanjut. Sedangkan untuk level risiko yang bernilai *Medium* dan *High*, maka risiko tersebut perlu mendapatkan pengolahan

risiko dengan menetapkan perlakuan risiko yaitu dengan menetapkan kontrol terhadap risiko (*Risk Reduction*), risiko dihindari atau ditolak (*Risk Avoid*), dan risiko dialihkan kepada pihak ketiga (*Risk Transfer*).

4.2.4 Identifikasi Risiko

Identifikasi risiko berdasarkan ISO 27001 pada PT PJB UP Gresik dilakukan dengan beberapa langkah sebagai berikut.

A. Identifikasi Aset

Identifikasi aset pada PT PJB UP Gresik bertujuan untuk menentukan aset-aset yang ada pada *information capital readiness* (ICR) pada bagian infrastuktur dan aplikasi. Berdasarkan hasil observasi yang dilakukan pada manajer SINFO, maka aset pada ICR PT PJB UP Gresik dapat digolongkan menjadi beberap jenis seperti aset perangkat keras (hardware), aset perangkat lunak (software), aset infrastruktur, dan aset informasi. Identifikasi jenis aset pada ICR dapat dilihat pada Tabel 4.4.

Tabel 4.4. Identifikasi Aset

No	Jenis Aset	Aset	
1	Aset Perangkat Keras (*Hardware*)	Perangkat Komputer	PC
			Server
			Server Farm
		Perangkat Jaringan	*Storage Area Network*
2	Aset Perangkat Lunak (Software)	Sistem Operasi	*Network Devices*
			Windows Server
		Jaringan	Windows
			Wide Area Network (WAN)
			Local Area Network (LAN
			Wireless-LAN
		Aplikasi	Aplikasi Core Business :

No	Jenis Aset	Aset	
			▪ Ellipse (MIMS)
			▪ Navitas (Energi Management)
			▪ Sistem Manajemen Perusahaan (E-SMP)
			▪ *Portal Knowledge Management*
			▪ Aplikasi *Monitoring* Pengadaan (AMP)
			Aplikasi Helpdesk
			Aplikasi *Toolsmonitoring* :
			▪ App. Whatsup
			▪ App. IP Centry
			▪ Network Analyzer
		Tools	Antivirus dan Firewall
		Database	Oracle
3	Aset Infrastruktur	Fasilitas	*Rack System*
			Cooling System
			Raised Floor
		Jaringan	kabel FO
			Patch Panel
		Listrik	*Centralized UPS*
		Keamanan	*Backup* Genset
			Pemadam kebakaran
			IPS
	Aset Data dan Informasi	Database	tabel *User* dan *Password*
		Materi training	Pelatihan aplikasi *Core Bussiness*

B. Menghitung Nilai Aset

Setelah melakukan identifikasi aset, langkah selanjutnya adalah melakukan perhitungan nilai aset berdasarkan pada pendekatan aspek keamanan informasi yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan

ketersediaan *(availiability*). Penilaian aset berdasarkan kriteria dari aspek diatas dapat dijelaskan pada Tabel 2.1 kriteria kerahasiaan (*confidentiality*), Tabel 2.2 kriteria keutuhan (*integrity*), dan Tabel 2.3 kriteria ketersediaan (*availability*).

Setelah mendefinisikan kriteria sesuai dengan aspek keamanan informasi, maka langkah selanjutnya yaitu melakukan perhitungan nilai aset dengan menggunakan persamaan matematis pada rumus 2.1 yaitu Nilai Aset (NS) = NC + NI + NA

Keterangan :

NC = Nilai *Confidentialy*

NI = Nilai *Integrity*

NA = Nilai *Availability*

Dari hasil wawancara dan observasi yang dilakukan diperoleh nilai dari masing-masing aset pada ICR yang dapat dilihat pada Tabel 4.5.

Tabel 4.5. Nilai Aset ICR

No	Aset	Kriteria			Nilai Aset (NC+NI+NA)
		NC	NI	NA	
1.	PC	2	0	1	3
2.	Server	4	4	4	12
3.	*Storage Area Network*	3	3	4	10
4.	*Network Devices*	2	2	1	5
5.	Windows Server	2	2	3	7
6.	Windows	1	2	1	4
7.	*Wide Area Network* (WAN)	2	3	3	8
8.	*Local Area Network* (LAN	1	2	2	5
9.	*Wireless*-LAN	1	3	1	5
10.	Server Farm	1	2	1	4
11.	*Patch* Panel	0	2	1	3
12.	Ellipse (MIMS)	3	2	3	8
13.	Navitas (Energi Management)	2	2	3	7

No	Aset	Kriteria			Nilai Aset (NC+NI+NA)
14.	Sistem Manajemen Perusahaan (E-SMP)	3	3	2	8
15.	*Portal Knowledge Management*	3	3	4	10
16.	Aplikasi *Monitoring* Pengadaan (AMP)	3	3	2	8
17.	Aplikasi Helpdesk	2	1	1	4
18.	App. Whatsup	2	1	1	4
19.	App. IP Centry	2	1	2	5
20.	Network Analyzer	2	2	2	6
21.	Antivirus dan Firewall	0	2	1	3
22.	Firewall	3	3	3	9
23.	Oracle	3	4	4	11
24.	*Rack System*	1	0	1	2
25.	*Cooling System*	1	0	2	3
26.	*Raised Floor*	1	0	1	2
27.	kabel FO	3	3	2	8
28.	*Centralized UPS*	1	3	2	6
29.	*Backup* Genset	1	0	1	2
30.	Pemadam kebakaran	0	0	2	2
31.	IPS	1	2	3	6
32.	tabel *User* dan *Password*	2	2	1	5
33.	Pelatihan aplikasi core bussiness	0	0	0	0

C. Mengidentifikasi Ancaman dan Kelemahan terhadap Aset

Tahapan selanjutnya setelah menghitung nilai aset yaitu mengidentifikasi ancaman dan kelemahan dari tiap aset yang telah diidentifikasi sebelumnnya. Dalam mengidentifikasi ancaman (*threat*) dan kelemahan (*vulnerable*) yang terdapat pada aset dapat dibuat tabel yang dinamakan tabel kemungkinan kejadian (*Probality of Occurrance*). Sebelum membuat tabel kemungkinan kejadian maka langkah sebelumnya yaitu menentukan rerata nilai probalitas. Rentang nilai dari probalitas yang telah ditentukan yaitu sebagai berikut.

LOW : nilai rerata probalitas 0,0 – 0,4

MEDIUM: nilai rerata probalitas 0,5 – 0,7

HIGH : nilai rerata probalitas 0,8 – 1,0

Setelah menentukan rerata nilai probalitas, maka dapat dihitung nilai ancaman dari suatu aset dengan menggunakan rumus yang terdapat pada rumus 2.2 yaitu

Nilai Ancaman (NT) = ∑PO / ∑Ancaman

dimana :

∑ PO : Jumlah rerata probabilitas (*Probability of Occurance)*

∑ Ancaman : Jumlah Ancaman

Dibawah ini merupakan contoh dari perhitungan nilai ancaman pada aset PC dapat dilihat pada Tabel 4.8.

1. Nilai ancaman terhadap aset PC dapat dilihat pada Tabel 4.6.

Tabel 4.6 . Nilai Ancaman PC

No	Ancaman	Jenis	Probabilitas	Rerata Probabilitas
1	Pencurian PC	Ancaman	Low	0,1
2	Serangan Virus	Kelemahan	High	0,8
3	Gangguan Perangkat Keras	Ancaman	Low	0,2
4	Akses Ilegal	Ancaman	Medium	0,5
Jumlah Ancaman= 4		Jumlah rerata Prob		1,6

NT (PC) = ∑PO / ∑Ancaman

= 1,6 / 4 = 0,4

Nilai ancaman untuk aset PC adalah 0,4 .

Detil nilai ancaman dapat dilihat pada Lampiran 9 dan rekap dari nilai ancaman pada masing-masing aset dapat ditunjukkan pada Tabel 4.7.

Tabel 4.7. Nilai Ancaman masing-masing Aset

No	Aset	Nilai Ancaman
1	PC	0,4
2	Server	0,74
3	*Storage Area Network*	0,34
4	*Network Devices*	0,175
5	Windows Server	0,63
6	Windows	0,46
7	*Wide Area Network* (WAN)	0,53
8	*Local Area Network* (LAN	0,325
9	*Wireless*-LAN	0,56
10	Server Farm	0,55
11	Aplikasi Sistem Manajemen Pengamanan (SMP)	0,55
12	Ellipse (MIMS)	0,64
13	Navitas (Energi Management)	0,43
14	Sistem Manajemen Perusahaan (E-SMP)	0,5
15	*Portal Knowledge Management*	0,47
16	Aplikasi *Monitoring* Pengadaan (AMP)	0,43
17	Aplikasi Helpdesk	0,3
18	App. Whatsup	0,43
19	App. IP Centry	0,33
20	Network Analyzer	0,4
21	Antivirus	0,45
22	Firewall	0,55
23	Oracle	0,63
24	*Rack System*	0,35
25	*Cooling System*	0,15
26	*Raised Floor*	0,3
27	kabel FO	0,7
28	*Centralized UPS*	0,5
29	*Backup* Genset	0,475
30	Pemadam kebakaran	0
31	IPS	0,67
32	tabel *User* dan *Password*	0,4
33	Pelatihan aplikasi core bussiness	0,45

D. Identifikasi Dampak jika terjadi Kegagalan Aspek Keamanan Informasi (CIA)

Mengidentifiasi dampak jika terjadi kegagalan aspek keamanan informasi yang dilakukan dengan mengidentifikasi dampak dari masing-masing aset sesuai dengan aspek keamanan informasi yaitu Kerahasiaan (Confidentiality), Keutuhan (Integrity), dan Ketersediaan (Availability).Berikut adalah salah satu identifikasi dampak dari tiga aset pada ICR. Detil dampak keamanan informasi dapat dilihat pada Lampiran 10.

1. Dampak keamanan informasi PC ditunjukkan pada Tabel 4.8.

Tabel 4.8. Dampak Keamanan Informasi pada PC

Kategori	Dampak
Kerahasiaan	Jika data yang terdapat pada PC diakses tanpa ijin dapat menyebabkan kerugian seperti kehilangan data utama, perubahan informasi yang dikases secara ilegal, dan kerahasiian dari data-data utama dapat diketahui oleh pihak luar yang tidak bertanggungjawab dapat menggangu dan memberikan kerugian bagi individu yang bersangkutan, proses bisnis bagi SINFO, dan proses bisnis intrernal PT PJB. (Referensi: ISO/IEC 27002:2005, menurut Garfinkel dan Spafford).
Keutuhan	Jika PC mengalami kerusakan atau terkena virus, data dan informasi yang ada di dalam PC dapat rusak (*corupt*) akibatnya informasi yang ada di dalam PC menjadi tidak utuh dan akurat. (Referensi: ISO/IEC 27002:2005, menurut Garfinkel dan Spafford).
Ketersediaan	Jika PC tidak dapat mengotorifikasi hak akses dari pemilik PC , maka pengguna (pemilik PC) tidak dapat mengakases data dan informasi yang berada pada PC. (Referensi: ISO/IEC 27002:2005, menurut Garfinkel dan Spafford).

2. Dampak keamanan informasi Server ditunjukkan pada Tabel 4.9.

Tabel 4.9. Dampak Keamanan Informasi pada 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 dan kehilangan data yang terdapat pada server disalahgunakan oleh pihak yang tidak bertanggung jawab. (Referensi: ISO/IEC 27001:2005, ISO/IEC 27002:2005, dan TIA 942).
Keutuhan	Jika server mengalami kerusakan, maka semua data yang terdapat di dalam PC dapat menjadi corupt bahkan hilang akibatnya informasi yang dihasilkan tidak utuh dan valid. (Referensi: ISO/IEC 27001:2005, ISO/IEC 27002:2005, dan TIA 942).
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. (Referensi: ISO/IEC 27001:2005, ISO/IEC 27002:2005, dan TIA 942).

3. Dampak keamanan informasi *Storage Area Network* pada Tabel 4.10.

Tabel 4.10. Dampak Keamanan Informasi pada *Storage Area Network*

Kategori	Dampak
Kerahasiaan	Jika *storage* diakses oleh pihak yang tidak bertanggung jawab bukan pada pemilik hak akses sesungguhnya dapat menimbulkan dampak yang sangat besar karena data yang terdapat pada penyimpanan tersebut dapat rusak atau hilang akibatnya data utama pada aplikasi *core business* atau aplikasi-aplikasi lain dapat hilang atau disalahgunakan oleh pihak yang tidak bertanggung jawab. (Referensi: ISO/IEC 27002:2005).

Kategori	Dampak
Keutuhan	Jika *storage* mengalami kerusakan dapat mengakibatkan data dan informasi yang tersimpan di dalam storage mengalami kerusakan atau bahkan informasi yang ada dapat berubah dan menjadi tidak valid. (Referensi: ISO/IEC 27002:2005).
Ketersediaan	Gangguan terhadap akses informasi yang terdapat pada *storage* tidak berfungsi dengan baik dapat mengakibatkan kerugian bagi staf, organisasi, dan pimpinan saat ingin mengakses sehingga data utama yang dibutuhkan tidak dapat tersedia karena gangguan eksternal maapun internal pada *storage.* (Referensi: ISO/IEC 27002:2005).

4.2.5 Analisa dan Evaluasi Risiko

Analisa risiko dan evaluasi risiko untuk menentukan level risiko dari masing-masing aset yang dilakukan dengan beberapa langkah sebagai berikut.

A. Melakukan Analisa Dampak Bisnis (*Bussiness Impact Analysis*)

Analisa dampak bisnis dilakukan dengan menentukan nilai BIA pada aset yang mengacu pada skala nilai BIA yang dapat dilihat pada Tabel 2.5. Nilai BIA pada masing-masing aset di dapat dari berbagai referensi yaitu :

1. *Telecommunications Infrastructure Standard for Data Centers* (TIA-942) yaitu untuk mendefinisikan standar infrastruktur komunikasi dalam data center yang menjelaskan bahwa dalam membangun data center yang baik dibutuhkan sebuah infrastruktur pendukung yaitu *cooling system, raised floor, rack system, centralized UPS, patch panel*, dan *backup* genset untuk membuat fasilitas keamanan bagi server yang masing-masing mempunyai peranan penting sehingga apabila salah satu infrastruktur pendukung (*cooling system, raised floor, rack system, centralized UPS, patch panel*, dan *backup*

genset) tidak tersedia atau rusak memiliki batas toleran penanganan sampai 1 hari, maka kinerja server tidak dapat berjalan dengan maksimal. Server harus dijaga agar tidak *down* atau mengalami gangguan dan apabila server mengalami gangguan harus segera diperbaiki tidak boleh lebih dari 1 jam karena apabila server rusak, maka perusahaan akan menanggung kerugian finansial yang sangat besar.

2. Instruksi Kerja Perbaikan Komputer dengan no IKG-07.1.4.8 adalah dokumen yang mengatur tentang tatacara dalam menangani perbaikan komputer atau PC agar data dan informasi tetap terjaga, pada perbaikan komputer/ PC dapat dilakukan dalam waktu 1 hari karena setiap didalam PC banyak terdapat data dan informasi penting bahkan rahasia sehingga apabila data dan informasi tesebut tidak segera diselamatkan staf PJB tidak dapat memaksimalkan kinerjanya.
3. Prosedur Operasi Baku *Strorage Area Network* dengan no POB-PA.02 adalah prosedur yang menjelaskan tentang alur rinci dalam menangani *strorage* dari pengelolaan, pemeliharaan, dan perbaikan pada *strorage* PT PJB. dalam poin perbaikan pada *strorage* dapat dilakukan oleh teknisi selama 1 hari dan tidak boleh lebih karena jika lebih data-data pada aplikasi *core bussiness* dan aplikasi unit tidak dapat tersimpan.
4. Instruksi Kerja Pengamanan Jaringan no IKG-07.1.4.6 adalah dokumen yang mengatur arahan secara rinci terhadap pengamanan jaringan dari WAN.LAN, dan WLAN serta infrastruktur jaringan pendukung seperti kabel *fyber optic*, *router, swtich*, hub, *firewall,* dan IPS yang harus selalu dijaga agar tidak mengalami kerusakan atau gangguan karena jika perangkat jaringan tersebut rusak sampai lebih dari 1 hari, maka seluruh aplikasi pusat dan unit tidak akan dapat diakses, sedangkan kabel *fyber optic* harus selalu dijaga dari kerusakan selama kurang dari 1 jam.

5. Prosedur Operasi Baku *Wide Area Network* dengan no POB-PS.03 adalah prosedur yang menjelaskan tentang alur rinci dalam menangani WAN dari pengelolaan, pemeliharaan, dan perbaikan pada WAN PT PJB. Dalam dokumen tentang pengolahan menjelaskan bahwa WAN tidak boleh mengalami gangguan atau serangan dari luar sehingga apabila WAN mengalami gangguan unit harus segera melakukan penanganan dalam waktu kurang dari 1 jam untuk memulihkan koneksi jaringan antar PJB.
6. Prosedur Operasi Baku *Local Area Network* dengan no POB-PS.02 adalah prosedur yang menjelaskan tentang alur rinci dalam menangani LAN dari pengelolaan, pemeliharaan, dan perbaikan pada LAN PT PJB. Dalam dokumen tentang perbaikan menjelaskan bahwa LAN tidak boleh mengalami gangguan atau serangan dari luar sehingga apabila LAN mengalami gangguan unit harus segera melakukan penanganan dalam waktu 1 hari untuk memulihkan koneksi jaringan dalam unit.
7. Prosedur Operasi Baku Pemadam Kebakaran dengan no POB-PS.07 adalah prosedur yang menjelaskan tentang tatacara dalam menggunakan, mengelola, dan meninjau sistem keamanan dalam mencegah terjadinya kebakaran. Dalam dokumen tersebut menjelaskan bahwa alat pemadam kebakaran harus selalu tersedia 24 jam dan berfungsi dengan baik.
8. Prosedur Operasi Baku *Security System* no POB-PA.11 adalah prosedur yang menjelaskan sistem keamanan yang berfungsi dalam melindungi aset data dan informasi dengan menerapkan sistem keamanan yaitu antivirus dan *firewall.* Antivirus dan firewall harus selalu dijaga dan ditinjau fungsi dan cara kerja agar tidak mengalami gangguan baik dari akses fisik maupun lojik karena jika antivirus& *firewall* mengalami gangguan harus segera ditangani tidak lebih dari 1 hari.
9. Prosedur Operasi Baku Pengolahan Aplikasi no POB-PA.14 adalah prosedur yang menjelaskan bagaimana mengelola, meninjau, dan memelihara aplikasi *core bussiness* dan aplikasi unit agar setiap data dan informasi yang terdapat dapat terjaga

kerahasiaan, keutuhan, dan ketersediaanya dari akses pihak yang tidak bertanggung jawab. Aplikasi *core bussiness* dan aplikasi Ellipse tidak boleh *down* atau mengalami gangguan lebih dari 1 jam karena jika mengalami gangguan, maka proses bisnis PJB akan terhambat, sedangkan aplikasi *core bussiness* dan aplikasi unit lainnya tidak boleh *down* selama kurang dari 1 hari.

10. Prosedur Operasi Baku Inventarisasi *Software* dengan no POB-PA.15 adalah prosedur yang mengatur tentang pengadaan dan pemeliharaan *software* yang meliputi oracle, window server dan window yang merupaka aset perangkat lunak yang sangat berperan penting dalam PT PJB karena sistem operasi merupakan alat pendukung dalam mendukung kinerja staf/karyawan dan proses bisnis PJB. Oracle harus selalu tersedia dan tidak boleh down selama lebih dari 1 jam. Window server harus selalu tersedia dan apabila window server mengalami gangguan harus segera diperbaiki dalam waktu kurang dari 1 hari, sedangkan window dapat diperbaiki dalam waktu 1 hari.
11. SK direksi no 047.K/020/UPGRK/2015 merupakan surat keputusan direksi tentang susunan keanggotaan tim *key user* aplikasi teknologi informasi unit pembangkitan Gresik yang didalamnya mengatur pentingnya sebuah pelatihan bagi *key user* agar para staf/karyawan dapat mengoperasikan aplikasi *core bussiness* dengan baik. Pelatihan *key user* dapat dilakukan dalam kurun waktu kurang dari 1 minggu.

Setelah menentukan referensi dari masing-masing nilai BIA pada aset, maka nilai analisa dampak bisnis pada masing-masing aset yang ditunjukkan pada Tabel 4.11.

Tabel 4.11 Nilai BIA pada masing-masing Aset

No	Aset	Dampak	Nilai BIA	Referensi
1	PC	Pelaporan data pada aplikasi core bussiness tertunda karena gangguan pada PC	1	Instruksi kerja perbaikan komputer no IKG-07.1.4.8

No	Aset	Dampak	Nilai BIA	Referensi
2	Server	Operasi layanan aplikasi pusat dan unit terhenti	4	Standar TIA-942
3	*Storage Area Network*	Penyimpanan data pusat dan unit terhenti atau tertunda	1	POB *Storage Area Network* no POB-PA.02
4	*Network Devices*	Jaringan antar unit terhenti sehingga komunikasi antar bagian terganggu	1	Instruksi kerja pengamanan jaringan no IKG-07.1.4.6.
5	Windows Server	Pelayanan terhadap admin data center terganggu sehingga dapat menghambat kinerja pengguna.	2	POB inventarisasi no POB-PA.15
6	Windows	Pelayanan terhadap individu (*user*) terganggu	1	POB inventarisasi no POB-PA.15
7	*Wide Area Network* (WAN)	Komunikasi antar PT PJB di Indonesia terhenti dan dapat menggangu pelayanan antar unit PJB.	4	POB WAN no POB-PS.03.
8	*Local Area Network* (LAN	Komunikasi antar unit terhenti dan dapat menggangu pelayanan terhadap *user*.	1	POB LAN no POB-PS.02
9	*Wireless*-LAN	Komunikasi *online* antar bagian tertunda akibat gangguan.	1	Instruksi kerja pengamanan jaringan no IKG-07.4.
10	Server Farm	Layanan operasi server cadangan tidak beroperasi	4	Standar TIA-942
11	*Patch* Panel	Tidak dapat mengkoneksikan jaringan yang ada pada *network devices*	1	Standar TIA-942
12	Ellipse (MIMS)	Sistem informasi manajamen aset menjadi terhambat	4	POB pengolahan aplikasi no POB-PA.14
13	Navitas (Energi Management)	Sistem informasi operasi unit menjadi terhambat	2	POB pengolahan aplikasi no POB-PA.14
14	Sistem Manajemen	Proses administrasi dan persetujuan pengaturan dokumen ISO terhambat	2	POB pengolahan aplikasi no

No	Aset	Dampak	Nilai BIA	Referensi
	Perusahaan (E-SMP)			POB-PA.14
15	*Portal Knowledge Management*	Integrasikan antara aplikasi PJB yang berbasis WEB (*single sign on*) terhambat	2	POB pengolahan aplikasi no POB-PA.14
16	Aplikasi *Monitoring* Pengadaan (AMP)	Monitoring proses pengadaan barang PT PJB UP Gresik terhambat	2	POB pengolahan aplikasi no POB-PA.14
17	Aplikasi Helpdesk	Modul-modul dalam aplikasi helpdek menjadi terhambat	2	POB pengolahan aplikasi no POB-PA.14
18	App. Whatsup	Pelaporan monitoring network tertunda	2	POB pengolahan aplikasi no POB-PA.14
19	App. IP Centry	Pelaporan avaibility dan performance network tertunda	2	POB pengolahan aplikasi no POB-PA.14
20	Network Analyzer	Pelaporan monitoring dan troubleshooting tertunda	4	POB pengolahan aplikasi no POB-PA.14
21	Antivirus	Merusak PC, OS, dan aplikasi yang berkaitan dengan kelangsungan proses bisnis PT PJB	2	POB *security system* no POB-PA.
22	Firewall	Kontrol akses antar 2 jaringan berlainan terhenti	2	POB *security system* no POB-PA.
23	Oracle	*Database* aplikasi pusat tidak dapat beroperasi	4	POB inventarisasi no POB-PA.15
24	*Rack System*	Kelangsungan proses bisnis data center tidak berjalan maksimal dan tidak sesuai standar keamanan yang telah ditetapkan	1	Standar TIA-942
25	*Cooling System*	Server tidak dapat berjalan dengan maksimal karena panas dan tidak sesuai standar keamanan yang	1	Standar TIA-942

No	Aset	Dampak	Nilai BIA	Referensi
		telah ditetapkan		
26	*Raised Floor*	Kinerja dari data center tidak berlangsung baik dan tidak sesuai standar keamanan yang telah ditetapkan	1	Standar TIA-942
27	Kabel FO	Transfer data dan koneksi jaringan tidak dapat digunakan untuk mengakses aplikasi pusat dan unit	4	Instruksi kerja pengamanan jaringan no IKG-07.4.
28	*Centralized UPS*	Listrik pada data center PT PJB UP Gresik terhenti	1	Standar TIA-942
29	*Backup* Genset	*Backup* data pada data center tidak dapat beroperasi	1	Standar TIA-942
30	Pemadam kebakaran	Dapat menimbulkan kebakaran pada PT PJB UP Gresik	4	POB pemadam kebakaran no POB-PS.07
31	IPS	*Monitoring traffic* jaringan yang mencurigakan tidak beroperasi.	1	Instruksi kerja pengamanan jaringan no IKG-07.4.
32	tabel *User* dan *Password*	Pengguna tidak mempunyai kontrol akses sehingga dapat menimbulkan akses ilegal oleh pihak lain.	4	POB *Security System* no POB-PA.11 dan POB pengolahan aplikasi no POB-PA.14
33	Pelatihan aplikasi *core bussiness*	*Key user* tidak mendapatkan pengetahuan untuk mengoperasikan aplikasi *core bussines*	0	SK direksi no 047.K/020/UP GRK/2015.

B. Mengidentifikasi Level Risiko

Setelah melakukan analisa dampak bisnis langkah selanjutnya yaitu mengidentifikasi level risiko yang akan digunakan untuk menentukan pilihan penanganan risiko. Level risiko yang mungkin dapat diterima oleh PT PJB UP

Gresik dapat ditentukan berdasar hubungan probabilitas ancaman dengan dampak bisnis yang ditimbulkan. Level probabilitas ancaman dapat dilihat pada Tabel 4.12

Tabel 4.12 Level Probabilitas

Level Probabilitas
0 < Low Probability < 0,1
0,1 < Medium Probability < 0,5
0,5 < High Probability < 1,0

Sedangkan level dampak (*impact*) dapat dilihat pada Tabel 4.13.

Tabel 4.13 Level Dampak

Level Dampak
0 < Not Critical impact < 20
20 < Low Critical impact < 40
40 < Medium Critical impact < 60
60 < High Critical impact < 80
80 < Very High Critical impact < 100

Berdasarkan ketentuan probabilitas ancaman dan dampak bisnis yang telah ditentukan pada Tabel 4.13 dan Tabel 4.14 sebelumnya, maka matriks level risiko yang dibuat dapat dilihat pada Tabel 2.6 sebelumnya. Matriks level risiko yang terdiri dari dampak bisnis (*impact)* dan kemungkinan (*probability*) dapat menghasilkan pengukuran nilai level risiko sesuai dengan dampak dan kemungkinan yang ditimbulkan dan mengacu pada pedoman umum manajemen risiko PT PJB dengan nomor 128.K/D10/DIR/2014 yaitu :

1. Dampak bisnis (*impact*) :
   a. *Not Critical* : Dapat merusak komputer *client* karena virus, spam, dan *malware*
   b. *Low Critical* : Dapat merusak LAN unit atau kantor pusat
   c. *Medium Critical* : Dapat merusak infrastruktur WAN PJB
   d. *High Critical* : Dapat merusak *database*/ aplikasi dan server
   e. *Very High Critical* : Data center PJB kantor pusat tidak berfungsi total karena bencana alam
2. Kemungkinan (*probability*):
   a. *Low* : Kemungkinan risiko tidak terjadi < 5 tahun
   b. *Medium* : Kemungkinan risiko dapat terjadi dalam rentan waktu 1 tahun
   c. *High* : Kemungkinan risiko terjadi lebih dari 12 kali dalam setahun

Pengukuran berdasarkan dampak dan kemungkinan tersebut digunakan untuk mendeskripsikan masing-masing nilai level risiko yang akan dihasilkan yang mengacu pada matriks level risiko yang telah dibuat sebelumnya.

C. Menentukan Risiko Diterima atau Perlu Penanganan Risiko

Sebelum menentukan risiko diterima atau perlu penangan risiko lebih lanjut,terlebih dahulu harus menghitung nilai risiko dari masing-masing aset. Cara menghitung nilai risiko dapat dihitung dengan persamaan matematis yang ada pada rumus 2.3 yaitu *Risk Value* = NA x BIA x NT

dimana :

Risk Value : Nilai Risiko

NA : Nilai Aset

BIA : Nilai BIA

NT : Nilai Ancaman

Dari hasil perhitungan yang telah dilakukan, maka dapat ditentukan nilai risiko dari masing-masing aset yang akan ditunjukkan pada Tabel 4.14

Tabel 4.14 Nilai Risiko pada Aset

No	Aset	Nilai Aset	Nilai BIA	Nilai Ancaman	Nilai Risiko
1	PC	3	1	0,4	1,2
2	Server	12	4	0,74	35,52
3	*Storage Area Network*	10	1	0,34	3,4
4	*Network Devices*	5	1	0,175	0,875
5	Windows Server	7	4	0,63	8,82
6	Windows	4	1	0,46	1,84
7	*Wide Area Network* (WAN)	8	4	0,53	16,96
8	*Local Area Network* (LAN	5	1	0,325	1,625
9	*Wireless*-LAN	5	1	0,56	2,8
10	Server Farm	4	4	0,55	8,8
11	*Patch* Panel	3	1	0,5	1,5
12	Ellipse (MIMS)	8	4	0,64	20,48
13	Navitas (Energi Management)	7	4	0,43	6,02
14	Sistem Manajemen Perusahaan (E-SMP)	8	4	0,5	8
15	*Portal Knowledge Management*	10	4	0,47	9,4
16	Aplikasi *Monitoring* Pengadaan (AMP)	8	4	0,43	6,88
17	Aplikasi Helpdesk	4	4	0,3	2,4
18	App. Whatsup	4	4	0,43	3,44
19	App. IP Centry	5	4	0,33	3,3
20	Network Analyzer	6	4	0,4	9,6
21	Antivirus	3	2	0,45	2,7

No	Aset	Nilai Aset	Nilai BIA	Nilai Ancaman	Nilai Risiko
22	Firewall	9	2	0,55	9,9
23	Oracle	11	4	0,63	27,72
24	*Rack System*	2	1	0,35	0,7
25	*Cooling System*	3	1	0,15	0,45
26	*Raised Floor*	2	1	0,3	0,6
27	kabel FO	8	4	0,7	22,4
28	*Centralized UPS*	6	1	0,5	3
29	*Backup* Genset	2	1	0,475	0,95
30	Pemadam kebakaran	2	4	0	0
31	IPS	6	1	0,67	4,02
32	tabel *User* dan *Password*	5	4	0,4	8
33	Pelatihan aplikasi core bussiness	0	0	0,45	0

Setelah dapat diketahui nilai risiko pada masing-masing aset, langkah selanjutnya yaitu menentukan level risiko pada masing-masing aset. Penentuan level risiko dilakukan dengan menyesesuaikan hasil dari nilai risiko pada matriks level risiko pada Tabel 4.15 yang telah dibuat sebelumnya. Hasil dari level risiko dari masing-masing aset ditunjukkan pada Tabel 4.15.

Tabel 4.15. Level Risiko pada Aset

No	Aset	Nilai Risiko	Level Risiko
1	PC	1,2	LOW
2	Server	35,52	**MEDIUM**
3	*Storage Area Network*	3,4	LOW
4	*Network Devices*	0,875	LOW
5	Windows Server	8,82	LOW
6	Windows	1,84	LOW
7	*Wide Area Network* (WAN)	16,96	**MEDIUM**

No	Aset	Nilai Risiko	Level Risiko
8	*Local Area Network* 1(LAN	1,625	LOW
9	*Wireless*-LAN	2,8	LOW
10	Server Farm	8,8	LOW
11	*Patch* Panel	1,5	LOW
12	Ellipse (MIMS)	20,48	**MEDIUM**
13	Navitas (Energi Management)	6,02	LOW
14	Sistem Manajemen Perusahaan (E-SMP)	8	LOW
15	*Portal Knowledge Management*	9,4	LOW
16	Aplikasi *Monitoring* Pengadaan (AMP)	6,88	LOW
17	Aplikasi Helpdesk	2,4	LOW
18	App. Whatsup	3,44	LOW
19	App. IP Centry	3,3	LOW
20	Network Analyzer	9,6	LOW
21	Antivirus	2,7	LOW
22	Firewall	9,9	LOW
23	Oracle	27,72	**MEDIUM**
24	*Rack System*	0,7	LOW
25	*Cooling System*	0,45	LOW
26	*Raised Floor*	0,6	LOW
27	kabel FO	22,4	**MEDIUM**
28	*Centralized UPS*	3	LOW
29	*Backup* Genset	0,95	LOW
30	Pemadam kebakaran	0	LOW
31	IPS	4,02	LOW
32	tabel *User* dan *Password*	8	LOW
33	Pelatihan aplikasi core bussiness	0	LOW

Dari hasil level risiko diatas, maka dapat ditentukan bahwa ada beberapa aset yang bernilai Medium yaitu Server, WAN, App. Ellipse, Oracle, dan Kabel

Fyber Optic. Pengolahan risiko hanya akan dilakukan dengan aset yang bernilai medium saja sesuai dengan kriteria penerimaan risiko yang telah dibuat pada sub tahapan sebelumnya. Sedangkan untuk aset yang level risikonya bernilai Low tidak perlu mendapatkan pengolahan risiko lebih lanjut karena risiko tersebut akan diterima sesuai dengan kriteria penerimaan risiko yang ada.

4.2.6 Analisa Penanganan Risiko

Pada tahapan analisa penanganan risiko adalah tahapan yang bertujuan untuk menentukan pilihan penanganan risiko jika risiko yang timbul tidak dapat langsung diterima tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan risiko yang telah ditetapkan sebelumnya. Pilihan penanganan risiko pada PT PJB UP Gresik ditentukan sebagai berikut.

1. Menerima risiko dengan menetapkan kontrol keamanan yang sesuai.
2. Menerima risiko dengan menggunakan kriteria penerimaan risiko yang ada.

Setelah menentukan pilihan penanganan risiko langkah selanjutnya adalah melakukan pilihan penanganan risiko pada setiap aset yang bernilai medium yaitu Server, WAN, App. Ellipse, Oracle, dan Kabel *Fyber Optic*. Plihan penanganan risiko pada masing-masing aset akan dijelaskan pada Tabel 4.16.

Tabel 4.16. 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

No	Aset	Pilihan Penanganan Risiko
		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

4.2.7 Menetapkan Kontrol Objektif dan Kontrol

Setelah menetapkan pilihan penanganan risiko, langkah selanjutnya yaitu menentukan kontrol keamanan yang sesuai pada aset yang memiliki level risiko lebih tinggi. Penetepan kontrol objektif dan kontrol disesuaikan dengan ancaman dan kelemahan dari masing-masing aset yang dipilih pada subbab 4.2.6. Tujuan penentuan kontrol keamanan ini dijadikan dasar untuk membuat prosedur kontrol dalam pengelolaan risiko. Berikut adalah kontrol objektif dan kontrol berdasarkan ISO/IEC 27002:2005 yang digunakan untuk masing-masing aset sebagai berikut.

1. Server

Kontrol objektif dan kontrol pada aset server yan terdiri dari klausul A.9.1, A.9.2, A.10.5, dan A.13.2.1 ditunjukkan pada Tabel 4.17

Tabel 4.17. Kontrol Objektif dan Kontrol Server

Kontrol Objektif dan Kontrol Server		
Kategori Keamanan Utama A.9.1 : Area yang aman Kontrol Objektif: untuk mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interferensi terhadap lokasi dan informasi organisasi.		
A.9.1.1	Perimeter keamanan fisik	Pengendalian : Perimeter keamanan (batasan untuk pintu masuk dikendalikan dengan kartu (*id card*) pada setiap area yang memiliki *priority*

Kontrol Objektif dan Kontrol Server		
		keamanan tingkat tinggi) harus digunakan untuk melindungi area yang berisi informasi sesuai dengan kebijakan keamanan fisik (KBJK.KA-001) yang ditentukan.
A.9.1.4	Perlindungan terhadap ancaman eksternal dan lingkungan	Pengendalian : Perlindungan fisik terhadap kerusakan akibat dari banjir, gempa bumi, kebakaran atau buatan manusia harus dirancang dan diterapkan sesuai dengan kebijakan keamanan fisik (KBJK.KA-001) dengan menetapkan sistem keamanan (sesuai dengan keputusan perusahaan) untuk mencegah terjadi ancaman baik bencana alam maupun bencana akibat ulah manusia.
Kategori Keamanan Utama A.9.2 Keamanan peralatan Kontrol Objektif: untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi		
A.9.2.1	Penempatan dan perlindungan peralatan	Pengendalian : Server harus ditempatkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan dan peluang untuk akses oleh pihak yang tidak berwenang sesuai dengan kebijakan keamanan fisik (KBJK.KA-001) dengan menentukan lokasi bagi server yang bebas dari berbagai macam gangguan
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 data back-up pada server

Kontrol Objektif dan Kontrol Server		
		harus pelihara secara berkala sesuai kebijakan back-up (KBJK.BC-004) yang ditentukan untuk memelihara nilai dari integritas dan ketersediaan pada informasi
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 : Kebijakan dan tanggung jawab manajemen dalam prosedur (PRDR.IKI.005.01) insiden keamanan informasi harus ditetapkan untuk memastikan penanganan yang cepat dan efisien terhadap insiden keamanan informasi.

2. *Wide Area Network* (WAN)

Kontrol objektif dan kontrol pada aset *wide area network* (WAN) yang terdiri dari klausul A.10.6 dan A.11.4 ditunjukkan pada Tabel 4.18

Tabel 4.18. Kontrol Objektif dan Kontrol WAN

Kontrol Objektif dan Kontrol WAN		
Kategori Keamanan Utama A.10.6 Manajemen keamanan jaringan Kontrol Objektif: untuk memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung.		
A.10.6.1	Pengendalian jaringan	Pengendalian : Kebijakan pengendalian akses pada jaringan (KBJK.PA-002) harus ditetapkan agar jaringan dapat dikendalikan dan terlindung dari ancaman untuk memelihara keamanan dari sistem dan aplikasi

Kontrol Objektif dan Kontrol WAN		
		yang menggunakan jaringan dengan menerapkan sistem pengamanan jaringan yang telah disetujui oleh perusahaan.
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 jaringan (WAN,LAN,WLAN) hanya dapat diberikan kepada pengguna akses yang berwenang sesuai dengan persetujuan perusahaan pada kebijakan penggunaan layanan jaringan (KBJK.PLJ-003) yang ditentukan.
A.11.4.6	Pengendalian koneksi jaringan	Pengendalian : Jaringan yang digunakan secara bersama (WAN,LAN,WLAN) dibatasi aksesnya yang sejalan dengan sistem pengamanan jaringan pada kebijakan pengendalian akses (KBJK.PA-002) yang ditentukan.

3. App. Ellipse

Kontrol objektif dan kontrol pada aset app. Ellipse yang terdiri dari klausul A.11.2 dan A.11.6 ditunjukkan pada Tabel 4.19

Tabel 4.19. Kontrol Objektif dan Kontrol app. Ellipse

Kontrol Objektif dan Kontrol 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 : Pendaftaran dan penghapusan/pembatalan

Kontrol Objektif dan Kontrol App. Ellipse		
		pengguna yang diatur dalam prosedur pengendalian akses (PRDR.PHA.002.01) dalam mengendalikan akses aplikasi terhadap seluruh layanan teknologi informasi untuk mencegah akses aplikasi oleh pihak yang tidak berwenang
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 pada aplikasi oleh pengguna harus dibatasi sesuai dengan kebijakan pengendalian akses (KBJK.PA-002) yang disetujui bahwa hanya personel yang memiliki hak akses yang dapat mengakses.

4. Oracle

Kontrol objektif dan kontrol pada aset oracle yang terdiri dari klausul A.11.6 ditunjukkan pada Tabel 4.20

Tabel 4.20. Kontrol Objektif dan Kontrol oracle

Kontrol Objektif dan Kontrol 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 pada oracle oleh pengguna harus dibatasi sesuai dengan kebijakan pengendalian akses (KBJK.PA-002) yang disetujui bahwa hanya personel yang berwenang saja yang dapat mengakses.

5. Kabel *Fyber Optic*

Kontrol objektif dan kontrol pada aset kabel *fyber optic* yang terdiri dari klausul A.9.2 ditunjukkan pada Tabel 4.21

Tabel 4.21. Kontrol Objektif dan Kontrol kabel FO

Kontrol Objektif dan Kontrol Kabel FO		
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 harus dilindungi dari ancaman bahaya terhadap kerusakan sesuai dengan kebijakan keamanan fisik (KBJK.KA-001) yang disetujui.

4.2.8 Pembuatan Kebijakan dan Prosedur

Pembuatan kebijakan dan prosedur dilakukan berdasarkan kontrol objektif dan kontrol yang telah ditentukan sebelumnya. Kebijakan dan prosedur yang dihasilkan berdasarkan kontrol objektif dan kontrol pada klausul-klausul seperti berikut ini.

1. Kebijakan keamanan fisik (klausul A.9.1.1, A.9.1.4, A.9.1.2, A.9.2.3)
2. Kebijakan pengendalian akses (klausul A.10.6.1, A.11.4.6, A.11.6.1)
3. Kebijakan penggunaan layanan jaringan (klausul A.11.4)
4. Kebijakan backup informasi (klausul A.10.5)
5. Prosedur pengendalian hak akses (klasul A.11.2)
6. Prosedur manajemen insiden keamanan informasi (klausul A.13.2)

Pembuatan prosedur lain juga dapat dihasilkan dari salah satu poin lingkup kebijakan yang telah dibuat, sedangkan instruksi kerja dihasilkan berdasarkan prosedur yang membutuhkan detil rinci langkah dalam pengerjaannya. Rekam kerja dihasilkan dari lampiran pada instruksi kerja atau prosedur. Tabel 4.22 merupakan rincian dari kebutuhan kebijakan, prosedur, instruksi kerja, dan rekam kerja berdasarkan tahap perencanaan sistem manajemen keamanan informasi PT PJB UP Gresik.

Tabel 4.22. Rincian Kebijakan, Prosedur, Instruksi Kerja, dan Rekam Kerja

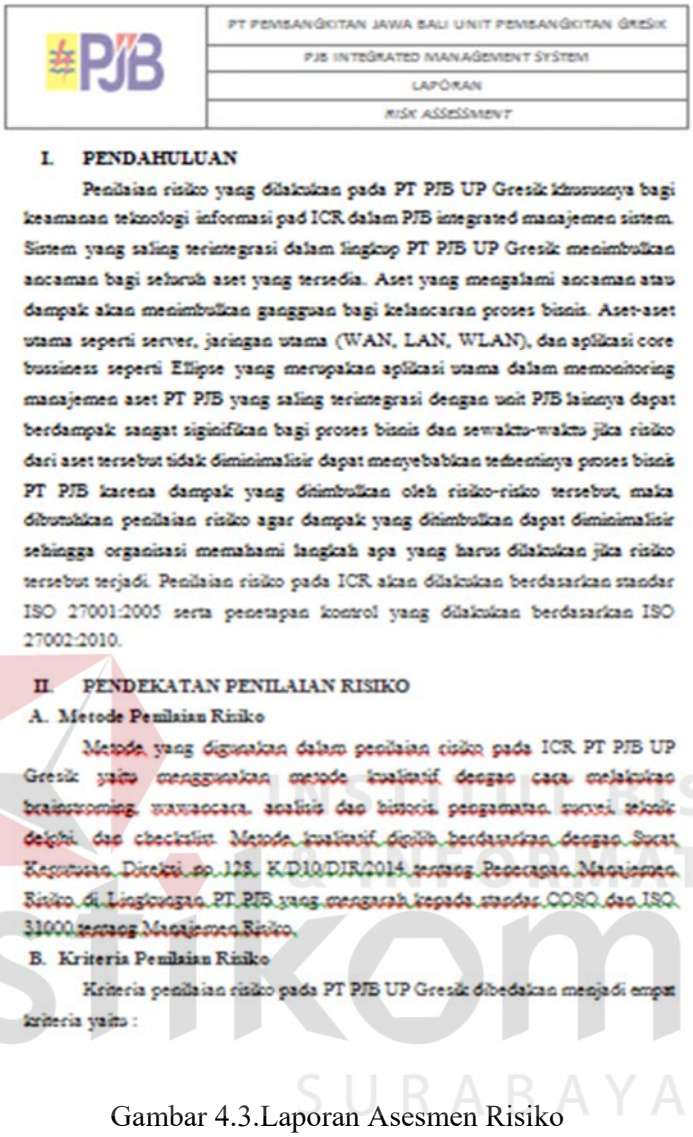
No	Nama	Referensi
1	Kebijakan Keamanan Fisik	Kontrol Objektif dan Kontrol klausul A.9.1.1, A.9.1.4, A.9.1.2, A.9.2.3
2	Kebijakan Pengendalian Akses	Kontrol Objektif dan Kontrol klausul A.10.6.1, A.11.4.6, A.11.6.1
3	Kebijakan Penggunaan Layanan Jaringan	Kontrol Objektif dan Kontrol klausul A.11.4
4	Kebijakan *Backup*	Kontrol Objektif dan Kontrol klausul A.10.5
5	Kebijakan Manajemen Insiden	Kontrol Objektif dan Kontrol klausul A.13.2.1
6	Prosedur Pengendalian Hak Akses	Kontrol Objektif dan Kontrol klasul A.11.2
7	Prosedur *Backup Database*	Kebijakan *Backup* Informasi
8	Prosedur Manajamen Insiden Keamanan Informasi	Kontrol Objektif dan Kontrol klausul A.13.2
9	Instruksi Kerja Pelaporan Insiden	Prosedur Manajemen Insiden Keamanan Informasi
10	Instruksi Kerja Penanganan Insiden	Prosedur Manajemen Insiden Keamanan Informasi
11	Instruksi Kerja Analisis dan Investigasi Insiden	Prosedur Manajemen Insiden Keamanan Informasi
12	Instruksi Kerja DRP	Prosedur Manajemen Insiden Keamanan Informasi
13	Instruksi Kerja Pembuatan Tiket *Helpdesk*	Prosedur Pengendalian Hak Akses
14	Form Pelaksanaan *Backup Database*	Prosedur Backup Database
15	Form Pelaporan Insiden	Instruksi Kerja Pelaporan Insiden
16	Form Penanganan Insiden	Instruksi Kerja Penanganan Insiden
17	Form Penghapusan/ Pembatalan Hak Akses	Prosedur Pengendalian Hak Akses
18	*Checklist* Kelengkapan DRP	Instruksi Kerja DRP
19	*Checklist* Kegiatan DRP	Instruksi Kerja DRP

4.3 Tahap Akhir

Tahap akhir merupakan tahapan dalam perencanaan sistem manajemen keamanan informasi yang menghasilkan keluaran atau *output* dalam dokumen perencanaan tersebut antara lain :

1. Laporan Asesmen Risiko

   Laporan asesmen risiko merupakan hasil dari penilaian risiko yang dilakukan pada ICR PT PJB UP Gresik berdasarkan standar ISO 27001:2005. Laporan asesmen risiko yang dibuat meliputi identifikasi risiko, analisa dan evaluasi risiko, identifikasi penanganan risiko, serta menetapkan kontrol objektif dan kontrol. Contoh laporan asesmen risiko pada ICR dapat dilihat pada Gambar 4.3.



PT PEMBANGKITAN JAWA BALI UNIT PEMBANGKITAN GRESIK
PJB INTEGRATED MANAGEMENT SYSTEM
LAPORAN
RISK ASSESSMENT

I. PENDAHULUAN

Penilaian risiko yang dilakukan pada PT PJB UP Gresik khususnya bagi keamanan teknologi informasi pad ICR dalam PJB integrated manajemen sistem. Sistem yang saling terintegrasi dalam lingkup PT PJB UP Gresik menimbulkan ancaman bagi seluruh aset yang tersedia. Aset yang mengalami ancaman atau dampak akan menimbulkan gangguan bagi kelancaran proses bisnis. Aset-aset utama seperti server, jaringan utama (WAN, LAN, WLAN), dan aplikasi core bussiness seperti Ellipse yang merupakan aplikasi utama dalam memonitoring manajemen aset PT PJB yang saling terintegrasi dengan unit PJB lainnya dapat berdampak sangat siginifikan bagi proses bisnis dan sewaktu-waktu jika risiko dari aset tersebut tidak diminimalisir dapat menyebabkan terhentinya proses bisnis PT PJB karena dampak yang ditimbulkan oleh risiko-risko tersebut, maka dibutuhkan penilaian risiko agar dampak yang ditimbulkan dapat diminimalisir sehingga organisasi memahami langkah apa yang harus dilakukan jika risiko tersebut terjadi. Penilaian risiko pada ICR akan dilakukan berdasarkan standar ISO 27001:2005 serta penetapan kontrol yang dilakukan berdasarkan ISO 27002:2010.

II. PENDEKATAN PENILAIAN RISIKO

A. Metode Penilaian Risiko

Metode yang digunakan dalam penilaian risiko pada ICR PT PJB UP Gresik yaitu menggunakan metode kualitatif dengan cara melakukan brainstorming, wawancara, analisis dan bisnis pengamatan, survei, teknik delphi, dan checklist. Metode kualitatif dipilih berdasarkan dengan Surat Keputusan Direksi no. 128. K/D10/DIR/2014 tentang Penerapan Manajemen Risiko di Lingkungan PT PJB yang mengarah kepada standar COSO dan ISO 31000 tentang Manajemen Risiko.

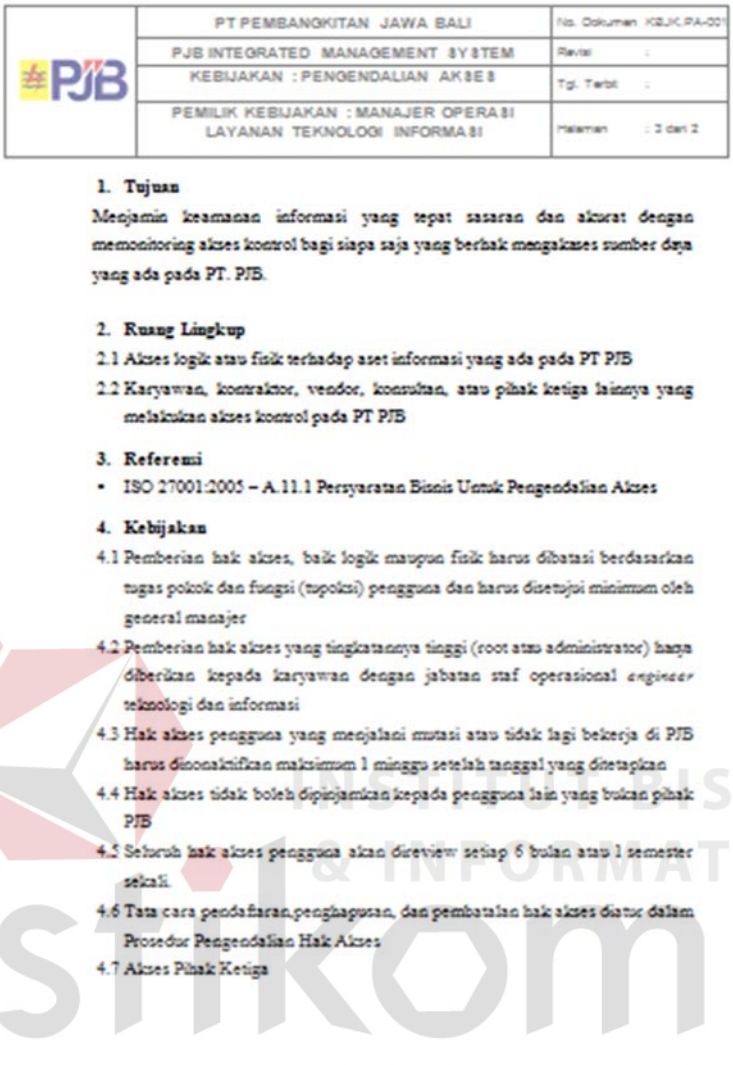
B. Kriteria Penilaian Risiko

Kriteria penilaian risiko pada PT PJB UP Gresik dibedakan menjadi empat kriteria yaitu :

Gambar 4.3.Laporan Asesmen Risiko

2. Kebijakan

Output kebijakan yang dihasilkan dalam perencanaan sistem manajamen keamanan informasi diperoleh lima kebijakan yaitu keamanan fisik, kebijakan pengendalian akses, kebijakan penggunaan layanan jaringan, kebijakan backup, dan kebijakan manajemen insiden. Gambar 4.4 merupakan salah satu contoh kebijakan yang dihasilkan yaitu kebijakan pengendalian akses.



	PT PEMBANGKITAN JAWA BALI	No. Dokumen : KEBIJK.PA-001
PJB	PJB INTEGRATED MANAGEMENT SYSTEM	Revisi :
	KEBIJAKAN : PENGENDALIAN AKSES	Tgl. Terbit :
	PEMILIK KEBIJAKAN : MANAJER OPERASI LAYANAN TEKNOLOGI INFORMASI	Halaman : 1 dari 2

1. Tujuan

Menjamin keamanan informasi yang tepat sasaran dan akurat dengan memonitoring akses kontrol bagi siapa saja yang berhak mengakses sumber daya yang ada pada PT. PJB.

2. Ruang Lingkup

2.1 Akses logik atau fisik terhadap aset informasi yang ada pada PT PJB

2.2 Karyawan, kontraktor, vendor, konsultan, atau pihak ketiga lainnya yang melakukan akses kontrol pada PT PJB

3. Referensi

- ISO 27001:2005 – A.11.1 Persyaratan Bisnis Untuk Pengendalian Akses

4. Kebijakan

4.1 Pemberian hak akses, baik logik maupun fisik harus dibatasi berdasarkan tugas pokok dan fungsi (tupoksi) pengguna dan harus disetujui minimum oleh general manajer

4.2 Pemberian hak akses yang tingkatannya tinggi (root atau administrator) hanya diberikan kepada karyawan dengan jabatan staf operasional *engineer* teknologi dan informasi

4.3 Hak akses pengguna yang menjalani mutasi atau tidak lagi bekerja di PJB harus dinonaktifkan maksimum 1 minggu setelah tanggal yang ditetapkan

4.4 Hak akses tidak boleh dipinjamkan kepada pengguna lain yang bukan pihak PJB

4.5 Seluruh hak akses pengguna akan direview setiap 6 bulan atau 1 semester sekali.

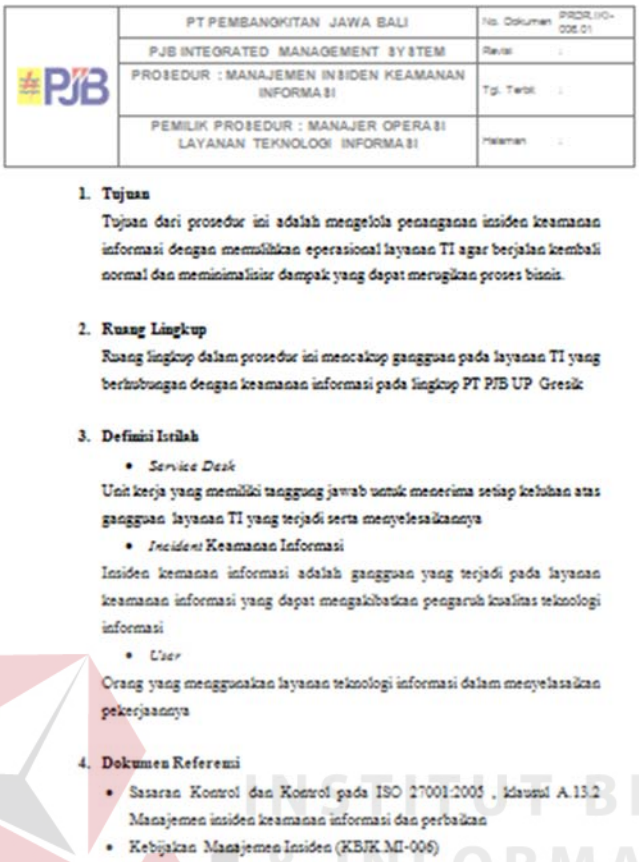
4.6 Tata cara pendaftaran,penghapusan, dan pembatalan hak akses diatur dalam Prosedur Pengendalian Hak Akses

4.7 Akses Pihak Ketiga

Gambar 4.4. Kebijakan Pengendalian Akses

3. Prosedur

Prosedur yang dihasilkan dalam perencaaan sistem manajemen keamanan informasi diperoleh tiga prosedur yaitu prosedur backup database, prosedur pengendalian hak akses, dan prosedur manajemen insiden keamanan informasi. Gambar 4.5 merupakan salah satu contoh dari prosedur yang dihasilkan yaitu prosedur manajemen insiden keamanan informasi.



	PT PEMBANGKITAN JAWA BALI	No. Dokumen PRDR.IKO-006.01
PJB	PJB INTEGRATED MANAGEMENT SYSTEM	Revisi :
	PROSEDUR : MANAJEMEN INSIDEN KEAMANAN INFORMASI	Tgl. Terbit :
	PEMILIK PROSEDUR : MANAJER OPERASI LAYANAN TEKNOLOGI INFORMASI	Halaman :

1. **Tujuan**

   Tujuan dari prosedur ini adalah mengelola penanganan insiden keamanan informasi dengan memulihkan operasional layanan TI agar berjalan kembali normal dan meminimalisisr dampak yang dapat merugikan proses bisnis.

2. **Ruang Lingkup**

   Ruang lingkup dalam prosedur ini mencakup gangguan pada layanan TI yang berhubungan dengan keamanan informasi pada lingkup PT PJB UP Gresik

3. **Definisi Istilah**

   - *Service Desk*

   Unit kerja yang memiliki tanggung jawab untuk menerima setiap keluhan atas gangguan layanan TI yang terjadi serta menyelesaikannya

   - *Incident* Keamanan Informasi

   Insiden keamanan informasi adalah gangguan yang terjadi pada layanan keamanan informasi yang dapat mengakibatkan pengaruh kualitas teknologi informasi

   - *User*

   Orang yang menggunakan layanan teknologi informasi dalam menyelasaikan pekerjaannya

4. **Dokumen Referensi**

   - Sasaran Kontrol dan Kontrol pada ISO 27001:2005 , klausul A.13.2 Manajemen insiden keamanan informasi dan perbaikan
   - Kebijakan Manajemen Insiden (KBJK.MI-006)

Gambar 4.5. Prosedur Manajemen Insiden Keamanan Informasi

4. Instruksi kerja

Instruksi kerja yang dihasilkan dalam perencanaan sistem manajemen keamanan informasi diperoleh lima instruksi kerja yaitu instruksi kerja pelaporan insiden, instruksi kerja penanganan insiden, instruksi kerja analisis dan investigasi insiden, instruksi kerja DRP, dan instruksi kerja pembuatan tiket *helpdesk*. Gambar 4.6 merupakan salah satu contoh dari instruksi kerja yang dihasilkan yaitu instruksi kerja DRP.

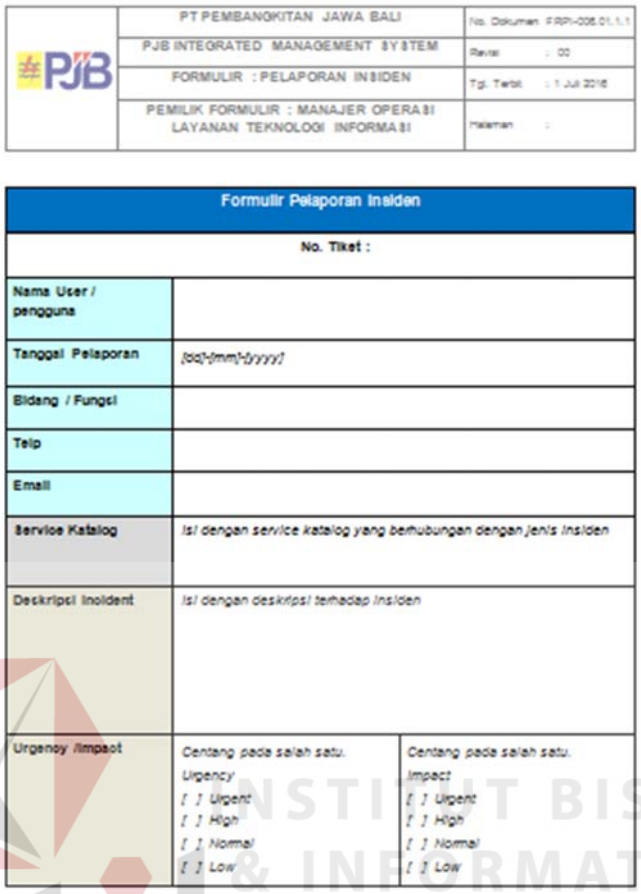
PJB	PT PEMBANGKITAN JAWA BALI UNIT PEMBANGKITAN GRESIK	No. Dokumen	IKOM-006.01.4
	PJB INTEGRATED MANAGEMENT SYSTEM	Tanggal Terbit	1 Juli 2016
	INSTRUKSI KERJA	No Revisi	00
	DISASTER RECOVERY PLAN	Halaman	

TUJUAN		
Memastikan penanganan *disaster recovery plan* pada PT PJB berjalan dengan baik dan sesuai dengan ketentuan prosedur *disaster recovery plan*.		
RUANG LINGKUP		
• Meliputi *disaster recovery plan* untuk konfigurasi setting VPN dan instalasi printer server.		
ACUAN / DOKUMEN TERKAIT		
- PRDR.IKI-006.01 (Manajemen Insiden Keamanan Informasi)		
SUMBER DAYA MANUSIA		
JUMLAH	**KEAHLIAN**	**CATATAN**
5	Mampu mengusasi Microsoft Windows dan Bistem Komputer	-
TOOL S/PERALATAN KERJA		
JUMLAH	**NAMA**	**CATATAN**
• 5 • 4 • 1	• Laptop /Komputer • Printer • Modem	-
SPARE PART/CONSUMABLE MATERIAL		
JUMLAH	**NAMA MATERIAL/SPARE PART**	**CATATAN**
-	-	-
APD/SAFETY WORKING PERMIT		
JUMLAH	**NAMA PERALATAN**	**CATATAN**
-	-	-

Gambar 4.6. Instruksi Kerja DRP

5. Rekam kerja

Rekam kerja yang dihasilkan dalam perencanaan sistem manajemen keamanan informasi diperoleh enam rekam kerja yaitu rekam kerja pelaksanaan backup database, rekam kerja pelaporan insiden, rekam kerja penanganan insiden, rekam kerja penghapusan/pembatalan hak akses, *checklist* kegiatan DRP, dan *checklist* kelengkapan DRP. Gambar 4.7 merupakan salah satu contoh dari rekam kerja yang dihasilkan yaitu form pelaporan insiden.



PT PEMBANGKITAN JAWA BALI	No. Dokumen : FRPI-008.01.1.1
PJB INTEGRATED MANAGEMENT SYSTEM	Revisi : 00
FORMULIR : PELAPORAN INSIDEN	Tgl. Terbit : 1 Juli 2016
PEMILIK FORMULIR : MANAJER OPERASI LAYANAN TEKNOLOGI INFORMASI	Halaman :

Formulir Pelaporan Insiden		
No. Tiket :		
Nama User / pengguna		
Tanggal Pelaporan	*[dd]-[mm]-[yyyy]*	
Bidang / Fungsi		
Telp		
Email		
Service Katalog	*Isi dengan service katalog yang berhubungan dengan jenis insiden*	
Deskripsi Insident	*Isi dengan deskripsi terhadap insiden*	
Urgency /Impact	*Centang pada salah satu.* *Urgency* *[ ] Urgent* *[ ] High* *[ ] Normal* *[ ] Low*	*Centang pada salah satu.* *Impact* *[ ] Urgent* *[ ] High* *[ ] Normal* *[ ] Low*

Gambar 4.7. Form Pelaporan Insiden

4.4 Pembahasan

Dari hasil tahapan dalam perencanaan sistem manajemen keamanan informasi pada ICR menunjukkan bahwa pada proses penilaian risiko hasil yang didapat yaitu terdapat lima aset dalam ICR yang memiliki level risiko paling tinggi dengan nilai Medium yaitu pada aset Server, *Wide Area Network* (WAN), App.Ellipse, Oracle, dan Kabel *Fyber Optic.* Level risiko pada masing-masing aset mendefinisikan pengukuran nilai tersendiri sesuai dengan pedoman umum manajemen risiko PT PJB yaitu server memiliki level risiko sebesar 35,52 dengan tingkat medium yang berarti bahwa dampak bisnis yang akan ditimbulkan dapat merusak *database/*aplikasi dan server itu sendiri dengan kemungkinan kejadian

pada jangka waktu 1 tahun , WAN memiliki level risiko sebesar 16,96 dengan tingkat medium pada dampak bisnis yang akan ditimbulkan dapat menggangu aktifitas LAN unit atau kantor pusat dengan kemungkinan kejadian pada jangka waktu 1 tahun, app.Ellipse memiliki level risiko sebesar 20,48 dengan tingkat medium dengan dampak bisnis yang akan ditimbulkan dapat merusak infrastruktur WAN PJB dengan kemungkinan kejadian pada jangka waktu 1 tahun, oracle memiliki level risiko sebesar 27,72 dengan tingkat medium yang menjelaskan bahwa dampak bisnis yang akan ditimbulkan dapat merusak infrastruktur WAN PJB dengan kemungkinan kejadian pada jangka waktu 1 tahun, dan kebel FO memiliki level risiko 22,4 dengan tingkat medium yang berarti bahwa dampak bisnis yang akan ditimbulkan dapat merusak infrastruktur WAN PJB dengan kemungkinan kejadian pada jangka waktu 1 tahun.

Dalam perencanaan sistem manajemen keamanan informasi pada ICR menghasilkan dokumen-dokumen perencanaan yang meliputi laporan asesmen risiko (identifikasi risiko, analisa dan evaluasi risiko, analisa penanganan risiko, dan pemilihan kontrol objektif dan kontrol), kebijakan, prosedur, instruksi kerja, dan rekam kerja. Kebijakan yang dihasilkan dalam hasil tugas akhir ini terdapat lima kebijakan diantaranya keamanan fisik, kebijakan pengendalian akses, kebijakan penggunaan layanan jaringan, kebijakan backup, dan kebijakan manajemen insiden. Prosedur yang dihasilkan dalam tugas akhir meliputi prosedur *backup database*, prosedur pengendalian akses, dan prosedur manajemen insiden keamanan informasi. Sedangkan instruksi kerja dan rekam kerja dihasilkan dari prosedur atau instruksi kerja yang terdapat pada dokumen terkait atau lampiran yang dihasilkan dari hasil diskusi dengan pihak SINFO. Instruksi kerja yang

didapatkan antara lain instruksi kerja *disaster recovery plan*, instruksi kerja pelaporan insiden, instruksi kerja analisis dan investigasi, instruksi kerja penanganan insiden, dan instruksi kerja pembuatan tiket *helpdesk*. Rekam kerja yang dihasilkan terdiri dari form pelaksanaan *backup*, form pelaporan insiden, form penanganan insiden, form penghapusan hak akses, *checklist* pelaksanaan DRP, dan *checklist* kelengkapan DRP.