TESIS PM – 147501

REKOMENDASI PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) MENGGUNAKAN METODE AHP-TOPSIS BERDASARKAN ISO/IEC 27001:2005 (STUDI KASUS: PT PJB SERVICES)

PURNOMO DWI DJAJANTO
09211650055004

DOSEN PEMBIMBING
Prof. Dr. Techn. Drs. M. Isa Irawan, MT

DEPARTEMEN MANAJEMEN TEKNOLOGI
BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI
FAKULTAS BISNIS DAN MANAJEMEN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2018

LEMBAR PENGESAHAN

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar
Magister Manajemen Teknologi (M.MT)
di
Institut Teknologi Sepuluh Nopember

Oleh:
PURNOMO DWI DJAJANTO
NRP. 09211650055004

Tanggal Ujian : 11 Juli 2018
Periode Wisuda : September 2018

Disetujui oleh:

1. **Prof. Dr. Techn, Drs. M. Isa Irawan, MT.** **(Pembimbing)**
   NIP. 19631225 198903 1 001

2. **Dr.Tech, Ir. R. V. Hari Ginardi, MSc** **(Penguji)**
   NIP. 19650518 199203 1 003

3. **Erma Suryani, ST, MT, PhD** **(Penguji)**
   NIP. 19700427200501 2 001

Dekan Fakultas Bisnis dan Manajemen Teknologi,

Prof. Dr. Ir. Udisubakti Ciptomulyono, M.Eng.Sc
NIP. 19590318 198701 1 001

LEMBAR PERNYATAAN

Saya yang bertandatangan dibawah ini,

Nama : Purnomo Dwi Djajanto

NRP : 09211650055004

Jurusan : Magister Manajemen Teknologi

Menyatakan bahwa tesis saya yang berjudul:

"REKOMENDASI PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) MENGGUNAKAN METODE AHP-TOPSIS BERDASARKAN ISO/IEC 27001:2005 (STUDI KASUS: PT PJB SERVICES)"

Seluruh hasil penelitian yang tertuang di makalah ini adalah hasil pekerjaan sendiri, tidak ada informasi *ilegal* atau meng-*copy* pekerjaan orang lain. Semua kutipan penelitian sesuai aslinya dan tertulis di referensi.

Jika pernyataan ini tidak benar, saya bersedia menerima konsekuensi sesuai peraturan yang berlaku.

Sidoarjo, 1 Juli 2018

Purnomo Dwi Djajanto

REKOMENDASI PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) MENGGUNAKAN METODE AHP-TOPSIS BERDASARKAN ISO/IEC 27001:2005 (STUDI KASUS: PT PJB SERVICES)

Nama : Purnomo Dwi Djajanto
NRP : 09211 6500 55004
Pembimbing : Prof. Dr. techn. Drs. M. Isa Irawan, MT.

ABSTRAK

PT. PJB Services adalah perusahaan yang didirikan untuk memenuhi kebutuhan lini bisnis dalam memberikan jasa operasi dan pemeliharaan unit pembangkit listrik. Pengelolaan keamanan informasi pada PT. PJB Services selama ini hanya didasarkan pada praktik dasar keamanan yang melalui proses peningkatan tanpa adanya dasar pedoman. Perusahaan cenderung melakukan peningkatan keamanan informasi berdasarkan *trend* yang berkembang saat itu atau saat terjadinya insiden yang berkaitan dengan keamanan informasi. Tanpa adanya pengelolaan keamanan informasi yang baik dan berkelanjutan pada perusahaan, maka perusahaan sangat rentan terdahap ancaman keamanan informasi yang ada.

Berdasarkan hal tersebut, penelitian difokuskan kepada rekomendasi perancangan Sistem Manajemen Keamanan Informasi (SMKI) untuk PT PJB Services khususnya di Divisi Teknologi Informasi (TI). SMKI merupakan sebuah sistem manajemen yang berdasarkan pendekatan risiko aset informasi untuk memantapkan, menerapkan, menjalankan, memantau, meninjau ulang, memelihara dan meningkatkan keamanan informasi. Penelitian ini menggabungkan penggunaan AHP-TOPSIS dengan berdasar pada ISO/IEC 27001:2005 dalam pembuatan perancangan SMKI. Proses *assessment* menggunakan ISO/IEC 27001:2005, dari hasil audit akan didapatkan kontrol beserta cara penanganan berdasarkan beberapa kriteria dari resiko tersebut, setelah itu akan dilakukan proses rekomendasi menggunakan metode AHP-TOPSIS sehingga akan mendapatkan prioritas kontrol dalam penanganan keamanan informasi.

Hasil dari penelitian ini, sebanyak 45 aset informasi dan 224 risiko yang dapat diidentifikasi. Prioritas kontrol yang direkomendasikan sesuai dari hasil penelitian ini adalah *Security Policy, Organization of Information Security, Human Resource Policy, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Security Incident Management, Asset Management, Information System Acquisition Development and Maintenance*.

Kata kunci: Sistem Manajemen Kemanan Informasi (SMKI), ISO/IEC 27001:2005, AHP-TOPSIS

(Halaman ini sengaja dikosongkan)

RECOMMENDATION DESIGN OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) USING AHP-TOPSIS METHOD BASED ON ISO/IEC 27001:2005 (CASE STUDY: PT PJB SERVICES)

Name : Purnomo Dwi Djajanto
Student ID : 09211 6500 55004
Supervisor : Prof. Dr. Techn.Drs. M. Isa Irawan, MT.

ABSTRACT

PT. PJB Services is a company established to meet the needs of business lines in providing services operation and maintenance of power plant. Information security management at PT. PJB Services has been based solely on basic security practices through an improvement process in the absence of a guideline. Companies improve information security based on current trends or incidents related to information security. In the absence of good and sustainable corporate information security management, companies are vulnerable to existing information security threats.

Based on that situation, this research focused on designing recommendation of Information Security Management System (ISMS) for PT PJB Services, especially in the Division of Information Technology (IT). The ISMS is a management system based on an information asset risk approach to consolidate, implement, monitor, review, maintain and enhance information security. This study combines the use of AHP-TOPSIS based on ISO / IEC 27001: 2005 in making ISMS design. The assessment process using ISO / IEC 27001: 2005, from the assessment results will be obtained control and how to handle based on several criteria of the risk, after that, the recommendation process will be done using AHP-TOPSIS method so it will get priority control in handling information security.

The results of this study, 45 information assets and 224 risks that can be identified. The recommended priority controls from the results of this study are Security Policy, Organization of Information Security, Human Resource Policy, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Security Incident Management, Asset Management, Information Systems Acquisition Development and Maintenance.

Keywords: Information Security Management System (ISMS), ISO/IEC 27001:2005, AHP-TOPSIS

(Halaman ini sengaja dikosongkan)

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT Yang Maha Esa, karena berkat rahmat dan hidayah-Nya, penulis dapat menyelesaikan proposal tesis ini tepat waktu. Semoga *Allah Subhanahu wa Ta'ala* selalu memberikan kemudahan dan pertolongannya kepada penulis untuk dapat menyelesaikan tesis ini dengan optimal.

Tesis ini berjudul Rekomendasi Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Menggunakan Metode AHP-TOPSIS Berdasarkan ISO/IEC 27001:2005 (Studi Kasus: PT PJB Services). Dalam prosesnya, penulis ingin mengucapkan rasa terima kasih yang sebesar-besarnya, teruntuk:

1. Keluarga penulis; kedua orang tua penulis, bapak Marwoto dan ibu Kisrawiyah yang selalu membimbing, mendoakan, dan mendukung penulis; kakak dan adik penulis, yang selalu menjadi motivasi penulis.
2. Bapak Prof. Dr. Techn. Drs. M. Isa Irawan, MT selaku dosen pembimbing yang selalu memberikan saran, masukan dan motivasi dalam pengerjaan proposal tesis ini.
3. Seluruh civitas akademika MMT ITS Surabaya khuusnya Teman-teman seperjuangan penulis, MMT MTI Eksekutif angkatan 2016
4. Rekan-rekan di Divisi Teknologi Informasi PT PJB Services, terima kasih atas waktu dan dukungan yang disediakan untuk penulis dalam pengerjaan proposal tesis ini.
5. Aura Fadhilah, yang selalu menemani, memberi motivasi, dan menjadi rekan berbagi untuk penulis.

Penulis menyadari bahwa dalam penyusunan tesis ini masih banyak kekurangan, baik format maupun kontennya. Untuk itu penulis sangat mengharapkan kritik dan saran yang membangun. Semoga hasil dari tesis ini dapat bermanfaat bagi pembaca maupun penulis.

Sidoarjo, 1 Juli 2018

Purnomo Dwi Djajanto

(Halaman ini sengaja dikosongkan)

DAFTAR ISI

(Halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

(Halaman ini sengaja dikosongkan)

DAFTAR TABEL

(Halaman ini sengaja dikosongkan)

BAB 1
PENDAHULUAN

Pada bab ini akan dibahas latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan dalam penelitian. Pemaparan tersebut diharapkan dapat memberikan gambaran secara umum mengenai penelitian yang akan dilaksanakan.

1.1 Latar Belakang

Pada masa ini, perkembangan Teknologi Informasi semakin pesat, Teknologi Informasi menjadi sangat penting bagi perusahaan karena dapat memudahkan pelaksanaan proses bisnis dan meningkatkan keunggulan kompetitif. Melalui Teknologi Informasi ini, proses bisnis dapat dilaksanakan lebih mudah, cepat, efisien dan efektif. Teknologi Informasi juga menawarkan banyak peluang kepada perusahaan untuk meningkatkan kinerja, dan mentransformasikan pelayanan, proses kerja. Namun Perkembangan teknologi informasi yang semakin pesat ini, memiliki resiko keamanan semakin besar pula jika perusahaan tidak mampu mengelola dan mengamankan informasi yang dimiliki secara baik.

PT. PJB Services adalah anak perusahaan dari PT. PJB (Pembangkitan Jawa Bali), yang didirikan untuk memenuhi kebutuhan lini bisnis dalam memberikan jasa operasi dan pemeliharaan unit pembangkit listrik. Perusahaan ini didirikan pada tanggal 30 Maret, 2001 dengan prosentase kepemilikan saham 98% dimiliki oleh PT. PJB dan 2% dimiliki oleh YK PT. PJB (Yayasan Kesejahteraan PT. PJB). Pada awalnya, PT. PJB Services hanya fokus pada bidang jasa pemeliharaan pembangkit listrik, kemudian berkembang menjadi perusahaan yang berkecimpung dalam jasa operasi dan pemeliharaan pembangkit listrik. Saat ini jumlah karyawan PT. PJB Services mencapai 3600, dan tersebar di unit-unit kerja di seluruh Indonesia.

Pengelolaan keamanan informasi pada PT. PJB Services selama ini hanya didasarkan pada praktik dasar keamanan yang melalui proses peningkatan tanpa adanya dasar pedoaman. Perusahaan cenderung melakukan peningkatan keamanan informasi berdasarkan *trend* yang berkembang saat itu atau saat terjadinya insiden

yang berkaitan dengan keamanan informasi. Tanpa adanya pengelolaan keamanan informasi yang baik dan berkelanjutan pada perusahaan, maka perusahaan sangat rentan terdahap ancaman keamanan informasi yang ada. Karenanya penggunaan Sistem Manajemen Keamanan Informasi (SMKI) sangat dibutuhkan untuk mencegah atau meminimalisir resiko terkait dengan keamanan informasi yang ada di dalam perusahaan.

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System (ISMS)* adalah sistem manajemen yang diterapkan perusahaan untuk mengamankan aset informasi terhadap ancaman yang mungkin terjadi. Oleh sebab itu, kemanan informasi secara tidak langsung menjamin kelangsungan bisnis perusahaan. Sistem manajemen keamanan informasi menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan. SMKI ini mempunyai tiga komponen kunci dalam menyediakan jaminan layanan keamanan informasi diantaranya Kerahasiaan yaitu memastikan bahwa informasi dapat diakses hanya untuk mereka yang *authorized* untuk mempunyai akses, integritas yaitu melindungi kelengkapan dan ketelitian informasi dan memproses metoda dan Ketersediaan yaitu memastikan bahwa para pemakai authorised mempunyai akses ke informasi dan berhubungan dengan asset ketika diperlukan.

Perusahaan membutuhkan sebuah kerangka kerja untuk memutuskan apa yang harus dilakukan di dalam manajemen keamanan informasi. Kerangka kerja ini dibentuk menggunakan konsep *PDCA* untuk memastikan perusahaan melakukan perbaikan berkelanjutan dan menggunakan hasil pemetaan dari Standar ISO 27001 untuk memastikan ancaman dan resiko yang kemunginan terjadi tidak akan mempengaruhi bisnis utama perusahaan. (Aginsa et al, 2016). Terdapat berbagai standar keamanan informasi yang berlaku saat ini. Yang paling banyak diterapkan adalah standar sistem manajemen informasi yang diterbitkan oleh ISO yaitu ISO/IEC 27001. ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh

sebuah perusahaan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan berdasarkan *"best practise"* dalam pengamanan informasi.

Metode AHP-TOPSIS mampu menyeleksi alternatif terbaik dari sejumlah alternatif, dalam hal ini alternatif yang dimaksudkan yaitu yang berhak menerima beasiswa berdasarkan kriteria-kriteria yang ditentukan. Penelitian dilakukan dengan mencari nilai bobot untuk setiap atribut, kemudian dilakukan proses pengurutan kandidat yang akan menentukan alternatif yang optimal, yaitu mahasiswa terbaik (Manurung, 2010).

Dalam penelitian ini, penulis menggabungkan penggunaan AHP-TOPSIS dengan berdasar pada ISO/IEC 27001 dalam pembuatan rekomendasi perancangan Sistem Manajemen Keamanan Informasi (SMKI) di Divisi Teknologi Informasi PT PJB Services. Penggunaan ISO/IEC 27001 sebagai acuan perancangan tata kelola keamanan informasi pada penelitian ini dikarenakan menyediakan kerangka kerja untuk netralitas penggunaan teknologi, termasuk kemampuan mengakses data secara berkelanjutan dengan adanya kerahasiaan dan integritas atas informasi yang dimiliki serta kebutuhan pihak-pihak berkepentingan sesuai dengan hak wewenang yang diperoleh. Dalam proses *assessment* menggunakan ISO/IEC 27001 akan didapatkan kontrol beserta cara penanganan berdasarkan beberapa kriteria dari resiko tersebut, setelah itu akan dilakukan proses rekomendasi menggunakan metode AHP-TOPSIS sehingga akan mendapatkan prioritas dalam penanganan keamanan informasi di PT. PJB Services.

1.2 Rumusan Masalah

Dari penjelasan pada latar belakang, maka terdapat beberapa permasalahan yang perlu diperhatikan dan diselesaikan antara lain:

1. Bagaimana cara mengetahui resiko keamanan informasi yang bisa terjadi terhadap asset yang dimiliki perusahaan?
2. Bagaimana penanganan terhadap resiko keamanan informasi yang ada pada perusahaan?

3. Bagaimana membuat kontrol prioritas dalam Sistem Manajemen Keamanan Informasi (SMKI) sebagai paduan dalam melakukan pengelolaan terhadap resiko dan perlindungan terhadap aset informasi?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi resiko keamanan informasi yang bisa terjadi terhadap asset informasi yang dimiliki penelitian.
2. Mengidentifikasi kontrol yang efektif untuk menanggulangi resiko keanaman yang ada pada perusahaan.
3. Memberikan rekomendasi berupa kontrol prioritas dalam Sistem Manajemen Keamanan Informasi (SMKI) yang disesuaikan dengan kondisi perusahaan.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dalam penelitian ini adalah

1. Dapat mengetahui resiko-resiko yang berkaitan dengan keaman informasi pada perusahaan
2. Dapat mengetahui kontrol-kontrol yang efektif untuk menanggulangi resiko keamanan yang ada pada perusahaan.
3. Memiliki pedoman untuk mengelola dan meningkatkan keamanan informasi pada perusahaan
4. Dapat memberikan rekomendasi berupa rancangan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001 yang disesuaikan dengan kondisi perusahaan
5. Dapat dijadikan acuan untuk implementasi Sistem Manajemen Keamanan Informasi (SMKI) di instansi atau perusahaan lainnya

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut

1. Kerangka kerja yang digunakan dalam penelitian adalah ISO/IEC 27001 versi 2005

2. Identifikasi resiko dilakukan terhadap asset-aset di Data Center dimiliki oleh Divisi Teknologi Informasi PT. PJB Services.
3. Metode yang digunakan untuk menentukan prioritas adalah AHP-TOPSIS.
4. Responden yang dilibatkan dalam penelitian ini pada lingkup Divisi Teknologi Informasi PT. PJB Services.

1.6 Sistematika Penulisan

Sistematika pembahasan penelitian ini disusun dengan kerangka pembahasan sebagai berikut:

- Bab 1 Pendahuluan

  Bab ini menyajikan gambaran permasalahan yang dihadapi dalam penelitian, yang mencangkup latar belakang permasalahan, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup dan batasan masalah serta sistematika penulisan.
- Bab 2 Dasar Teori dan Kajian Pustaka

  Bab ini menyajikan kajian literature mengenai teori yang digunakan dalam penelitian, serta penelitian sebelumnya yang berkaitan dengan topik yang akan diteliti.
- Bab 3 Metodologi Penelitian

  Bab ini menyajikan metodologi dan langkah-langkah yang diambil untuk melaksanakan penelitian
- Bab 4 Hasil Penelitian dan Pembahasan

  Bab ini menyajikan hasil penelitian yang telah dilakukan serta analisis terkait hasil yang telah didapat.
- Bab 5 Kesimpulan dan Saran

  Bab ini menyajikan kesimpulan dan saran dari penelitian yang telah dilakukan.

(Halaman ini sengaja dikosongkan)

BAB 2
DASAR TEORI DAN KAJIAN PUSTAKA

Bab ini menguraikan tentang dasar teori dan referensi atau kajian pustaka yang mendukung proses penelitian Rekomendasi Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Menggunakan Metode AHP-TOPSIS Berdasarkan ISO/IEC 27001:2005 (Studi Kasus: PT PJB Services).

2.1 Profil Perusahaan

PT. PJB Services adalah anak perusahaan dari PT. PJB (Pembangkitan Jawa Bali), yang didirikan untuk memenuhi kebutuhan lini bisnis dalam memberikan jasa operasi dan pemeliharaan unit pembangkit listrik. Perusahaan ini didirikan pada tanggal 30 Maret, 2001 dengan prosentase kepemilikan saham 98% dimiliki oleh PT. PJB dan 2% dimiliki oleh YK PT. PJB (Yayasan Kesejahteraan PT. PJB). Pada awalnya, PT. PJB Services hanya fokus pada bidang jasa pemeliharaan pembangkit listrik, kemudian berkembang menjadi perusahaan yang berkecimpung dalam jasa operasi dan pemeliharaan pembangkit listrik.

Gambar 2. 1 Logo PT PJB Services

Untuk meningkatkan performa, mempertahankan kepercayaan pelanggan, dan kepedulian perusahaan terhadap aspek-aspek yang menjadi perhatian fokus perusahaan, PT PJB Services mengimplementasikan sistem manajemen yang telah ada dengan menambahkan standar yang akan diintegrasikan dengan sistem

manajemen operasionalnya dengan menerapkan PAS 99 yang dikeluarkan dari PT. SGS. PT PJB Services sebagai perusahaan pengelola Jasa O&M Pembangkit Listrik selalu berusaha meningkatkan kepercayaan pelanggan dengan melakukan pengelolaan aset yang dipercayakan padanya sesuai dengan standar internasional. Oleh karena itu, dilakukanlah sertifikasi ISO 55001 sebagai pembuktian bahwa jasa O&M yang diberikan oleh PT PJB Services telah memenuhi kriteria standar internasional. PT PJB Services saat ini dipercaya mengelola unit pembangkit di berbagai daerah di Indonesia dengan total kapasitas sampai dengan tahun 2017 sebesar 5.208 MW dengan lokasi yang tersebar dari Aceh sampai dengan Tidore dengan jumlah karyawan mencapai 3664 yang tersebar di unit-unit PT PJB Services.

2.1.1 Visi dan Misi

Adapun Visi dari PT PJB Services adalah Menjadi Perusahaan Pengelola Aset Pembangkit Listrik Dan Pendukungnya Dengan Standar Internasional. Sedangkan Misi dari PT PJB Services antara lain:

- Melaksanakan pengelolaan asset pembangkit listrik dan pendukungnya dengan standar internasional
- Menerapkan manajemen total solusi untuk meningkatkan kinerja unit pembangkit listrik secara berkelanjutan
- Mengembangkan sumber daya perusahaan untuk meningkatkan kinerja perusahaan secara berkelanjutan guna memenuhi harapan stakeholders.

2.1.2 Produk dan Jasa

Adapun Produk dan Jasa yang ditawarkan oleh PT PJB Services antara lain

- *O&M Power Plant*

Jasa operasi dan pemeliharaan unit pembangkit listrik merupakan inti bisnis PT PJB Services dengan pengelolaan pembangkit listrik beserta sumberdaya pendukungnya untuk menyediakan energi listrik dengan proses yang aman, andal, efisien dan berkualitas tinggi.

- *O&M Balance Of Plant*

Dalam pengoperasian unit pembangkit listrik, ketersediaan (availability) dan keandalan (reliability) unit pembangkit merupakan dua parameter yang perlu menjadi perhatian untuk mencapai efisiensi unit pembangkit yang tinggi. Komponen pendukung dan Auxiliary System di pembangkit listrik dibutuhkan untuk memberikan energi pada pembangkit listrik yang berperan penting untuk Avalaibility dan Reliability Unit.

- *O&M Coal And Ash Handling Plant*

Keandalan proses pembangkitan tenaga listrik akan sangat bergantung pada keandalan instalasi system yang mendukungnya. Salah satu instalasi sitem tersebut adalah coal handling system yang merupakan system penangan batubara sebagai bahan bakar PLTU mulai dari pembongkaran batubara dari coalbarge ke stockpile dan memindahkannya sampai batubara tersebut siap digunakan pada furnace.

- *Routine Maintenance*

Preventive Maintenance yang merupakan pemeliharaan berdasarkan variabel waktu yang bertujuan untuk mencegah atau meminimalisasi terjadinya kegagalan dengan mendeteksi dan menemukan kegagalan tersembunyi untuk meningkatkan keandalan suatu sistem.

Predictive Maintenance, yaitu melakukan monitoring kondisi peralatan pembangkit dengan interval waktu tertentu (sesuai dengan standar dan best practice) yang menggunakan teknologi terbaru

- *HSE Management*

Implementasi pengelolaan lingkungan dilakukan dengan penerapan Sistem Manajemen Lingkungan (SML) dan pemenuhan kriteria PROPER sesuai dengan PerMen LH No. 3 Tahun 2014 tentang Program Penilaian Peringkat Kinerja Perusahaan Dalam Pengelolaan Lingkungan Hidup

- *Setup Management*

Dalam menjalankan bisnisnya, PT PJB Services menerapkan kaidah-kaidah standar internasional asset management, dengan mempertimbangkan dan mengoptimalkan berbagai prioritas pemanfaatan danpemeliharaan aset baik untuk kinerja jangka pendek maupun kesinambungan jangka panjang, dan antara investasi modal dan biaya operasi, risiko dan kinerja.

- *Overhaul Power Plant*

PT PJB Services menyediakan jasa overhaul yang komprehensif untuk pemeliharaan pembangkit listrik yang mengacu pada OEM (Original Equipment Manufacturer) procedure dan standar kualitas.

- *Project Services*

Jasa lainnya berhubungan dengan Pembangkit Listrik yang menjadi unggulan untuk memenuhi ekspektasi pelanggan, seperti Relocation, Refurbishment & Rehabilitation, Remaining Life Assesment dan Retrofit.

Gambar 2. 2 Produk dan Jasa PT PJB Services

2.1.3 Wilayah Operasional

PT PJB Services telah mengelola unit jasa O&M yang tersebar di 26 lokasi dari Aceh sampai dengan Tidore. Persebaran unit jasa O&M Perseroan sebagai berikut

- PLTU Kertas Kraft Aceh 2 x 18 MW
- PLTA Asahan 2 x 90 MW
- PLTG Duri 20 MW
- PLTU Tenayan 2 x 110 MW

- PLTU Air Anyir Bangka 2 x 30 MW
- PLTU Belitung 2 x 16,5 MW
- PLTU Banjarsari 2 x 110 MW
- PLTU Indramayu 3 x 330 MW
- PLTU Rembang 2 x 315 MW
- PLTU Tanjung Awar-Awar 2 x 350 MW
- PLTMG Bawean 3 x 1 MW
- PLTA Brantas 18 MW
- PLTU Pacitan 2 x 315 MW
- PLTU Paiton 1 x 660 MW
- PLTU Pulang Pisau 2 x 60 MW
- PLTU Balikpapan 2 x 110 MW
- PLTU Amurang 2 x 55 MW
- PLTU Kendari 2 x 12 MW
- PLTU Ropa 2 x 7 MW
- PLTU Bolok 2 x 16,5 MW
- PLTU Tidore 2 x 7 MW

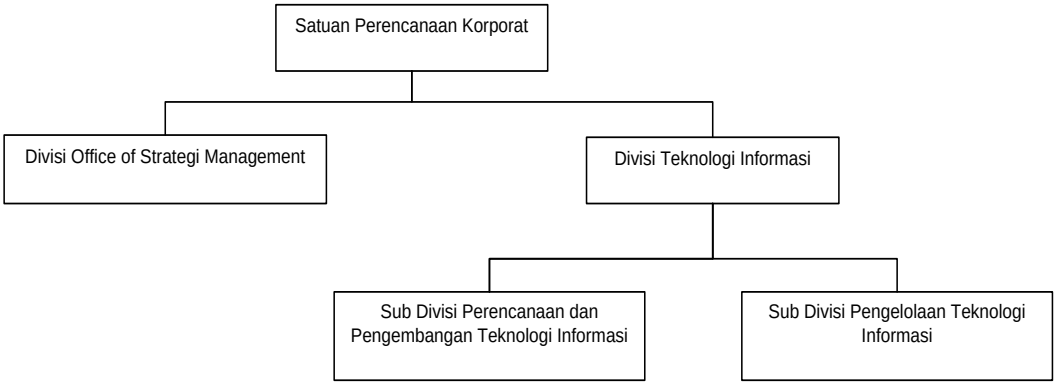
2.1.4 Profil Divisi Teknologi Informasi

Sesuai dengan SK DIREKSI PT PJB Services Nomor:136.K/010/DIR-PJBS/2017, fungsi utama dari Divisi Teknologi Informasi adalah memastikan ketersediaan dan pengembangan teknologi informasi yang handal, cepat dan mutakhir sesuai dengan bisnis perusahaan sehingga mendukung kelancaran dan kecepatan bisnis perusahaan. Adapun tugas pokok dari Divisi Teknologi Informasi antara lain:

a. Merencanakan dan mengembangkan *IT Management System* yang sistematis, sinergis dan profitable dengan bisnis maupun operasional perusahaan
b. Mengelola strategi tenologi informasi sehingga tercapai sasaran sesuai dengan master plan yang telah disusun
c. Mengelola pemutahiran perangkat lunak dan infrastruktur teknologi informasi guna mempercepat proses dan memberinilai tambah pada bisnis perusahaan

d. Mengelola perencanaan dan penggunaan anggaran investasi yang berkaitan dengan teknologi informasi guna menjamin ketersediaan infrastruktur dan aplikasi yang handal dan mendukung operasional perusahaan
e. Mengelola layanan infrastruktur, aplikasi serta pemeliharaannya (fisik dan kemanan data) baik yang dilaksanakan sendiri maupun menggunakan provider sehingga tercapai jaminan tingkat layanan dan keamanan sistem informasi yang telah ditetapkan
f. Memastikan seluruh kegiatan divisi sesuai dengan *IMS (Integrated Management System),* peraturan yang berlaku dan telah dimitigasi resikonya sehingga mampu memberikan kinerja optimal bagi perusahaan

Adapun struktur organisasi dari Divisi Teknologi Informasi sebagai berikut



Gambar 2.3 Struktur Organisasi Divisi Teknologi Informasi

Sumber: SK DIREKSI PT PJB Services Nomor:136.K/010/DIR-PJBS/2017

Dari Gambar 2.3, terlihat bahwa Divisi Teknologi Informasi dalam PT PJB Services berada dibawah Satuan Perencanaan Korporat. Hal ini bertujuan agar Divisi Teknologi Informasi ini dapat menjadi pendorong dalam inovasi dan percepatan pengambilan bisnis di perusahaan dengan menggunakan teknologi informasi.

2.1.5 Budaya Perusahaan

Budaya perusahaan PT PJB Services merupakan cerminan dari tata nilai dan perilaku yang melekat diseluruh karyawan dalam melaksanakan misi guna mewujudkan visi perusahaan. Tata nilai yang merupakan kristalisasi dari nilai-nilai

budaya PT PJB Services terangkum dalam akronim **SIAP** yang merupakan kepanjangan dari ***Service Oriented, Integrity, Active Learning,*** dan ***Professional***, yang memiliki makna sebagai berikut :

- ***Service Oriented*** (Orientasi Pelayanan Pelanggan), yaitu kemauan dan kemampuan untuk peduli terhadap kebutuhan pelanggan (internal/ eksternal) dalam memberikan layanan produk / jasa dalam rangka mencapai kepuasan pelanggan sehingga mampu membangun dan menjaga loyalitas pelanggan
- ***Integrity*** (Integritas), yaitu kemauan dan kemampuan mematuhi peraturan dan etika perusahaan, menegakkan kejujuran, bertanggung jawab, berani menyampaikan kebenaran, menyelaraskan perilaku pribadi terhadap nilai-nilai perusahaan agar terwujud landasan yang kuat dalam mencapai tujuan perusahaan
- ***Active Learning*** (Pembelajaran Aktif), yaitu secara aktif mencari dan menemukan area-area baru untuk pembelajaran, secara regular menciptakan dan mengambil keuntungan dari kesempatan belajar yang ada, menggunakan pengetahuan dan keterampilan yang baru diperoleh pada pekerjaan dan belajar melalui aplikasinya.
- ***Professional*** (Orientasi Pada Pencapaian), yaitu kemauan dan kemampuan untuk bekerja dengan lebih baik, mencapai standar keberhasilan yang lebih tinggi, berorientasi pada kualitas dengan mengoptimalkan sumber daya yang tersedia

Gambar 2.4 Budaya Perusahaan

Mengadopsi cara Perusahaan ekselen kelas dunia dalam membangun dan mengelola budaya, maka Perusahaan kemudian menjabarkan *Core Values* itu menjadi 14 *Common Behavior* (Perilaku). 14 Perilaku yang mencerminkan *Core Values* itu disingkat dengan kata ***REACHING THE SKY*** yang sekaligus menggambarkan keinginan seluruh insan perusahaan untuk membawa perusahaan meraih prestasi yang sangat tinggi. Huruf pertama dalam kata ***REACHING THE SKY*** merupakan huruf pertama dari perilaku yang ditetapkan yaitu :

- 4 huruf pertama *(REAC)* mencerminkan *Core Values Service Oriented* (Orientasi Pada Pelayanan)
- 4 huruf kedua *(HING)* mencerminkan *Core Values Integrity* (Integritas)
- Huruf dalam *THE* mencerminkan *Core Values Active Learning* (Pembelajaran aktif)
- Huruf dalam *SKY* mencerminkan *Core Values Professional* (Orientasi Pada Pencapaian)

Perilaku yang menjadi ciri dari *Core Values Service Oriented*. Seorang yang melayani dengan sepenuh hati, maka akan mempunyai 2 ciri perilaku: *Responsive* (cepat tanggap) dan *Enthusiastic* (antusias). Kedua perilaku itu kurang powerful kalau ternyata cepat tanggap dan antusias itu tidak sesuai dengan permintaan/ekspektasi pelanggan. Oleh karena itu kita letakkan *Affirmative* dan *Care* sebagai perilaku berikutnya. Selanjutnya untuk *Core Values Integrity*. Ciri perilaku pertama orang yang berintegritas adalah *Honest* (jujur). Orang yang berintegritas, maka dirinya akan berperilaku sebagai orang *Independent* (bebas dari benturan kepentingan). Selanjutnya orang yang berintegritas, maka ia punya perilaku *Noble-Minded* (berbudi luhur). Akhirnya orang yang berintegritas dalam perilakunya selalu dibimbing oleh *Godly* (nilai-nilai ketuhanan). Selanjutnya *Core Values Active Learning*. Perilaku pertama dari pembelajar adalah selalu berpikir untuk pengembangan diri berdasarkan refleksi pengalamannya. Perilaku berikutnya adalah kemauan untuk belajar dari orang dengan Humble Learner (rendah hati). Akhirnya seorang yang pembelajar, maka perilakunya selalu mencerminkan keinginan untuk menjadi ahli (*expert minded*). Selanjutnya *Core Values Professional* (berorientasi pada pencapaian). Seorang profesional akan memulai pekerjaan dengan menetapkan target yang terus meningkat dan menantang (*stretching targets*). Selanjutnya profesional akan selalu berinovasi dalam melaksanakan pekerjaannya (*keep innovating*) dan selalu fokus pada hasil (*yield focus*)

2.2 Sistem, Informasi, Keamanan Informasi, Sistem Manajemen Keamanan Informasi

Sebagai mana yang kita ketahui, pengertian dari sebuah sistem, informasi, kemanan informasi dan sistem manajemen keamanan informasi memiliki pengertian yang berbeda, sehingga perlu dijabarkan pengertian dari masing- masing sistem, informasi, kemanan informasi dan sistem manajemen keamanan informasi itu sendiri.

2.2.1 Sistem

Adapun pengertian dari sistem dari beberapa pendapat yaitu sebagai berikut.

- Menurut KBBI (Kamus Besar Bahasa Indonesia) pengertian sistem yaitu perangkat unsur yang secara teratur saling berkaitan sehingga membentuk suatu totalitas, bisa juga diartikan sebagai sususan yang teratur dari pandangan teori, asas maupun sebuah metode (KBBI, 2017).
- Menurut Jogiyanto (2003:34), Sistem merupakan suatu pendekatan prosedur dan pendekatan komponen. Dengan pendekatan prosedur, sistem dapat didefinisikan sebagai kumpulan dari prosedur-prosedur yang mempunyai tujuan tertentu. Sedangkan sistem didefinisikan sebagai pendekatan komponen yaitu kumpulan dari komponen yang saling berhubungan satu dengan yang lainnya membentuk satu kesatuan untuk mencapai tujuan tertentu.
- Menurut Williams dan Sawyes (2007:552), Sistem adalah kumpulan dari komponen-komponen yang saling berhubungan yang saling berinteraksi untuk melakukan suatu tugas untuk mencapai suatu tujuan.
- Menurut O'Brian dan Marakas (2009:24), Sistem adalah kumpulan komponen yang saling berhubungan dengan batasan yang jelas, dan bekerja sama untuk mencapai tujuan dengan menerima input dan menghasilkan output dalam suatu proses transformasi yang terorganisasi.

Dari pemaparan diatas maka dapat disimpulkan sistem merupakan seperangkat elemen yang saling berinteraksi atau terhubung satu sama yang lainnya untuk mencapai tujuan tertentu.

2.2.2 Informasi

Adapun pengertian informasi dari beberapa pendapat pendapat ahli sebegai berikut.

- Menurut KBBI (Kamus Besar Bahasa Indonesia), Informasi merupakan penerangan, pemberitahuan atau kabar maupun berita tentang sesuatu,keseluruhan makna yang menunjang amanat yang terlihat dalam bagianbagian amanat tersebut (KBBI, 2017).
- Menurut Jogiyanto (1999:692), Informasi merupakan hasil dari pengolahan data dalam satu bentuk yang lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian - kejadian (event) yang nyata (fact) digunakan untuk pengambilan keputusan.

- Informasi adalah pengetahuan atau data yang memiliki nilai pada suatu organisasi (ISO/IEC, 2009)

Sehingga dapat disimpulkan bahwa informasi merupakan hasil pengolahan data yang berguna bagi penerimanya

2.2.3 Keamanan Informasi

Keamanan informasi adalah suatu usaha bagaimana menjaga/mempertahankan kerahasiaan, integritas, dan ketersediaan dari suatu informasi (ISO/IEC, 2009). Keamanan informasi melibatkan penerapan dan pengelolaan dari langkah-langkah pengamanan yang tepat dan melihatkan pertimbangan dari berbagai ancaman, dengan tujuan memastikan keberhasilan bisnis yang berkelanjutan dan dapat meminimalkan insiden keamanan informasi. Keamanan informasi dapat dicapat dengan melalui penerapan dari berbagai macam kontrol, yang dipilih berdasarkan pertimbangan dari proses manajemen risiko dan dikelola melalui sistem manajemen keamanan informasi. Kontrol dapat berupa kebijakan, proses, prosedur, struktur organisasi, software maupun hardware untuk mengamankan aset informasi yang ada. Setiap kontrol harus dispesifikasikan, diterapkan, dipantau, dikaji dan ditingkatkan ketika dibutuhkan, untuk dapat memastikan bahwa keamanan informasi dapat terjaga dan tujuan bisnis perusahaan dapat tercapai. Kontrol-kontrol diharapkan dapat terintegrasi dengan baik sesuai dengan keadaan dan proses bisnis perusahaan.

Pencapaian keamanan informasi pada suatu organisasi bukan berarti bahwa organisasi tersebut tidak akan mengalami kebocoran atau insiden keamanan informasi sama sekali. Melalui adanya praktik – praktik keamanan informasi yang dilengkapi dengan adanya sistem manajemen yang mendukung dan telah distandarkan, maka organisasi akan dapat meningkatkan keamanan informasi secara terus menerus. Aspek-aspek dasar keamanan informasi (ISO/IEC, 2009) adalah meliputi 3 aspek sebagai berikut:

1. *Confidentiality* (Kerahasiaan)

   Merupakan aspek yang memastikan bahwa suatu informasi hanya bisa diakses oleh orang-orang yang berwenang saja, dan menjamin kerahasiaan dari data yang dikirim, diterima maupun disimpan.

2. *Integrity* (Integritas)

   Merupakan aspek yang menjamin tidak adanya perubahan pada data tanpa seizin pihak yang berwenang, sehingga terjaga keutuhan dan keakuratan informasi beserta prosesnya.

3. *Availability* (Ketersediaan)

   Merupakan aspek yang memberi jaminan atas ketersediaan data pada saat dibutuhkan, kapanpun dan dimanapun. Aspek ini juga memastikan bahwa hanya pengguna yang berhak saja ang dapat menggunakan informasi dan perangkat terkait.

Gambar 2. 5 Aspek Keamanan Informasi

Ketika ketiga aspek ini dapat terpenuhi, maka pada saat itulah suatu informasi dapat dikatakan telah aman. Ketika salah satu aspek tidak terpenuhi maka pada saat itulah terjadi insiden keamanan informasi. Dampak dari insiden keamanan informasi bergantung pada seberapa penting proses bisnis yang terganggu ketika salah satu aspek tersebut tidak dipenuhi.

2.2.4 Sistem Manajemen Keamanan Informasi

Sistem manajemen keamanan informasi (SMKI) adalah pendekatan yang sistematis untuk membangun, mengimplementasi, mengoperasikan, memantau, mengkaji, menjaga dan meningkatkan keamanan informasi pada suatu organisasi untuk dapat mencapai tujuan bisnis (ISO/IEC, 2009). Suatu sistem manajemen

keamanan informasi dapat terdiri dari kebijakan, prosedur, pedoman dan sumber daya maupun aktivitas terkait yang dikelola oleh organisasi, dengan tujuan untuk menjaga aset informasi.

Sistem manajemen keamanan informasi dilakukan berdasarkan pada penilaian risiko dan risiko yang diterima oleh organisasi untuk dapat secara efektif merancang penanggulangan dan pengelolaan risiko. Analisis dari persyaratan atau kebutuhan, dan penerapan kontrol yang tepat untuk memastikan pengamanan pada aset informasi merupakan kunci dari suksesnya implementasi sistem manajemen keamanan informasi. Berikut ini adalah faktor – faktor utama kesuksesan implementasi SMKI (Peltier, 2014):

1. Adanya praktik dan kerangka kerja untuk implementasi, pengelolaan, pemantauan dan peningkatan keamanan informasi agar terus konsisten dengan budaya organisasi.
2. Dukungan dan komitmen yang nyata dari semua level manajemen.
3. Proses – proses untuk menunjuang aktivitas manajemen keamanan informasi
4. Implementasi dan penggunaan sistem untuk mengukur kinerja manajemen keamanan informasi

Dari kesuksesan keamanan informasi yang dijabarkan oleh Peltier, dapat terlihat jelas bahwa bila suatu perusahaan ingin menerapkan keamananan informasi dengan sukses pada organisasinya, maka organisasi tersebut harus memiliki pendekatan atau kerangka kerja yang jelas untuk implementasi, pengelolaan, pemantauan hingga peningkatan keamanan informasi. Kesuksesan keamanan informasi pada perusahaan sangat bergantung pada sistem manajemen keamanan informasi yang diterapkan pada perusahaan tersebut.

2.3 ISO 27001:2005

ISO/IEC 27001 merupakan sebuah standar internasional tentang teknologi informasi yang dibuat oleh 2 (dua) organisasi yaitu ISO/IEC (the International Organization for Standardization) dan IEC (the Internasional Elechtrotecgnical Comission). ISO 27001:2005 adalah sebuah dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Managemen System (ISMS)* yang memberikan gambaran secara umum mengenai apa saja yang harus

dilakukan oleh sebuah organisasi atau enterprise dalam usaha rangka mengimplementasikan konsep konsep keamanan informasi.

Berdasarkan ISO/IEC 27001, tujuan dari sistem manajemen keamanan informasi pada dasarnya adalah untuk menjaga kerahasiaan, integritas dan ketersediaan informasi dengan menerapkan proses manajemen risiko dan memberikan keyakinan terhadap pihak yang berkepentingan bahwa risiko yang ada telah dikelola dengan baik. ISO/IEC 27001 secara khusus merupakan standar persyaratan teknologi informasi yang membahas sistem manajemen keamanan informasi (ISO/IEC, 2005). Standar internasional ini dapat digunakan sebagai persyaratan untuk membangun, menerapkan, mengelola dan terus meningkatkan sistem manajemen keamanan informasi dalam suatu organisasi. ISO 27001: 2005 memiliki 11 kelompok domain yaitu:

A.5. Kebijakan keamanan

A.6. Organisasi keamanan informasi

A.7. Manajemen aset

A.8. Keamanan sumber daya manusia

A.9 Keamanan fisik dan lingkungan

A.10 Manajemen komunikasi dan operasi

A.11 Kontrol akses

A.12 Akuisisi, pengembangan dan perawatan sistem informasi

A.13 Manajemen insiden keamanan informasi

A.14 Manajemen keberlangsungan bisnis

A.15 Kesesuaian

Dalam struktur ISO 27001:2005, kontrol domain dimulai pada A.5, sedangkan A.1 sampai A.4 merupakan pendahuluan sebelum mengimplementasi kontrol-kontrol yang ada pada ISO 27001:2005. Adapun isi dari A.1 sampai A.4 itu adalah sebagai berikut:

A.0. Pengantar

A.1. Ruang Lingkup

A.2. Istilah dan Definisi

A.3. Struktur Standar

A.4. Penilaian Risiko dan Penanggulangan

ISO 27001:2005 memiliki 133 kontrol keamanan informasi, dan pada pelaksanaannya perusahaan dapat memilih kontrol mana yang paling relevan dengan kondisi di lapangan dengan melakukan penilaian resiko dan aset pada tahapan awal. Detail dan tahapan implementasi dari kontrol disebutkan pada dokumen ISO yang lain yaitu ISO 27002. Sehingga dapat dikatakan ISO 27001 sebenarnya merupakan suatu standar untuk mendapatkan sertifikasi keamanan dari manajemen viewpoint yang menggunakan ISO 27002 untuk panduan dari sisi *security control*.

ISO/IEC 27001:2005 menggunakan model siklus *PDCA* atau *Plan-DoCheck-Act*, yang menggambarkan keseluruhan proses sistem manajemen keamanan informasi (Pramudita, 2016). Siklus ini akan dilakukan secara rutin untuk mempertahankan dan mengembangkan sistem manajemen keamanan informasi.

Gambar 2.6 Skema *PDCA*

Berikut ini adalah penjelasan dari tahap-tahap siklus *PDCA*:

1. *Plan* atau Perencanaan

   Perencanaan disini merupakan proses dalam membangun Sistem Manajemen Keamanan Informasi dengan menerapkan peraturan, kebijakan dan tujuan dengan mengembangkan prosedur-prosedur untuk mengelola risiko yang ada

2. *Do* atau Pelaksanaan

   Pelaksanaan adalah proses pengimplementasian dan pengoperasian sistem manajemen keamanan informasi yang telah direncanakan pada tahap sebelumnya

3. *Check* atau Pengecekan

   Pengecekan adalah proses pemantauan dan pengkajian dari sistem manajemen keamanan informasi dengan menukur kinerja dari kontrol - kontrol yang diterapkan, seperti peraturan dan kebijakan, lalu hasil dari pengecekan akan dijadikan bahan kajian manajemen.

4. *Act* atau Penindakan

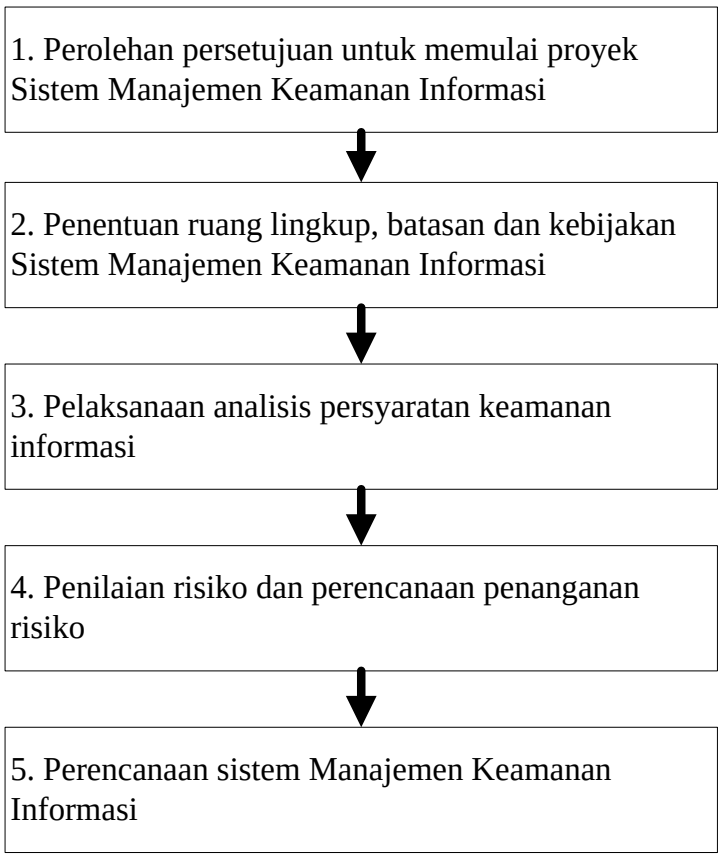
   Pada tahap penindakan ini, berdasarkan kajian manajemen pada tahap sebelumnya, pengembangan atau perbaikan dari sistem manajemen keamanan informasi dilakukan pada tahap ini.

2.4 ISO 27002

ISO/IEC 27002 merupakan standar yang dikeluarkan oleh organisasi yang sama dengan pembuat ISO/IEC 27001. ISO 27002 adalah seperangkat standar dan prosedur yang berkaitan dengan keamanan dan kontrol informasi yang memungkinkan bisnis untuk menerapkan keamanan yang tepat. Standar ini merupakan penjelasan detail dari ISO 27001 dalam hal rekomendasi praktik terbaik untuk pembuatan Sistem Manajemen Keamanan Informasi (SMKI). ISO 27002 memuat ratusan cara untuk menangani keamanan informasi dan memiliki banyak bab tentang cara mengamankan informasi. Beberapa bab berkaitan dengan sumber daya manusia dan interaksi mereka dengan informasi, sementara yang lain memuat cara sebuah bisnis untuk mengontrol akses dan kelangsungan usaha dengan prosedur keamanan mereka. Keamanan informasi biasanya identik dengan teknologi informasi (TI), tetapi ISO 27002 juga berkaitan dengan mengamankan informasi diatas kertas, meskipun sebagian besar dari standar ini ditujukan untuk departemen TI.

2.5 ISO 27003

ISO/IEC 27003 merupakan standar yang dikeluarkan oleh organisasi yang sama dengan pembuat ISO/IEC 27001. ISO/IEC 27003 merupakan panduan pengimplementasian sistem manajemen keamanan informasi untuk suatu organisasi yang didasarkan pada persyaratan ISO/IEC 27001 (ISO/IEC, 2009). Standar internasional ini berfokus pada aspek-aspek penting yang dibutuhkan untuk dapat mendesain dan mengimplementasi sistem manajemen keamanan informasi dengan sukses. Panduan penerapannya dapat digunakan oleh semua tipe organisasi seperti perusahaan komersial, pemerintah, atau bahkan organisasi non profit dalam semua ukuran organisasi. Setiap organisasi pada dasarnya memiliki kompleksitas dan risiko yang unik. Organisasi yang kecil dapat memperkecil lingkup aktivitas dari ISO/IEC 27003 dan organisasi dengan kompleksitas yang lebih besar dapat secara efektif menerapkan semua aktivitas yang disarankan oleh ISO/IEC 27003.



Gambar 2.7 Alur implementasi SMKI (ISO/IEC 27003)

Penerapan ISO/IEC 27001 berdasarkan panduan dari ISO/IEC 27003 memiliki 5 tahap utama (Pramudita, 2016) yaitu :

1. **Perolehan persetujuan manajemen untuk memulai proyek Sistem Manajemen Keamanan Informasi**

   Pada tahap pertama ini, proses diawali dengan melakukan klarifikiasi terhadap prioritas pada organisasi dalam penerapan sistem manajemen keamanan informasi. Dialanjutkan dengan proses selanjutnya adalah penentuan dan penataan ruang lingkup awal Sistem Manajemen Keamanan Informasi. Dilanjutkan dengan penentuan peran dan tanggung jawab dari ruang lingkup sistem manajen keamanan informasi. Dan diakhiri dengan pembuatan kasus bisnis dan rencana proyek untuk mendapatkan persetujuan manajemen.

2. **Penentuan ruang lingkup, batasan dan kebijakan Sistem Manajemen Keamanan Informasi**

   Pada tahap ini diawali dengan penentuan ruang lingkup dan batasan pada organisasi. Lalu dilanjutkan dengan penentuan ruang lingkup dan batasan dari teknologi komunikasi informasi dan fisik. Proses selanjutnya adalah pengintegrasian setiap ruang lingkup dan batasan yang ada untuk mendapatkan ruang lingkup dan batasan Sistem Manajemen Keamanan Informasi. Dan diakhiri dengan pembuatan kebijakan dan peraturan sistem manajemen keamanan informasi dan mendapatkan persetujuan dari manajemen.

3. **Pelaksanaan analisis persyaratan keamanan informasi**

   Analisa dilakukan dengan menentukan persyaratan keamanan informasi untuk setiap proses sistem manajemen keamanan informasi dan pengidentifikasian aset dari ruang lingkup dan batasan sistem manajemen keamanan informasi. Lalu diakhiri dengan penilaian keamanan informasi pada organisasi tersebut.

4. **Penilaian risiko dan perencanaan penanganan risiko**

   Proses diawali dengan melakukan penilaian risiko, dan ditindak lanjuti dengan penentuan tujuan kontrol beserta kontrol-kontrol yang ada. Lalu diakhiri dengan mendapatkan otorisasi dari manajemen untuk mengimplementasikan dan mengoperasikan sistem manajemen keamanan informasi.

5. Perencanaan sistem manajemen keamanan informasi

Tahap terakhir ini akan mengolah data dan informasi yang dihasilkan dari 4 tahap sebelumnya untuk membuat perencanaan aktual untuk melengkapi sistem manajemen keamanan informasi.

2.6 ISO 27005

ISO/IEC 27005 merupakan standar yang dikeluarkan oleh organisasi yang sama dengan pembuat ISO/IEC 27001 dan ISO/IEC 27003. ISO/IEC 27005 merupakan panduan manajemen risiko keamanan informasi untuk suatu organisasi yang didasarkan pada persyaratan ISO/IEC 27001 (ISO/IEC, 2009). Standar ISO/IEC 27005 sebagai panduan manajemen risiko keamanan informasi berisi :

1. Penilaian risiko (klausa 8)
2. Penanganan risiko (klausa 9)
3. Penerimaan risiko (klausa 10),
4. Komunikasi risiko (klausa 11), dan
5. Pemantauan dan pengkajian risiko (klausa 12)

ISO/IEC 27005 mengukur risiko dalam 2 dimensi yaitu dampak bisnis (*business impact*) dan kemungkinan terjadi (*likelihood*). Dalam contoh yang diberikan dari ISO/IEC 27005 pada bagian Annex E menggunakan skala 1 – 5 untuk dimensi dampak dan kemungkinan terjadi. Berikut ini contoh tabel Skala Dampak dan Kemungkinan berdasarkan ISO/IEC 27005

Tabel 2.1 Contoh Skala Dampak dan Kemungkinan (ISO/IEC 27005)

Skala	Dampak Bisnis	Kemungkinan
1	Sangat Kecil	Hampir tidak mungkin terjadi
2	Kecil	Kecil kemungkinan terjadi
3	Sedang	Mungkin terjadi
4	Besar	Sering terjadi
5	Sangat Besar	Sangat sering terjadi

2.7 Sistem Pendukun Keputusan (SPK)

Sistem Pendukung Keputusan (SPK) atau *Decision Support System (DSS)* adalah sebuah sistem yang mampu memberikan kemampuan pemecahan masalah

maupun kemampuan pengkomunikasian untuk masalah dengan kondisi semi terstruktur dan tak terstruktur. Sistem ini digunakan untuk membantu pengambilan keputusan dalam situasi semi terstruktur dan situasi yang tidak terstruktur, dimana tak seorangpun tahu secara pasti bagaimana keputusan seharusnya dibuat (Turban, 2001). SPK bertujuan untuk menyediakan informasi, membimbing, memberikan prediksi serta mengarahkan kepada pengguna informasi agar dapat melakukan pengambilan keputusan dengan lebih baik.

Sprague dan Watson mendefinisikan Sistem Pendukung Keputusan (SPK) sebagai sistem yang memiliki lima karakteristik utama yaitu (Sprague et.al, 1993):

1. Sistem yang berbasis komputer.
2. Dipergunakan untuk membantu para pengambil keputusan
3. Untuk memecahkan masalah-masalah rumit yang mustahil dilakukan dengan kalkulasi manual
4. Melalui cara simulasi yang interaktif
5. Dimana data dan model analisis sebaai komponen utama

Dalam membangun sistem pendukung keputusan tentunya melibatkan berbagai metode sistem pendukung keputusan, berbagai metode telah diterapkan pada sistem pendukung keputusan untuk menghasilkan alternatif yang sesuai dengan kriteria-kriteria yang telah ditetapkan oleh suatu organisasi atau perusahaan. Berbagai metode yang telah diterapkan tentunya terdapat kelebihan dan kelemahan yang banyak dipaparkan di setiap kajian, penyempurnaan tentunya selalu dilakukan dari berbagai penelitian.

Adapun beberapa metode SPK yaitu *Multi-Atribute Utility Theory (MAUT), Analytical Hierarchy, Process (AHP), Fuzzy Set Theory, Case-based Reasoning (CBR), Data Envelopment Analysis (DEA), Simple Multi-Attribute Rating Technique (SMART), Goal Programming (GP), ELECTRE, PROME THEE, Simple Addictive Weighting (SAW), dan Technique for Order of Preference by similiarity to Ideal Solution (TOPSIS).*

Adapun dalam penelitian ini, penulis akan menggabungkan 2 (dua) metode SPK, yaitu *AHP* dan *TOPSIS*. Kombinasi metode *AHP* dan *TOPSIS* pernah diterapkan dalam menentukan objek wisata terbaik di Pulau Bali. Metode AHP digunakan untuk pembobotan masing - masing kriteria kemudian metode TOPSIS

digunakan untuk analsis data dalam menentukan prioritas objek wisata terbaik (Anhar & Widodo 2013). Kombinasi metode AHP dan TOPSIS dipilih dengan alasan metode AHP memliki kelebihan berdasar pada matriks perbandingan pasangan dan melakukan analisis konsistensi. Sedangkan metode TOPSIS dapat menyelesaikan pengambilan keputusan secara praktis, karena konsepnya sederhana dan mudah dipahami, komputasinya efisien, serta memiliki kemampuan mengukur kinerja relatif dari alternatif-alternatif keputusan (Juliyanti et al. 2011).

.

2.8 Analytical Hierarchy Process (AHP)

Metode *AHP* dikembangkan oleh Dr. Thomas L. Saaty dari Wharton School of Bussines pada tahun 1970-an untuk mengorganisasikan informasi dan judgement dalam memilih alternatif yang disukai (Marimin, 2004). Pada dasarnya proses pengambilan keputusan menggunakan metode AHP adalah memilih suatu alternatif. Peralatan utama AHP adalah sebuah hierarki fungsional dengan input utamanya persepsi manusia.

Prosedur atau langkah-langkah dalam metode AHP meliputi (Kusrini, 2007):

a) Mengidentifikasi masalah dan menentukan solusi yang diinginkan, lalu menyusun hierarki dari permasalahan yang dihadapi.
b) Menentukan prioritas elemen
   1) Membuat perbandingan pasangan, yaitu membandingkan elemen secara berpasangan sesuai kriteria yang diberikan.
   2) Matriks perbandingan berpasangan diisi menggunakan bilangan untuk merepresentasikan kepentingan relatif dari suatu elemen terhadap elemen yang lainnya.
c) Sintesis

   Hal-hal yang dilakukan dalam langkah ini adalah :

   1) Menjumlahkan nilai-nilai dari setiap kolom pada matriks
   2) Membagi setiap nilai dari kolom dengan total kolom yang bersangkutan untuk memperoleh normalisasi matriks.
   3) Menjumlahkan nilai-nilai dari setiap baris dan membaginya dengan jumlah elemen untuk mendapatkan nilai rata-rata.
d) Mengukur Konsistensi

Dalam membuat keputusan, penting untuk mengetahui seberapa baik konsistensi yang ada karena kita tidak menginginkan keputusan berdasarkan pertimbangan dengan konsistensi yang rendah. Hal-hal yang dilakukan dalam langkah ini adalah:

1) Kalikan setiap nilai pada kolom pertama dengan prioritas relatif elemen pertama, nilai pada kolom kedua dengan prioritas relatif elemen kedua, dan seterusnya.

2) Jumlahkan setiap baris.

3) Hasil dari penjumlahan baris dibagi dengan elemen prioritas relatif yang bersangkutan.

4) Jumlahkan hasil bagi di atas dengan banyaknya elemen yang ada, hasilnya disebut maks.

e) Menghitung *Consistency Indeks (CI)* dengan rumus

$$CI = \frac{\lambda_{max} - 1}{n-1} \quad (2.1)$$

Dimana n = banyaknya elemen

f) Hitung Rasio Konsistensi / *Consistency Ratio (CR)* dengan rumus:

$$CR = \frac{CI}{CR} \quad (2.2)$$

Dimana :

CR = Consistency Ratio

CI = Consistency Indeks

IR = Indeks Random Consistency

g) Memeriksa konsistensi hierarki. Jika nilainya lebih dari 10%, maka penilaian data judgment harus diperbaiki. Namun jika rasio konsistensi (CI/IR) kurang atau sama dengan 0,1, maka hasil perhitungan bisa dinyatakan benar. Daftar Indeks Random Konsistensi (IR) bisa dilihat pada Tabel 2.2.

Tabel 2. 2 Daftar Indeks random Konsistensi (IR)

Ukuran matriks	1.2	3	4	5	6	7	8
Nilai IR	0	0.58	0.9	1.12	1.24	1.32	1.41
Ukuran matriks	9	10	11	12	13	14	15
Nilai IR	1.45	1.49	1.51	1.48	1.56	1.57	1.59

2.9 Technique for Others Preference by Similarity to Ideal Solution (TOPSIS)

Metode TOPSIS pertama kali diperkenalkan oleh Hwang dan Yoon tahun 1981, dengan gagasan utamanya datang dari konsep kompromi solusi yakni alternatif yang dipilih memiliki jarak terdekat dengan solusi ideal positif (solusi optimal) dan memiliki jarak terjauh dari solusi ideal negatif (solusi non-optimal). Jadi memilih yang terbaik dari pemilahan, akan menjadi alternatif yang terbaik (Tzeng, 2011). Berikut ini adalah contoh sebuah matriks dengan alternatif dan kriteria

$$D = \begin{bmatrix} x_{ij} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \quad (2.3)$$

Dimana:

D = matriks keputusan

m = alternatif

n = kriteria

Xij = alternatif ke – i dan kriteria ke - j

Langkah-langkah metode TOPSIS sebagai berikut (Manurung 2010):

a) Menentukan matriks keputusan yang ternormalisasi

Setiap elemen pada matriks *D* dinormalisasikan untuk mendapatkan matriks normalisasi *R*. Setiap normalisasi dari nilai r_{ij} dapat dilakukan dengan perhitungan sebagai berikut:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad (2.4)$$

Untuk *i=1,2,3,…,m;*

j=1,2,3,…,n

b) Pembobotan pada matriks yang telah dinormalisasi

Diberikan bobot W = (w1,w2,…,wn), sehingga *weighted normalized matrix* V dapat dihasilkan sebagai berikut:

$$V = \begin{bmatrix} w_{11}r_{11} & \cdots & w_{1n}r_{1n} \\ \vdots & \ddots & \vdots \\ w_{m1}r_{m1} & \cdots & w_{nm}r_{nm} \end{bmatrix} \quad (2.5)$$

Dengan $i=1,2,3,\ldots,m;$

$j=1,2,3,\ldots,n$

c) Menentukan solusi ideal positif dan solusi ideal negative

Solusi ideal positif dinotasikan dengan A^+ dan solusi ideal negatif dinotasikan dengan A^-, sebagai berikut:

$$A^+ = \{(\max v_{ij} \mid j \in J)(\min v_{ij} \mid j \in J'), i = 1,2,3,\ldots m\} = \{v_1^+, v_2^+, \ldots v_m^+\} \quad (2.6)$$

$$A^- = \{(\max v_{ij} \mid j \in J)(\min v_{ij} \mid j \in J'), i = 1,2,3,\ldots m\} = \{v_1^-, v_2^-, \ldots v_m^-\} \quad (2.7)$$

Dimana:

v_{ij} = elemen matriks v baris ke-*i* dan kolom ke-*j*

J = {j=1,2,3,…,n dan j berhubung dengan *benefit criteria*}

J’ = {j=1,2,3,…,n dan j berhubung dengan *cost criteria*}

d) Menghitung *Separation Measure*

Separation measure ini merupakan pengukuran jarak dari suatu alternatif ke solusi ideal positif dan solusi ideal negatif. Perhitungan matematisnya adalah sebagai berikut:

Separation measure untuk solusi ideal positif

$$D_1^+ = \sqrt{\sum_{j=1}^{n}(v_{ij} - v_{j1}^+)^2} \text{ , dengan } i = 1,2,3,\ldots,n \quad (2.8)$$

Separation measure untuk solusi ideal negatif

$$D_1^- = \sqrt{\sum_{j=1}^{n}(v_{ij} - v_{j1}^-)^2} \text{ , dengan } i = 1,2,3,\ldots,n \quad (2.9)$$

e) Menghitung kedekatan relative dengan ideal positif

Kedekatan relative dari alternatif A^+ dengan solusi ideal A^- direpresentasikan dengan:

$$V_i = \frac{V_1^-}{V_1^- + V_1^+} \text{ , dengan } 0 < Vi < 1 \text{ dan } i = 1,2,3,\ldots,m \quad (2.10)$$

f) Mengurutkan Pilihan

Alternatif dapat dirangking berdasarkan urutan *Vi*. Maka dari itu, alternatif terbaik adalah salah satu yang berjarakterpendek terhadap solusi ideal dan berjarak terjauh dengan solusi ideal negatif.

2.10 Penelitian Terdahulu

Berikut ini beberapa penelitian terdahulu yang digunakan sebagai referensi dalam penelitian Rekomendasi Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Menggunakan Metode AHP-TOPSIS Berdasarkan ISO/IEC 27001 (Studi Kasus: PT PJB Services).

Referensi pertama, Thesis yang berjudul "Perancangan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001 (Studi Kasus : PT Sentra Vidya Utama) ". Ditulis oleh Eka Pramudita Purnomo pada tahun 2016. Thesis ini menjelaskan bagaimana cara membuat Perancangan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001:2005 dan ISO 27001:2013. Thesis ini juga menjelaskan perbedaan antara ISO 27001:2005 dan ISO 27001:2013.

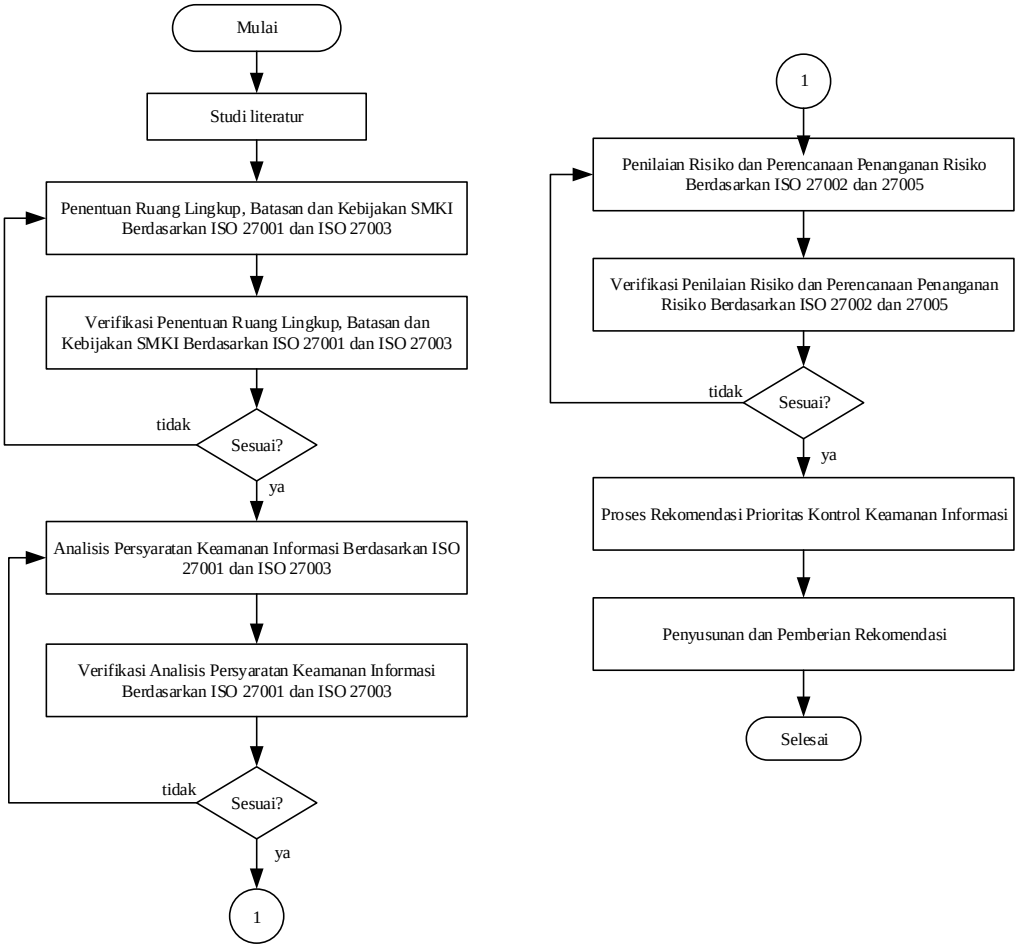
Referensi kedua, Jurnal yang dipublikasikan oleh ITSMART berjudul "Analisis Perbandingan Menggunakan Metode AHP, TOPSIS, dan AHP-TOPSIS dalam Studi Kasus Sistem Pendukung Keputusan Penerimaan Siswa Program Akselerasi". Ditulis oleh Estining Nur et al pada tahun 2013. Pada jurnal ini membandingkan tiga metode Sistem Pendukung Keputusan (SPK) yaitu AHP (Analytical Hierarchy Process), TOPSIS (Technique For Order Preference by Similarity to Ideal Solution) dan metode gabungan AHP-TOPSIS dengan mengambil studi kasus mengenai seleksi penerimaan siswa program percepatan belajar (akselerasi) di SMP Negeri 1 Wonogiri. Pada penelitian ini menerapkan analisis perbandingan dengan menggunakan Hamming Distance dan Euclidean Distance. Untuk parameter yang dipakai yaitu hasil perangkingan sekolah dan peringkat rapor siswa akselerasi dengan tujuan melihat kesesuaian hasil dengan ketetapan sekolah. Parameter lainnya yaitu nilai rapor siswa akselerasi untuk melihat tingkat keberhasilan dan juga sebagai parameter untuk menentukan metode rekomendasi. Hasil yang diperoleh dari nilai Hamming Distance terhadap hasil perangkingan sekolah, didapatkan metode AHP-TOPSIS menjadi urutan terbaik dengan 96.02%. Untuk nilai Hamming Distance terhadap peringkat rapor siswa akselerasi diperoleh bahwa metode TOPSIS menjadi metode terbaik dengan persentase 84.21%. Merujuk pada hasil Euclidean Distance nilai rapor, metode AHP menjadi metode terbaik dengan nilai 0.47367.

Referensi ketiga, jurnal yang dipublikasikan oleh IEEE berjudul "*Enhanced Information Security Management System Framework Design Using ISO 27001 And Zachman Framework A Study Case of XYZ Company*". Ditulis oleh Andre Aginsa et al pada tahun 2016. Di jurnal ini, penulis membuat Sistem Manajemen Keamananan Informasi yang sesuai dengan kondisi perusahaan dengan mengadopsi ISO 27001 dan menggabungkan dengan *Zachman Framework* (5W1H). Pada awal penelitian, penulis meggunakan *Zachman Framework* untuk menentukan ruang lingkup SMKI yang akan dibuat, dengan menerapkan *What, Why, Where, Who, When,* dan *How*. Setelah itu dilakukan perencanaan pembuatan SMKI mengadopsi ISO 27001 berdasarkan ruang lingkup yang sudah diidentifikasi oleh *Zachman Framework* sebelumnya. Hasil dari penelitian ini berupa kerangka kerja yang mudah digunakan oleh berbagai perusahaan untuk membuat Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan pada ISO/IEC 27001.

Referensi keempat, penelitian yang berjudul "Sistem Pendukung Keputusan Seleksi Penerima Beasiswa Dengan Metode AHP Dan TOPSIS (Studi Kasus: FMIPA USU)". Ditulis oleh Manurung pada tahun 2010. Dalam Pada penelitian ini akan diangkat suatu kasus yaitu mencari alternative terbaik berdasarkan kriteria-kriteria yang telah ditentukan dengan mengggunakan metode AHP kemudian mencari solusi dengan metode TOPSIS. Metode ini dipilih karena mampu menyeleksi alternative terbaik dari sejumlah alternatif, dalam hal ini alternatif yang dimaksudkan yaitu yang berhak menerima beasiswa berdasarkan kriteria-kriteria yang ditentukan. Penelitian dilakukan dengan mencari nilai bobot untuk setiap atribut, kemudian dilakukan proses pengurutan kandidat yang akan menentukan alternatif yang optimal, yaitu mahasiswa terbaik.

BAB 3
METODOLOGI PENELITIAN

Bab ini akan dibahas mengenai tahapan dan prosedur yang dilakukan dalam penelitian dan pemecahan masalah yang ada. Bagian ini berfungsi sebagai gambaran kerangka yang mengarahkan penelitian untuk mencapai tujuan yang telah ditetapkan. Proses dalam penelitian ini dapat dilihat pada gambar 3.1 berikut ini:



Gambar 3.1 Diagram Alur Penelitian

3.1 Studi Literatur

Sebelum melaksanakan penelitian, studi literatur terlebih dahulu dilaksanakan untuk memperkuat dasar-dasar pelaksanaan penelitian. Studi literatur dilakukan dengan cara mengumpulkan serta mempelajari literatur-literatur yang berkaitan maupun mendukung untuk proses penelitian. Studi literature yang digunakan pada

penelitian ini bersumber pada practice book, jurnal nasional dan internasional, artikel, media internet, serta wawancara langsung terhadap pihak Divisi Teknologi Informasi PT PJB Services. Adapun tahapan dalam studi literature ini adalah kajian pustaka mengenai implementasi ISO/IEC 27001:2005, Metode *Analytical Hierarchy Process (AHP) - Technique for Others Preference by Similarity to Ideal Solution (TOPSIS),* dan telaah proses bisnis dan keamanan informasi pada PT PJB Services.

3.1.1 Kajian Pustaka

Kajian pustaka dilakukan untuk mengetahui landasan teori sebagai acuan dasar penelitian yang terkait dengan topik penelitian yang dilaksanakan. Teori dasar yang dikaji antara lain

- ISO 27001: Berisi tentang aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan
- ISO 27002: Terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.
- ISO 27003: Panduan implementasi sistem manajemen keamanan informasi perusahaan.
- ISO 27005: Tentang panduan pelaksanaan manajemen risiko terkait ISO/IEC 27001.
- *Analytical Hierarchy Process (AHP) - Technique for Others Preference by Similarity to Ideal Solution (TOPSIS).* Berkaitan dengan metode Sistem Pengambilan Keputusan untuk prioritas kontrol pada penelitian ini.

3.1.2 Telaah Proses Bisnis

Telaah proses bisnis dilakukan untuk mengetahui kondisi perusahaan tempat studi kasus dilaksanakan, yaitu PT PJB Services. Proses yang dilakukan antara lain mengumpulkan data-data tentang perusahaan, seperti visi, misi, struktur organisasi perusahaan, proses bisnis, serta kaitannya dengan keamanan informasi seperti divisi yang bertanggung jawab terhadap keamanan informasi pada perusahaan. Langkah

ini diperlukan agar gambaran umum tentang perusahaan dapat diketahui, sehingga hal tersebut akan membantu proses penelitian yang akan dilaksanakan.

3.2 Penentuan Ruang Lingkup, Batasan dan Kebijakan SMKI Berdasarkan ISO 27001 dan ISO 27003

Penentuan ruang lingkup, batasan dan kebijakan SMKI harus dibuat sebagai dasar dari proses perancangan SMKI tahap berikutnya.

3.2.1 Penetapan Ruang Lingkup dan Batasan

Proses mendapatkan informasi pada pada penetapan ruang lingkup dan batasan dilakukan dalam bentuk wawancara langsung dengan tingkatan manajemen di Divisi Teknologi Informasi PT PJB Services. Hasil dari tahap ini adalah dokumen ruang lingkup SMKI adalah:

1. Batasan organisasi yang termasuk dalam ruang lingkup pembuatan SMKI
2. Fungsi dan bagian dari organisasi dalam lingkup pembuatan SMKI
3. Tanggung jawab untuk asset informasi yang dimiliki oleh organisasi dalam lingkup pembuatan SMKI

Rencana form kuesioner dapat dilihat pada Lampiran 1

3.2.2 Pembuatan Kebijakan SMKI

Input dasar untuk pembuatan kebijakan SMKI adalah dokumen ruang lingkup SMKI dan wawancara langsung dengan perwakilan manajemen yang dipilih oleh PT PJB Services sebagai penanggung jawab penerapan SMKI pada perusahaan. Berdasarkan ISO/IEC 27003 kebijakan SMKI yang akan dibuat harus memiliki bagian:

1. Pendahuluan

   Penjelasan singkat terkait topik dari kebijakan yang dibuat.
2. Ruang Lingkup

   Berisi bagian atau aktivitas dari organisasi yang mendapat dampak dari kebijakan yang dibuat.
3. Tujuan

   Berisi tujuan dari kebijakan yang dibuat

4. Tanggung Jawab

   Berisi siapa saja yang bertanggungjawab terhadap tindakan yang termasuk dalam kebijakan yang dibuat.

5. Hasil Yang Diharapkan

   Berisi hasil yang akan diperoleh perusahaan ketika tujuan tercapai.

6. Kebijakan Terkait

   Berisi kebijakan-kebijakan lainnya yang relevan untuk mencapai tujuan dari kebijakan yang dibuat.

3.3 Verifikasi Ruang Lingkup, Batasan dan Kebijakan SMKI Berdasarkan ISO 27001 dan ISO 27003

Verifikasi terhadap ruang lingkup, batasan dan kebijakan yang dibuat harus dilakukan antara pihak auditor dengan pihak perusahaan dalam hal ini adalah PT PJB Services agar hasil dari tahap penentuan sebelumnya terbukti sesuai dengan kebutuhan perusahaan. Hasil berupa dokumen ruang lingkup dan kebijakan SMKI dari tahapan sebelumnya diserahkan kepada PT PJB Services untuk dikaji kesesuaiannya. Bila ruang lingkup, batasan dan kebijakan SMKI belum sesuai dengan kebutuhan PT PJB Services maka akan dilakukan revisi dengan menentukan ulang ruang lingkup, batasan dan kebijakan SMKI terkait. Bila verifikasi berupa persetujuan telah didapatkan maka tahap selanjutnya yaitu analisis persyaratan keamanan informasi berdasarkan ISO 27001 dan 27003 dapat dimulai.

3.4 Analisis Persyaratan Keamanan Informasi Berdasarkan ISO 27001 dan ISO 27003

Analisis persyaratan keamanan informasi harus dilakukan dan ditetapkan. Kesepakatan dari tahap sebelumnya serta aset – aset informasi yang ada pada perusahaan merupakan pertimbangan utama dalam penetapan persyaratan keamanan informasi.

3.4.1 Penetapan Persyaratan Keamanan Informasi

Melalui wawancara dengan pihak Divis Teknologi Informasi PT PJB Services sesuai dengan lingkup yang telah dibuat, maka hasil yang diharapkan dari tahap ini

adalah dokumen pendukung yang berisisi arsitektur jaringan komunikasi, daftar proses utama beserta lokasi dan penanggung jawabnya dan sistem informasi yang digunakan untuk mendukung proses tersebut.

3.4.2 Identifikasi Aset Informasi

Setiap aset informasi yang masuk dalam lingkup dari proses-proses yang ada, akan diidentifikasi dan dijelaskan secara detail sesuai dengan proses-proses utama terkait. Wawancara akan dilakukan terhadap setiap penanggung jawab atau perwakilan dari proses-proses utama untuk mendapatkan informasi aset-aset informasi apa saja yang perlu dilindungi.

Hasil dari tahapan ini adalah dokumen daftar aset informasi pada Divisi Teknologi PT PJB Services. Dokumen daftar aset informasi setidaknya dapat memberikan informasi seperti aset informasi, proses dimana aset informasi dilibatkan,penanggung jawab dari aset informasi terkait. Daftar pertanyaan yang ditanyakan pada wawancara dapat dilihat pada Lampiran 2

3.5 Verifikasi Analisis Persyaratan Keamanan Informasi Berdasarkan ISO 27001 dan ISO 27003

Verifikasi terhadap analisis persyaratan keamanan informasi harus dilakukan oleh pihak auditor dengan perusahaan dalam hal ini adalah PT PJB Services agar hasil dari tahap sebelumnya terbukti sesuai dengan kondisi perusahaan. Hasil berupa dokumen analisis persyaratan keamanan informasi sebelumnya diserahkan kepada PT PJB Services untuk dikaji kesesuaiannya. Bila hasil dari analisa tersebut belum sesuai dengan kondisi PT PJB Services maka akan dilakukan revisi dengan melakukan analisa persyaratan keamanan informasi lagi. Bila verifikasi berupa persetujuan telah didapatkan maka tahap selanjutnya yaitu penilaisan resiko dan perencanaan risiko berdasarkan ISO 27001 dan 27005.

3.6 Penilaian Risiko dan Perencanaan Penanganan Risiko Berdasarkan ISO 27002 dan 27005

Implementasi dari SMKI diharapkan dapat menempatkan risiko keamanan informasi secara tepat. Identifikasi, evaluasi dan perencanaan penanganan risiko

seperti pemilihan kontrol yang tepat merupakan langkah penting dalam implementasi SMKI

3.6.1 Penilaian Risiko

Penilaian risiko dilakukan dengan mempertimbangkan ruang lingkup dan kebijakan sistem manajemen keamanan informasi yang telah disepakati dan berdasarkan pada aset – aset informasi yang telah diidentifikasi sebelumnya. Wawancara dengan para penanggung jawab aset informasi yang telah diidentifikasi dari tahap sebelumnya dilakukan untuk memperoleh informasi terkait risiko terhadap aset informasi yang ada.

Tahap pertama yang dilakukan yaitu dengan melakukan wawancara terhadap pihak-pihak yang bertanggung jawab terhadap proses bisnis yang sesuai dengan lingkup sistem manajemen keamanan informasi serta penetapan kriteria risiko. Setelah waawancara dilakukan, maka tahap selanjutnya adalah melakukan estimasi tingkat risiko dengan membuat kesepakatan kriteria risiko dengan pihak perusahaan baik dalam segi dampak maupun kemungkinan terjadinya risiko. Estimasi akan dilakukan terlebih dahulu terhadap aspek dampak dan kemungkinan pada masing - masing risiko lalu dilanjutkan dengan mengestimasikan tingkat risiko dari besaran dampak dan kemungkinan risiko. Setelah melakukan estimasi resiko, hasil dari tahap ini adalah berupa dokumen daftar risiko dan hasil penilaian risiko terhadap masing-masing risiko yang ada.

Tabel 3.1 Contoh Penilaian Resiko

No	Risiko	Penanggung jawab	Dampak	Kemungkinan	Level Risiko
S1	Harddisk Rusak	Bagian Data Center & Storage	2	4	3 – High
S2	Virus	bagian network & Security	2	2	2 – Medium

Contoh pada Tabel 3.1 menggunakan asumsi skala 1 – 5 untuk penilaian dampak dan kemungkinan risiko. Pengisian dampak dan kemungkinan risiko dilakukan oleh pihak Divisi Teknologi Informasi PT PJB Services dengan mempertimbangkan kriteria dan skala yang disepakati perusahaan. Level risiko akan didiskusikan

dengan perusahaan untuk menentukan bagaimana cara penilaian dan tingkat risiko yang paling tepat dengan kondisi perusahaan. Pada penelitian ini penilaian risiko dibagi menjadi 4 (empat) yaitu kemungkinan terjadi serta dampak resiko yang dibagi menjadi 3 (tiga) yaitu dampak reputasi, dampak kerugian dan dampak produktivitas. Rencana wawancara untuk penilaian risiko ada pada Lampiran 3

3.6.2 Pembuatan Rencana Penanganan Risiko

Rencanan penaganan risiko harus dibuat agar risiko-risiko yang telah teridentifikasi pada tahap sebelumnya mendapatkan penanganan secara tepat. Perencanaan dilakukan dengan melakukan pemilihan terhadap kontrol-kontrol yang dapat diterapkan agar risiko-risiko yang ada dapat dikelola dengan baik sesuai dengan penjelasan detail pada ISO 27002.

Proses perencanaan penanganan risiko tahap awal, memerlukan data dari hasil penilaian risiko yang merupakan tahap sebelumnya. Perencanaan penanganan risiko akan difokuskan pada risiko-risiko dengan tidak dapat diterima oleh kriteria yang ditentukan perusahaan. Risiko-risiko yang tidak dapat diterima ini akan dicarikan alternatif kontrol berdasarkan ISO/IEC 27002. Alternatif kontrol didapatkan dengan membuat hubungan antara risiko yang ada dengan klausa kontrol masing-masing berdasarkan ISO/IEC 27002. Setelah mendapatkan klausa kontrol yang ada, maka akan dilakukan pemilihan kontrol sebagai tindakan penanganan risiko bersama dengan penanggung jawab sistem manajemen keamanan informasi pada Divisi Teknologi Informasi PT PJB Services. Penanggung jawab sistem manajemen keamanan informasi akan melakukan pemilihan alternatif kontrol yang diajukan. Hasil dari tahap ini adalah daftar kontrol yang dipilih beserta tujuan pemilihan kontrol dalam bentuk dokumen pernyataan pemberlakuan *(Statement Of Applicability).*

Tabel 3.2 Contoh Pernyataan Pemberlakuan (Statement of Applicability)

ID Kontrol	Kontrol	Diterapkan (Ya/Tidak)	Tanggung Jawab	Rekomendasi Implementasi
5.1.1	Kebijakan untuk keamanan informasi	Ya	Manajer TI	Kebijakan terkait akses ke intranet dan aplikasi intranet berdasarkan jabatan dan fungsi karyawan
8.1.1	Inventaris Asset	Ya	Manajer TI	Setiap hardware dan software di inventarisir dalam sebuah sistem database

3.7 Verifikasi Penilaian Risiko dan Perencanaan Penanganan Risiko Berdasarkan ISO 27002 dan 27005

Pada tahapan ini hasil dari penilaian risiko dan perencanaan penanganan risiko berupa daftar risiko dan pernyataan pemberlakukan akan diverifikasi oleh pihak perusahaan yaitu penanggung jawab SMKI PT PJB Services. Verifikasi dilakukan agar memberi keyakinan bahwa penilaian risiko dan perencanaan penanganan risiko telah sesuai dengan kondisi, keinginan dan kebutuhan perusahaan. Bila perusahaan menilai bahwa penilaian dan perencanaan penanganan risiko belum sesuai maka akan dilakukan revisi terhadap hasil penilaian risiko ataupun hasil perencanaan penanganan risiko.

3.8 Proses Rekomendasi Prioritas Kontrol Keamanan Informasi

Pada tahap ini, hasil dari penilaian risiko dan perencanaan penganganan risiko yang sudah diverifikasi akan dilakukan perhitungan dengan metode AHP-TOPSIS. Tujuan dari proses ini adalah dapat memberikan rekomendasi prioritas terhadap kontrol apa saja yang yang dilakukan. Perhitungan dengan metode AHP-TOPSIS ini mengambil inputan bobot dari metode AHP kemudian mendapatkan urutannya dengan metode TOPSIS. Adapun kriteria yang akan dijadikan sebagai pemilihan alternatife adalah dari penilaian risiko yaitu kemungkinan terjadi, dampak reputasi, dampak financial dan dampak produktivitas

3.9 Penyusunan dan Pemberian Rekomendasi

Tahap terakhir yaitu penyususnan dan pemberian rekomendasi berdasarkan tahapan sebelumnya. Penanggung jawab yang tertulis dalam proses pembuatan SMKI akan diwawancarai langsung untuk mendapatkan *feedback* atau respon balik terkait hasil rekomendasi. Feedback atau respon balik ini diharapkan dapat memberikan gambaran terkait penilaian dan penanganan risiko yang ada di Divisi Teknologi Informasi PT. PJB Services

3.10 Jadwal Penelitian

Penelitian ini dilakukan selama 5 (lima) bulan. Terdapat 6 (enam) kegiatan yang akan dilakukan selama penelitian. Adapun rincian kegiatan dapat dilihat pada Tabel 3.3.

Tabel 3. 3 Jadwal Penelitian

No	Kegiatan	Maret				April				Mei				Juni			
		2018				2018				2018				2018			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur	■	■														
2	Menentukan objek penelitian			■	■												
3	Pengumpulan Data - Wawancara - Pengamatan Objek					■	■	■	■	■	■	■	■	■	■		
4	Analisis Data													■	■		
5	Pengambilan keputusan dan pembuatan laporan rekomendasi															■	■
6	Kesimpulan																■

BAB 4
HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini akan dibahas mengenai hasil penelitian pada masing-masing tahapan atau prosedur yang telah disepakati pada bagian metode penelitian. Hasil penelitian berupa dokumen yang lebih detail akan dilampirkan pada bagian lampiran, sesuai dengan kompleksitas dari hasil masing-masing tahapan atau prosedur.

4.1 Penetapan Ruang Lingkup dan Batasan

Penetapan ruang lingkup dan batasan dilakukan dengan cara melakukan pertemuan dan diskusi dengan pihak manajemen di Divisi Teknologi Informasi PT PJB Services dalam hal ini adalah Manajer Teknologi Informasi. Berikut ini adalah beberapa keputusan utama yang diambil mengenai ruang lingkup dan batasan assessment untuk pembuatan rekomendasi Sistem Manajemen Keamanan Informasi dari pertemuan tersebut:

1. Seluruh asset baik hardware maupun aplikasi *production* yang berada di Data Center Divisi Teknologi Informasi PT PJB Services termasuk dalam lingkup Sistem Manajemen Keamanan Informasi (SMKI).
2. Manajemen Divisi Teknologi Informasi PT PJB Services berkomitmen dan mendukung *assessment* untuk pembuatan rekomendasi Sistem Manajemen Keamanan Informasi (SMKI). Dukungan dapat berupa dukungan keuangan, tambahan sumber daya manusia atau sumber daya lainnya yang dibutuhkan menyesuaikan antara kebutuhan dan kemampuan Divisi Teknologi Informasi PT PJB Services dalam menerapkannya.
3. Belum ada peraturan hukum ataupun peraturan kontrak yang mengikat Divisi Teknologi Informasi PT PJB Services dalam hal penerapan implementasi kontrol keamanan informasi.
4. Disaster Recovery Center milik Divisi Teknologi Informasi PT PJB Services yang berlokasi di Jakarta, unit-unit dari PT PJB Services dan Aplikasi yang

masih berstatus pengembangan merupakan pengecualian pada ruang lingkup SMKI.

Hasil dari keputusan tersebut dibuatkan dokumen berjudul "Dokumen Ruang Lingkup SMKI" yang dapat dilihat lebih detail pada Lampiran A - Dokumen Ruang Lingkup SMKI.

4.2 Pembuatan Kebijakan SMKI

Pada proses pembuatan kebijakan SMKI, diawali dengan melakukan wawancara sekaligus diskusi langsung dengan pihak Manajer Divisi Teknologi Informasi PT PJB Services. Fokus pertanyaan mengenai kebijakan SMKI adalah penetapan tujuan SMKI, hasil yang diharapkan dan tanggung jawab SMKI pada Divisi Teknologi Informasi PT PJB Services. Berikut ini adalah hasil dari wawancara langsung mengenai kebijakan SMKI dari pertemuan tersebut:

1. Tujuan utama dari *assessment* untuk pembuatan rekomendasi SMKI ini adalah untuk mengetahui risiko-risiko beserta kontrol prosedur apa yang harus dilakukan untuk meminimalisasi risiko terkait keamanan informasi dan sekaligus sebagai bahan masukan jika perusahaan akan mengimplementasikan SMKI
2. Hasil yang diharapkan melalui *assessment* ini adalah dokumen daftar risiko beserta kontrolnya sesuai dengan kondisi perusahaan.
3. Tanggung jawab pada Sistem Manajemen Keamanan Informasi di Divisi Teknologi Informasi PT PJB Services dibagi pada 3 (tiga) peran yaitu manajer sebagai penanggung jawab utama, asisten manajer sebagai penanggung jawab pelaksana SMKI, dan masing-masing pemilik aset informasi sebagai pelaksana perlindungan terhadap aset informasinya.
4. Saat ini belum ada kebijakan tertulis yang ada untuk menunjang kebijakan SMKI.

Hasil lebih detail mengenai kebijakan Sistem Manajemen Keamanan Informasi lebih detail pada Lampiran B - Kebijakan Sistem Manajemen Keamanan Informasi.

4.3 Verifikasi Ruang Lingkup, Batasan dan Kebijakan SMKI Berdasarkan ISO 27001 dan ISO 27003

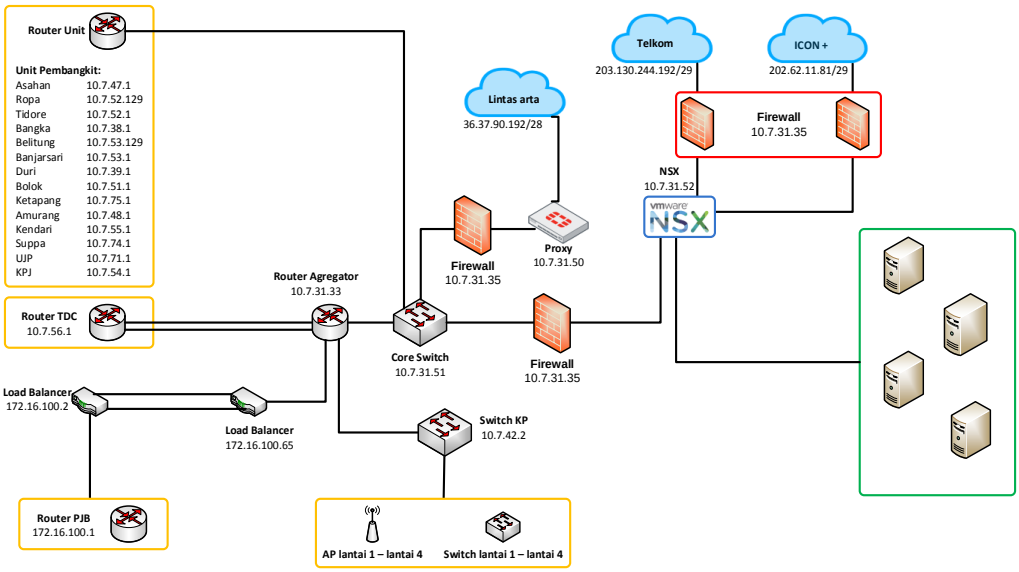
Verifikasi terhadap ruang lingkup dan kebijakan SMKI telah dilakukan dengan pemberian kedua dokumen kepada pihak manajemen Divisi Teknologi Informasi PT PJB Services untuk dilakukan revisi bilamana ada informasi yang tidak sesuai. Verifikasi dokumen dilakukan Manajer Divisi Teknologi Informasi PT PJB Services. Dalam penelitian ini, persetujuan terhadap Ruang Lingkup dan Kebijakan SMKI dilakukan dengan penandatanganan dokumen oleh Manajer Divisi Teknologi Informasi terhadap kedua dokumen tersebut. Hasil akhir dokumen ruang lingkup dan kebijakan SMKI dapat dilihat pada Lampiran A - Ruang Lingkup SMKI dan pada Lampiran B – Kebijakan Sistem Manajemen Keamanan Informasi.

4.4 Penetapan Persyaratan Keamanan Informasi

Penetapan persyaratan keamanan informasi dilakukan dengan menetapkan bagian atau proses bisnis mana saja yang harus dianalisa lebih lanjut terkait aset-aset informasi yang ada pada Divisi Teknologi Informasi PT PJB Services untuk dilindungi. Ada 5 (lima) bagian yang dipilih untuk mewakili keseluruhan proses yang ada yaitu adalah Bagian *Data Center & Storage*, Bagian *Network & Security*, Bagian *Core Businees Application*, Bagian *Enterprise Asset Management (EAM) Application*, dan Bagian *Supporting Application*. Melalui diskusi dengan Manajer Divisi Teknologi Informasi PT PJB Services, berikut ini penetapan orang-orang yang akan dijadikan sumber acuan dalam identifikasi aset informasi untuk langkah selanjutnya disesuaikan dengan bagian dan proses bisnis yang ada pada Divisi Teknologi Informasi PT PJB Services:

1. Perwakilan Bagian *Data Center & Storage* yaitu Saudara Bagus Dahono Putro
2. Perwakilan Bagian *Network & Security* yaitu Saudara Rahmat Sudrajat
3. Perwakilan Bagian *Core Business Application* yaitu Saudara Muhammad Rendra Suryadi
4. Perwakilan Bagian *Enterprise Asset Management (EAM) Application* yaitu Saudara Slamet Fajar Suryadi
5. Perwakilan Bagian *Supporting Application* yaitu Saudara Roynther Ayub Djami

Dari Manajemen Divisi Teknologi Informasi PT PJB Services menyatakan bahwa belum ada persyaratan kontrol keamanan informasi khusus yang diturunkan dari peraturan, undang-undang, hukum atau kontrak perjanjian pada perusahaan.



Gambar 4. 1 Arsitektur Jaringan

Dari gambar diatas, secara umum dapat dijelaskan sebagai berikut

1. Komponen terpenting dalam arsitektur jaringan ini adalah Core Switch karena perangkat inilah yang menghubungkan jaringan antara user (unit dan kantor pusat) dengan Server Farm.
2. Setiap data yang akan menuju dari dan ke Server Farm serta data yang keluar menuju internet terlebih dahulu diinspeksi oleh Firewall
3. Pada Server Farm memiliki 3 (tiga) jenis kategori yaitu
    a. Server DMZ: Server ini digunakan untuk mempublish aplikasi yang akan di akses melalui internet secara langsung, contohnya website PT PJB Services
    b. Server Production: Server ini digunakan untuk aplikasi internal yang digunakan untuk mendukung kegiatan perusahaan tetapi tidak di publish ke internet secara langsung, contohnya aplikasi presensi
    c. Server Development: Server ini digunakan untuk aplikasi yang masih dalam tahap pengembangan/pengerjaan.
4. Aplikasi production pada PT PJB Services dibedakan menjadi 3 (tiga) yaitu

a. *Core Business Application* : Aplikasi ini berkaitan dengan kegiatan operasional perusahaan sehari-hari seperti keuangan dan surat-menyurat
b. *Enterprise Asset Management (EAM) Application* : Aplikasi ini berkaitan dengan pengelolaan asset pembangkit yang digunakan di unit-unit kerja PT PJB Services. Aplikasi ini bernama IBM Maximo.
c. *Supporting Application.* : Aplikasi ini untuk mendukung suatu divisi atau unit tertentu untuk melakukan operasional, contohnya aplikasi helpdesk IT

5. PT PJB Services memiliki 3 (tiga) link provider untuk menunjang kebutuhan akses internet yaitu PT Aplikanusa Lintas Arta, PT Telkom, dan PT ICON+.
6. Akses internet user, website dan aplikasi di filter pada perangkat proxy. Proxy ini digunakan untuk memblokir akses ke situs maupun aplikasi yang dapat mengganggu produktivitas pada saat jam kerja, contohnya pornografi serta membedakan akses antara staf dan manajemen.
7. Pengaturan arus informasi (NAT, VLAN dan Routing) pada Server Farm diatur oleh NSX VMWARE yaitu suatu software diciptakan oleh perusahaan VMWARE yang berfungsi seperti perangkat keras router dan switch tetapi berbasis aplikasi/software (*Software Defined Network*).

4.5 Identifikasi Aset Informasi

Setiap bagian yang telah diidentifikasi dari tahap sebelumnya, maka akan diidentifikasi lebih lanjut aset-aset informasi yang terlibat dalam proses-proses yang ada. Wawancara dilakukan terhadap setiap penanggung jawab atau perwakilan dari bagian untuk mendapatkan informasi aset-aset informasi apa saja yang perlu dilindungi. Daftar pertanyaan yang ditanyakan pada wawancara dapat dilihat pada bagian Lampiran C – Kuesioner Identifikasi Aset dan Risiko. Berikut ini adalah hasil identifikasi aset informasi yang ada pada Divisi Teknologi Informasi PT PJB Services :

Tabel 4.1 Aset–Asset Informasi

No	Bagian	PIC	Asset Informasi
1	*Data Center & Storage*	Bagus Dahono Putro	Access Data Center
			Server Aplikasi
			VM Ware
			Storage
			Media Backup
			UPS Data Center
			Precision AC
			Monitoring Kelembapan dan Suhu
			Fire Protection
2	*Network & Security*	Rahmat Sudrajat	Router Agregator
			Firewall Server Farm
			Proxy Internet
			Endpoint Protection
			Core Switch
			Access Switch
			Load Balancer
			Access Point
			DNS
			DHCP Server
			Active Directory
3	*Core Business Application*	Muhammad Rendra Suryadi	Aplikasi Pengelolaan Pelanggan
			Aplikasi Monitoring Proyek
			Aplikasi SDM
			Aplikasi Knowledge Management
			Aplikasi Forum Diskusi Karyawan
			Aplikasi Audit Internal
			Aplikasi Recruitment
			Aplikasi Presensi
			Aplikasi Keuangan
			Aplikasi Penilaian Kinerja Karyawan
4	*Enterprise Asset Management (EAM) Application*	Slamet Fajar Suryadi	Aplikasi Manajemen Asset Pembangkit
			Aplikasi LK3
			Aplikasi Dashboard Pembangkit
5	*Supporting Application*	Roynther Ayub Djami	Aplikasi Helpdesk IT
			Aplikasi Dokumen Center
			Aplikasi Event
			Aplikasi Manajemen Resiko
			Aplikasi Inventaris
			Aplikasi Good Corporate Governance

			Aplikasi Pemesanan Kendaraan
			Aplikasi Portal Berita
			Website Perusahaan
			Email
			Aplikasi Pengadaan / SCM
			Aplikasi Dokumentasi Proyek

Tabel diatas merupakan daftar asset informasi yang dimiliki oleh setiap penanggung jawab bagian di Divisi Teknologi Informasi PT PJB Services.

4.6 Verifikasi Analisis Persyaratan Keamanan Informasi Berdasarkan ISO 27001 dan ISO 27003

Verifikasi terhadap analisis persyaratan keamanan informasi telah dilakukan dengan pemberian dokumen kepada masing-masing penanggung jawab terhadap asset informasi pada Divisi Teknologi Informasi PT PJB Services untuk dilakukan revisi bilamana ada informasi yang tidak sesuai. Dalam penelitian ini, persetujuan terhadap Analisis Persyaratan Keamanan Informasi dilakukan dengan penandatanganan dokumen hasil wawancara oleh masing-masing penanggung jawab terhadap asset informasi pada Divisi Teknologi Informasi PT PJB Services. Dokumen akhir dari Analisis Persyaratan Keamanan Informasi dapat dilihat pada Lampiran C – Kuesioner Identifikasi Aset dan Risiko.

4.7 Penilaian Risiko

Penilaian risiko dilakukan dengan mempertimbangkan ruang lingkup dan kebijakan sistem manajemen keamanan informasi yang telah disepakati dan berdasarkan pada aset – aset informasi yang telah diidentifikasi sebelumnya. Wawancara dengan para penanggung jawab aset informasi yang telah diidentifikasi dari tahap sebelumnya dilakukan untuk memperoleh informasi terkait insiden yang pernah terjadi terhadap aset informasi yang ada. Daftar risiko merupakan gabungan antara insiden yang pernah terjadi dengan risiko umum dapat terjadi pada aset-aset tersebut.

Berikut ini adalah daftar risiko yang telah disepakati dengan pihak penanggung jawab di setiap bagian Divisi Teknologi Informasi PT PJB Services:

Tabel 4.2 Aset Informasi Bagian *Data Center & Storage*

No	Asset	Kode	Risiko
1	Access Data Center	A1	Access dari orang yang tidak berkepentingan
		A2	Adanya kerusakan Scan Kartu untuk masuk
		A3	Hilangnya Access Card
		A4	Tidak mendapat daya listrik
		A5	Database access hilang
2	Server	A6	Access dari orang yang tidak berkepentingan
		A7	Adanya kerusakan Hardware
		A8	Terserang virus/malware
		A9	Tidak terkoneksi dengan jaringan
		A10	Tidak mendapat daya listrik
		A11	Kesalahan konfigurasi
3	VM Ware	A12	Access dari orang yang tidak berkepentingan
		A13	Adanya kerusakan Hardware
		A14	Kesalahan konfigurasi
		A15	Lisensi Expired
		A16	Tidak terkoneksi dengan jaringan
4	Storage	A17	Kapasitas Penuh
		A18	Access dari orang yang tidak berkepentingan
		A19	Adanya kerusakan Hardware
		A20	Kesalahan konfigurasi
		A21	Tidak kompatible dengan server
		A22	Tidak mendapat daya listrik
		A23	Tidak terkoneksi dengan jaringan
5	Media Backup	A24	Kapasitas Penuh
		A25	Access dari orang yang tidak berkepentingan
		A26	Tidak terkoneksi dengan jaringan
		A27	Adanya kerusakan Hardware
		A28	Tidak mendapat daya listrik
		A29	Kesalahan konfigurasi
6	UPS Data Center	A30	Baterai tidak dapat menyimpan daya
		A31	Kesalahan konfigurasi
		A32	Tidak mendapat daya listrik
		A33	Adanya kerusakan Hardware
7	Precision AC	A34	Kesalahan konfigurasi
		A35	Adanya kerusakan Hardware
		A36	Tidak mendapat daya listrik
		A37	AC tidak dingin
8		A38	Adanya kerusakan Hardware
		A39	Tidak terkoneksi dengan jaringan

	Monitoring Kelembapan dan Suhu	A40	Tidak mendapat daya listrik
		A41	Data yang ditampilkan tidak sesuai (kalibrasi)
9	Fire Protection	A42	Kesalahan konfigurasi
		A43	Gas Habis
		A44	Adanya kerusakan Hardware
		A45	Tidak terkoneksi dengan sensor

Dari table diatas, terlihat bahwa risiko access dari orang yang tidak berkepentingan dan adanya kerusakan hardware terdapat pada semua asset informasi pada bagian *Data Center & Storage*. Total risiko yang ada di bagian *Data Center & Storage* berjumlah 45 risiko.

Tabel 4.3 Aset Informasi Bagian *Network & Security*

No	**Asset**	**Kode**	**Risiko**
1	Router Agregator	B1	Access dari orang yang tidak berkepentingan
		B2	Tidak mendapat daya listrik
		B3	Adanya kerusakan Hardware
		B4	Kapasitas melebihi batas
		B5	Kesalahan konfigurasi
2	Firewall Server Farm	B6	Access dari orang yang tidak berkepentingan
		B7	Tidak mendapat daya listrik
		B8	Adanya kerusakan Hardware
		B9	Kapasitas melebihi batas
		B10	Kesalahan konfigurasi
3	Proxy Internet	B11	Access dari orang yang tidak berkepentingan
		B12	Tidak mendapat daya listrik
		B13	Adanya kerusakan Hardware
		B14	Kapasitas melebihi batas
		B15	Kesalahan konfigurasi
4	Endpoint Protection	B16	Access dari orang yang tidak berkepentingan
		B17	Lisensi expired
		B18	Kapasitas lisensi melebihi batas
		B19	Kesalahan konfigurasi
5	Core Switch	B20	Access dari orang yang tidak berkepentingan
		B21	Tidak mendapat daya listrik
		B22	Adanya kerusakan Hardware
		B23	Kapasitas melebihi batas
		B24	Kesalahan konfigurasi
6	Access Switch	B25	Access dari orang yang tidak berkepentingan

		B26	Tidak mendapat daya listrik
		B27	Adanya kerusakan Hardware
		B28	Kapasitas melebihi batas
		B29	Kesalahan konfigurasi
7	Load Balancer	B30	Access dari orang yang tidak berkepentingan
		B31	Tidak mendapat daya listrik
		B32	Adanya kerusakan Hardware
		B33	Kapasitas melebihi batas
		B34	Kesalahan konfigurasi
8	Access Point	B35	Access dari orang yang tidak berkepentingan
		B36	Tidak mendapat daya listrik
		B37	Adanya kerusakan Hardware
		B38	Kapasitas melebihi batas
		B39	Kesalahan konfigurasi
		B40	User tidak bisa terkoneksi
9	DNS	B41	Kesalahan konfigurasi
		B42	Access dari orang yang tidak berkepentingan
		B43	Data rusak
		B44	Service tidak berjalan
10	DHCP Server	B45	Kesalahan konfigurasi
		B46	Access dari orang yang tidak berkepentingan
		B47	Data rusak
		B48	Service tidak berjalan
		B49	User tidak mendapatkan IP Address
11	Active Directory	B50	Kesalahan input
		B51	Access dari orang yang tidak berkepentingan
		B52	Data rusak
		B53	Service tidak berjalan
		B54	User tidak bisa melakukan otentikasi

Dari table diatas, terlihat bahwa risiko access dari orang yang tidak berkepentingan, tidak mendapat daya listrik, kapasitas melebihi batas, dan kesalahan konfigurasi terdapat pada semua asset informasi pada bagian *Network & Security*. Total risiko yang ada di bagian *Network & Security* berjumlah 54 risiko.

Tabel 4.4 Aset Informasi Bagian *Core Business Application*

No	Asset	Kode	Risiko
1	Aplikasi Pengelolaan Pelanggan	C1	Access dari orang yang tidak berkepentingan
		C2	Pencurian Data
		C3	Data pada aplikasi hilang
		C4	Aplikasi tidak bisa diakses
		C5	Kesalahan dalam input data
2	Aplikasi Monitoring Proyek	C6	Access dari orang yang tidak berkepentingan
		C7	Pencurian Data
		C8	Data pada aplikasi hilang
		C9	Aplikasi tidak bisa diakses
		C10	Kesalahan dalam input data
3	Aplikasi SDM	C11	Access dari orang yang tidak berkepentingan
		C12	Pencurian Data
		C13	Data pada aplikasi hilang
		C14	Aplikasi tidak bisa diakses
		C15	Kesalahan dalam input data
4	Aplikasi Knowledge Management	C16	Access dari orang yang tidak berkepentingan
		C17	Pencurian Data
		C18	Data pada aplikasi hilang
		C19	Aplikasi tidak bisa diakses
		C20	Kesalahan dalam input data
5	Aplikasi Forum Diskusi Karyawan	C21	Access dari orang yang tidak berkepentingan
		C22	Pencurian Data
		C23	Data pada aplikasi hilang
		C24	Aplikasi tidak bisa diakses
		C25	Kesalahan dalam input data
6	Aplikasi Audit Internal	C26	Access dari orang yang tidak berkepentingan
		C27	Pencurian Data
		C28	Data pada aplikasi hilang
		C29	Aplikasi tidak bisa diakses
		C30	Kesalahan dalam input data
7	Aplikasi Recruitment	C31	Access dari orang yang tidak berkepentingan
		C32	Pencurian Data
		C33	Data pada aplikasi hilang
		C34	Aplikasi tidak bisa diakses
		C35	Kesalahan dalam input data
8	Aplikasi Presensi	C36	Access dari orang yang tidak berkepentingan
		C37	Pencurian Data
		C38	Data pada aplikasi hilang
		C39	Aplikasi tidak bisa diakses

		C40	Kesalahan dalam input data
9	Aplikasi Keuangan	C41	Access dari orang yang tidak berkepentingan
		C42	Pencurian Data
		C43	Data pada aplikasi hilang
		C44	Aplikasi tidak bisa diakses
		C45	Kesalahan dalam input data
10	Aplikasi Penilaian Kinerja Karyawan	C46	Access dari orang yang tidak berkepentingan
		C47	Pencurian Data
		C48	Data pada aplikasi hilang
		C49	Aplikasi tidak bisa diakses
		C50	Kesalahan dalam input data

Dari table diatas, terlihat bahwa risiko access dari orang yang tidak berkepentingan, pencurian data, data aplikasi hilang, aplikasi tidak bisa diakses, dan kesalahan dalam input data pada semua asset informasi pada bagian *Core Business Application*. Total risiko yang ada di bagian *Core Business Application* berjumlah 50 risiko.

Tabel 4.5 Aset Informasi Bagian *Enterprise Asset Management Application*

No	**Asset**	**Kode**	**Risiko**
1	Aplikasi Manajemen Asset Pembangkit	D1	Access dari orang yang tidak berkepentingan
		D2	Pencurian Data
		D3	Data pada aplikasi hilang
		D4	Aplikasi tidak bisa diakses
		D5	Kesalahan dalam input data
2	Aplikasi LK3	D6	Access dari orang yang tidak berkepentingan
		D7	Pencurian Data
		D8	Data pada aplikasi hilang
		D9	Aplikasi tidak bisa diakses
		D10	Kesalahan dalam input data
3	Aplikasi Dashboard Pembangkit	D11	Access dari orang yang tidak berkepentingan
		D12	Pencurian Data
		D13	Data pada aplikasi hilang
		D14	Aplikasi tidak bisa diakses
		D15	Kesalahan dalam input data

Dari table diatas, terlihat bahwa risiko access dari orang yang tidak berkepentingan, pencurian data, data aplikasi hilang, aplikasi tidak bisa diakses, dan kesalahan

dalam input data pada semua asset informasi pada bagian *Enterprise Asset Management (EAM) Application*. Total risiko yang ada di bagian *Enterprise Asset Management (EAM) Application* berjumlah 15 risiko.

Tabel 4.6 Aset Informasi Bagian *Supporting Application*

No	**Asset**	**Kode**	**Risiko**
1	Aplikasi Helpdesk IT	E1	Access dari orang yang tidak berkepentingan
		E2	Pencurian Data
		E3	Data pada aplikasi hilang
		E4	Aplikasi tidak bisa diakses
		E5	Kesalahan dalam input data
2	Aplikasi Dokumen Center	E6	Access dari orang yang tidak berkepentingan
		E7	Pencurian Data
		E8	Data pada aplikasi hilang
		E9	Aplikasi tidak bisa diakses
		E10	Kesalahan dalam input data
3	Aplikasi Event	E11	Access dari orang yang tidak berkepentingan
		E12	Pencurian Data
		E13	Data pada aplikasi hilang
		E14	Aplikasi tidak bisa diakses
		E15	Kesalahan dalam input data
4	Aplikasi Manajemen Resiko	E16	Access dari orang yang tidak berkepentingan
		E17	Pencurian Data
		E18	Data pada aplikasi hilang
		E19	Aplikasi tidak bisa diakses
		E20	Kesalahan dalam input data
5	Aplikasi Inventaris	E21	Access dari orang yang tidak berkepentingan
		E22	Pencurian Data
		E23	Data pada aplikasi hilang
		E24	Aplikasi tidak bisa diakses
		E25	Kesalahan dalam input data
6	Aplikasi Good Corporate Governance	E26	Access dari orang yang tidak berkepentingan
		E27	Pencurian Data
		E28	Data pada aplikasi hilang
		E29	Aplikasi tidak bisa diakses
		E30	Kesalahan dalam input data
7	Aplikasi Pemesanan Kendaraan	E31	Access dari orang yang tidak berkepentingan
		E32	Pencurian Data

		E33	Data pada aplikasi hilang
		E34	Aplikasi tidak bisa diakses
		E35	Kesalahan dalam input data
8	Aplikasi Portal Berita	E36	Access dari orang yang tidak berkepentingan
		E37	Pencurian Data
		E38	Data pada aplikasi hilang
		E39	Aplikasi tidak bisa diakses
		E40	Kesalahan dalam input data
9	Website Perusahaan	E41	Access dari orang yang tidak berkepentingan
		E42	Pencurian Data
		E43	Data pada aplikasi hilang
		E44	Aplikasi tidak bisa diakses
		E45	Kesalahan dalam input data
10	Email	E46	Access dari orang yang tidak berkepentingan
		E47	Pencurian Data
		E48	Data pada aplikasi hilang
		E49	Aplikasi tidak bisa diakses
		E50	Kesalahan dalam input data
11	Aplikasi Pengadaan / SCM	E51	Access dari orang yang tidak berkepentingan
		E52	Pencurian Data
		E53	Data pada aplikasi hilang
		E54	Aplikasi tidak bisa diakses
		E55	Kesalahan dalam input data
12	Aplikasi Dokumentasi Proyek	E56	Access dari orang yang tidak berkepentingan
		E57	Pencurian Data
		E58	Data pada aplikasi hilang
		E59	Aplikasi tidak bisa diakses
		E60	Kesalahan dalam input data

Dari table diatas, terlihat bahwa risiko access dari orang yang tidak berkepentingan, pencurian data, data aplikasi hilang, aplikasi tidak bisa diakses, dan kesalahan dalam input data pada semua asset informasi pada bagian *Supporting Application*. Total risiko yang ada di bagian *Supporting Application* berjumlah 60 risiko.

Pada daftar risiko di atas, karakter pertama pada kode risiko merupakan kode untuk risiko setiap bagian dalam Divisi Teknologi Informasi PT PJB Services. Bagian *Data Center & Storage* memiliki kode A, Bagian *Network & Security* memiliki kode B, Bagian *Core Businees Application* memiliki kode C, Bagian *Enterprise Asset Management (EAM) Application* memiliki kode D, dan Bagian

Supporting Application memiliki kode E. Total risiko yang ada pada asset informasi di Data Center Divisi Teknologi Informasi PT PJB Services sebanyak 224 risiko.

Setelah mendapatkan daftar risiko yang ada, kemudian melalui diskusi langsung dengan manajer Divisi Teknologi Informasi PT PJB Services sebagai pembuat kebijakan penilaian risiko untuk menetapkan kriteria penilaian risiko keamanan informasi. Maka ditetapkan bahwa penilaian risiko mengacu pada **KEP.DIR. Nomor: 082.K/020/DIR-PJBS/2017 - Tentang Pedoman Penerapan Manajemen Risiko PT Pembangkitan Jawa Bali Services**. Berikut ini adalah kriteria penilaian risiko yang telah disepakati dalam proses penilaian risiko:

Tabel 4.7 Kriteria Penilaian Risiko Tingkat Kemungkinan *(Likelihood)*

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Dari table diatas, kriteria risiko aspek kemungkinan terjadi (*likelihood*) telah disepakati bahwa penilaian menggunakan 5 (lima) tingkat kemungkinan yaitu

sangat kecil dengan nilai 0.1, kecil dengan nilai 0.3, sedang dengan nilai 0.5, besar dengan nilai 0.7 dan sangat besar dengan nilai 0.9.

Tabel 4.8 Penilaian Risiko Aspek Dampak Kemungkinan

No Kriteria	**Tingkat Risiko**	**Nilai**	**Dampak Reputasi**	**Dampak Finansial**	**Dampak Produktivitas / Operasional**
1	Tidak Signifikan	0.05	Tidak berdampak terhadap reputasi	Tidak berdampak pada kerugian finansial	Kegiatan perusahaan terganggu, tidak memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak tidak dirasakan secara lokal maupun keseluruhan sistem.
2	Minor	0.1	Reputasi perusahaan menurun, upaya atau biaya yang dibutuhkan untuk memperbaiki minimal	Kerugian finansial tidak mengganggu kegiatan operasional	Kegiatan perusahaan terganggu, tidak signifikan memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan secara lokal (pada alat tersebut saja).
3	Medium	0.2	Reputasi perusahaan terganggu dan diperlukan upaya dan biaya untuk memperbaiki reputasi perusahaan	Kerugian finansial dapat mengganggu kegiatan operasional	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada satu entitas Unit Pembangkit.
4	Signifikan	0.4	Reputasi perusahaan rusak namun bisa diperbaiki	Kerugian finansial dapat menyebabkan kegiatan	Kegiatan perusahaan terganggu memberikan dampak terhadap

			dengan upaya dan biaya yang besar	operasional berhenti sementara	keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada Unit Kerja/ Pembangkit PJBS.
5	Malapetaka	0.8	Reputasi perusahaan rusak dan tidak bisa diperbaiki	Kerugian finansial dapat menyebabkan kebangkrutan	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada keseluruhan sistem PJBS.

Dari tabel kriteria risiko aspek dampak, dibagi menjadi 3 dampak yaitu dampak finansial, reputasi dan produktivitas/operasional. Tingkat penilaian risiko dibagi menjadi 5 (lima) tingkatan yaitu tidak signifikan dengan nilai 0.05, minor dengan nilai 0.1, medium dengan nilai 0.2, signifikan dengan nilai 0.4 dan malapetaka dengan nilai 0.8.

Penanggung jawab risiko akan memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek kemungkinan terjadi dan dampak (reputasi, kerugian, dan produktivitas) untuk masing-masing risiko yang ada. **Penilaian ini merupakan representasi dari nomor kriteria yang nantinya akan dikonversikan dengan nilai risiko sesuai dengan nomor kriteria yang dipilih**.

Tabel 4.9 Contoh Pengisian Penilaian Risiko

No	Asset	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
1	Access Data Center	Access dari orang yang tidak berkepentingan	1	2	1	1
		Adanya kerusakan Scan Kartu untuk masuk	1	1	1	1

Dari table diatas akan dilakukan konversi ke nilai risiko berdasarkan nilai risiko yang telah disepakati sebelumnya. Sebagai contoh konversi pada aset Access Data Center yang memiliki risiko akses dari orang yang tidak berkepentingan memiliki

nilai risiko kemungkinan terjadi 1 (satu). Dari tabel 4.7, kriteria 1 (satu) memiliki nilai 0,1. Sehingga nilai untuk aset Access Data Center yang memiliki risiko akses dari orang yang tidak berkepentingan dikonversi menjadi 0.1,

Tabel 4.10 Contoh Hasil Konversi Penilaian Kriteria Risiko

No	Asset	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
1	Access Data Center	Access dari orang yang tidak berkepentingan	0.1	0.1	0.05	0.05
		Adanya kerusakan Scan Kartu untuk masuk	0.1	0.05	0.05	0.05

Tahap selanjutnya adalah pemberian nilai risiko sesuai dengan kriteria yang ditentukan. Pada ISO 27001 versi 2005 penilaian risiko dilakukan oleh penanggung jawab aset informasi. Sebelum proses penilaian risiko, auditor memberikan gambaran terkait risiko-risiko yang ada serta menjelaskan cara memberikan penilaian terhadap responden atau penanggung jawab pada setiap bagian. Detail penilaian risiko dapat dilihat pada Lampiran D – Proses Penilaian Risiko. Kuesioner penilaian risiko dapat dilihat pada Lampiran E – Kuesioner Penilaian Risiko dan hasil konversi penilaian risiko pada Lampiran F – Konversi Penilaian Risiko.

4.8 Pembuatan Rencana Penanganan Risiko

Rencana penanganan risiko dibuat untuk menentukan kontrol yang tepat sesuai dengan ISO 27001:2005 yang didetailkan lagi di ISO 27002. Bersama dengan pihak Manajemen Divisi Teknologi Informasi PT PJB Services telah dilakukan penentuan hubungan antara alternative klausa kontrol dengan risiko yang harus dikontrol. Pada proses ini, masing-masing risiko akan dicocokkan dengan klausa yang dijabarkan pada ISO 27002. Berikut ini adalah kelompok risiko yang harus dikontrol dengan klausa kontrol berdasarkan ISO 27001:2005

Tabel 4.11 Kontrol Risiko

No	Klausa	Kelompok Risiko
A.5	*Security Policy*	Semua Risiko
A.6	*Organization of Information Security*	• Access dari orang yang tidak berkepentingan • Pencurian Data • Data pada aplikasi hilang
A.7	*Asset Management*	• Adanya kerusakan Scan Kartu untuk masuk • Hilangnya Access Card • Adanya kerusakan Hardware • Lisensi Expired
A.8	*Human Resource Policy*	• Access dari orang yang tidak berkepentingan • Pencurian Data • Adanya kerusakan Scan Kartu untuk masuk • Database access hilang • Hilangnya Access Card • Data pada aplikasi hilang
A.9	*Physical and Environmental Security*	• Access dari orang yang tidak berkepentingan • Adanya kerusakan Scan Kartu untuk masuk • Hilangnya Access Card • Tidak mendapat daya listrik • Adanya kerusakan Hardware • Tidak terkoneksi dengan jaringan • Baterai tidak dapat menyimpan daya • AC tidak dingin • Data yang ditampilkan tidak sesuai (kalibrasi) • Gas Habis • Tidak terkoneksi dengan sensor
A.10	*Communications and Operations Management*	• Access dari orang yang tidak berkepentingan • Pencurian Data • Adanya kerusakan Scan Kartu untuk masuk • Hilangnya Access Card • Database access hilang • Terserang virus/malware • Tidak terkoneksi dengan jaringan • Kesalahan konfigurasi • Lisensi Expired • Baterai tidak dapat menyimpan daya • AC tidak dingin • Data yang ditampilkan tidak sesuai (kalibrasi) • Gas Habis • Tidak terkoneksi dengan sensor

		• Kapasitas melebihi batas / penuh • Kapasitas lisensi melebihi batas • Data pada aplikasi hilang • Aplikasi tidak bisa diakses • Kesalahan dalam input data • Data rusak • Service tidak berjalan • User tidak bisa melakukan otentikasi • User tidak bisa terkoneksi • User tidak mendapatkan IP Address
A.11	*Access Control*	• Access dari orang yang tidak berkepentingan • Pencurian Data • Database access hilang • Terserang virus/malware • Data pada aplikasi hilang • Data rusak
A.12	*Information System Acquisition Development and Maintenance*	• Kesalahan konfigurasi • Tidak kompatible dengan server
A.13	*Information Security Incident Management*	Semua Risiko

Dari table diatas, dapat terlihat bahwa pemilihan alternative kontrol akan mengacu pada klausa 5 hingga klausa 13 pada ISO 27001:2005. Pengecualian yang dilakukan pada klausa 14 *Business Continuity* dan klausa 15 *Compliance*. Pengecualian pada klausa 14 dikarenakan ruang lingkup hanya terkait keamanan di Data Center Divisi Teknologi Informasi PT PJB Services. Pengecualian kedua yang dilakukan pada klausa 15 dikarenakan saat ini belum ada persyaratan yang mengikat pada Divisi Teknologi Informasi PT PJB Services dalam menerapkan keamanan informasi tertentu.

Tahap selanjutnya adalah pemilihan kontrol yang akan diterapkan oleh Divisi Teknologi Informasi PT PJB Services. Proses penanganan risiko berada pada Lampiran G – Proses Penanganan Risiko, hasil detail dari kontrol yang dipilih beserta implementasinya yang direkomendasikan ada pada lampiran H – Pernyataan Pemberlakuan.

4.9 Verifikasi Penilaian Risiko dan Perencanaan Penanganan Risiko Berdasarkan ISO 27002 dan 27005

Verifikasi terhadap analisis penilaian risiko dan perencanaan penanganan risiko telah dilakukan dengan pemberian dokumen kepada masing-masing penanggung jawab terhadap asset informasi serta manajeman di Divisi Teknologi Informasi PT PJB Services untuk dilakukan revisi bilamana ada informasi yang tidak sesuai. Dalam penelitian ini, persetujuan terhadap Penilaian Risiko dan Perencanaan Penanganan Risiko dilakukan dengan penandatanganan dokumen oleh Manajer Divisi Teknologi Informasi.

4.10 Proses Rekomendasi Prioritas Kontrol Keamanan Informasi

Hasil dari penilaian risiko dan perencanaan penganganan risiko yang sudah diverifikasi akan dilakukan perhitungan dengan metode AHP-TOPSIS. Tujuan dari proses ini adalah dapat memberikan rekomendasi prioritas terhadap kontrol apa saja yang yang dilakukan. Perhitungan dengan metode AHP-TOPSIS ini mengambil inputan bobot dari metode AHP kemudian mendapatkan urutannya dengan metode TOPSIS. Adapun kriteria yang akan dijadikan sebagai pemilihan alternatif adalah dari penilaian risiko yaitu **Kemungkinan Terjadi (KT), Dampak Reputasi (R), Dampak Financial (F)** dan **Dampak Produktivitas (P)**.

Berikut ini adalah tahapan proses perhitungan metode *AHP* – TOPSIS utuk mendapatkan prioritas kontrol terhadap risiko-risiko yang telah diidentifikasi.

a. Menetapkan perbandingan berpasangan antara kriteria-kriteria dalam bentuk matriks.

   Nilai perbandingan berpasangan berdasarkan pembobotan dari masing-masing kriteria. Adapun tingkat perbandingan untuk setiap kriteria adalah sebagai berikut:

   - Kriteria KT sedikit lebih penting dari kriteria F dan P
   - Kriteria R lebih penting dari pada kriteria KT, F dan P. Kriteria R menjadi lebih penting dari pada kriteria lainnya dikarenakan PT PJB Services merupakan perusahaan jasa sehingga reputasi sangat penting sebagai *value* dari perusahaan.

- Kriteria F sama penting dengan kriteria P
- Kriteria P sama penting dengan kriteria F

Dari penjelasan diatas, dapat di buat Matriks Perbandingan Berpasangan seperti pada tabel 4.12.

Tabel 4.12 Matriks Perbandingan Berpasangan

	KT	R	F	P
KT	1.000	0.200	3.000	3.000
R	5.000	1.000	5.000	5.000
F	0.333	0.200	1.000	1.000
P	0.333	0.200	1.000	1.000

b. Normalisasi Matriks Perbandingan

Normalisasi matriks dilakukan dengan cara membagi setiap nilai dengan total nilai per kolom. Sebagai contoh, Jumlah kolom KT adalah 6,333. Maka untuk baris dan kolom pertama perhitungannya

N_{11} = 1/6,333 = 0,150.

Adapun hasil matriks perbandingan ditunjukkan pada Tabel 4.13.

Tabel 4.13 Normalisasi Matriks Perbandingan

	KT	R	F	P
KT	0.150	0.125	0.300	0.300
R	0.750	0.625	0.500	0.500
F	0.050	0.125	0.100	0.100
P	0.050	0.125	0.100	0.100

c. Nilai Bobot / *Eigen Vector*

Nilai Bobot / *eigen vector* didapatkan dengan cara menghitung rata-rata kriteria per baris. Hasil dari nilai bobot / *eigen vector* setiap kriteria adalah sebagai berikut

- Kemungkinan Terjadi (KT) : 0.21875
- Dampak reputasi (R) : 0.59375
- Dampak financial (F) : 0.09375

- Dampak produktivitas (P) : 0.09375

d. Konsistensi Bobot

Bobot yang telah didapatkan diuji konsistensinya dengan langkah berikut:

1. Menghitung nilai *eigen max (λmax)*

   Cara mendapatkan *λmax* adalah dengan mengkalikan nilai matriks perbandingan awal dengan bobot, kemudian hasil dari perkalian matriks tersebut bagi dengan bobot. Dari hasil pembagian tersebut jumlahkan setiap baris dan bagi dengan jumlah kriteria dalam hal ini nilainya 4 (empat).

   λmax = 16.62422723/4

   λmax = 4.156056809

2. Menghitung nilai *Consistency Index* (CI)

   CI = (*λmax*-*n*) / (n-1)

   CI = (4.156056809 - 4) / (4 - 1)

   CI = 0.052018936

3. Menghitung CR

   Berdasarkan dari table index random, untuk n = 4, maka RI = 0.9

   CR = CI/RI

   CR = 0.052018936 / 0.9

   CR = 0.057798818

Rasio konsistensi sebesar 0,026 kurang dari batas toleransi 0,1. Maka matriks perbandingan berpasangan dikatakan **konsisten**. Hal ini menunjukkan bahwa penilaian tidak perlu diperbaiki / diulang.

e. Data Daftar Risiko

Data daftar risiko yang akan diolah menggunakan TOPSIS adalah data dari kuesioner penilaian risiko yang telah dikonversi kemudian dikelompokkan berdasarkan nama risiko dengan menjumlahkan nilai pada tiap-tiap risiko berdasarkan nama risiko. Contohnya untuk risiko Service tidak berjalan memiliki kode risiko B44, B49 dan B53 dimana masing-masing memiliki nilai yang berbeda. Kemudian nilai tersebut dijumlahkan berdasarkan kriteria sehingga untuk risiko Service tidak berjalan memiliki nilai KT=1.7, R=0.25,

F=0.35, dan P=0.35. Untuk detail hasil dari pengelompokan risiko bisa dilihat pada tabel 4.14.

Tabel 4.14 Data Daftar Risiko

No	Risiko	KT	Dampak		
			R	F	P
1	AC tidak dingin	0.5	0.05	0.05	0.2
2	Access dari orang yang tidak berkepentingan	9.1	5.6	6.1	6.55
3	Adanya kerusakan Hardware	3.9	1.2	1.75	2.8
4	Adanya kerusakan Scan Kartu untuk masuk	0.1	0.05	0.05	0.05
5	Aplikasi tidak bisa diakses	6.1	3.9	3.75	4.25
6	Baterai tidak dapat menyimpan daya	0.3	0.1	0.1	0.1
7	Data pada aplikasi hilang	5.9	4.55	5.05	5.55
8	Data rusak	12	0.35	0.35	0.45
9	Data yang ditampilkan tidak sesuai (kalibrasi)	0.1	0.05	0.1	0.4
10	Database access hilang	0.1	0.05	0.05	0.05
11	Gas Habis	0.1	0.05	0.1	0.2
12	Hilangnya Access Card	0.3	0.05	0.05	0.05
13	Kapasitas lisensi melebihi batas	0.3	0.05	0.05	0.05
14	Kapasitas melebihi batas / penuh	2.5	0.65	0.85	1.7
15	Kesalahan dalam input data	5.6	3.05	3.6	4.5
16	Kesalahan konfigurasi	3.3	1	1.25	1.75
17	Lisensi expired	0.4	0.1	0.15	0.15
18	Pencurian Data	5.9	5.25	5.35	5.05
19	Service tidak berjalan	1.7	0.25	0.35	0.35
20	Terserang virus/malware	0.5	0.1	0.1	0.1
21	Tidak kompatible dengan server	0.1	0.05	0.05	0.2
22	Tidak mendapat daya listrik	5.2	1.15	1.3	2.95
23	Tidak terkoneksi dengan jaringan	1.1	0.3	0.35	0.75
24	Tidak terkoneksi dengan sensor	0.1	0.05	0.2	0.2
25	User tidak bisa melakukan otentikasi	0.5	0.1	0.1	0.1
26	User tidak bisa terkoneksi	0.7	0.05	0.1	0.05
27	User tidak mendapatkan IP Address	0.5	0.05	0.05	0.05

Pada tabel diatas, nilai pada setiap kriteria diambil dari penjumlahan dari setiap kriteria berdasarkan nama risiko yang ada.

f. Normalisasi matriks keputusan (R)

Cara menghitung matriks ternormalisasi (R) dengan membagi nilai pada setiap kolom dengan akar kuadrat dari total penjumlahan kuadrat total kolom setiap kriteria. Sebagai contoh untuk menemukan pembagi untuk kolom KT.

$\sqrt{0.5^2 + 9.1^2 + 3.9^2 + 0.1^2 + \ldots + 0.5^2}$ = 20.74777096

Maka untuk risiko AC tidak dingin pada kriteria KT maka nilai normalisasinya adalah 0.5 / 20.74777096 = 0.024098974

Berikut ini merupakan tabel hasil normalisasi matriks keputusan

Tabel 4. 15 Normalisasi Matriks Keputusan

No	**Risiko**	**KT**	**R**	**F**	**P**
1	AC tidak dingin	0.024098974	0.0048	0.00446	0.01574803
2	Access dari orang yang tidak berkepentingan	0.438601333	0.53721	0.54364	0.51574803
3	Adanya kerusakan Hardware	0.187972	0.11512	0.15596	0.22047244
4	Adanya kerusakan Scan Kartu untuk masuk	0.004819795	0.0048	0.00446	0.00393701
5	Aplikasi tidak bisa diakses	0.294007487	0.37413	0.33421	0.33464567
6	Baterai tidak dapat menyimpan daya	0.014459385	0.00959	0.00891	0.00787402
7	Data pada aplikasi hilang	0.284367897	0.43648	0.45006	0.43700787
8	Data rusak	0.578375384	0.03358	0.03119	0.03543307
9	Data yang ditampilkan tidak sesuai (kalibrasi)	0.004819795	0.0048	0.00891	0.03149606
10	Database access hilang	0.004819795	0.0048	0.00446	0.00393701
11	Gas Habis	0.004819795	0.0048	0.00891	0.01574803
12	Hilangnya Access Card	0.014459385	0.0048	0.00446	0.00393701
13	Kapasitas lisensi melebihi batas	0.014459385	0.0048	0.00446	0.00393701
14	Kapasitas melebihi batas / penuh	0.120494872	0.06235	0.07575	0.13385827
15	Kesalahan dalam input data	0.269908513	0.29259	0.32084	0.35433071
16	Kesalahan konfigurasi	0.159053231	0.09593	0.1114	0.13779528
17	Lisensi expired	0.019279179	0.00959	0.01337	0.01181102
18	Pencurian Data	0.284367897	0.50363	0.4768	0.3976378
19	Service tidak berjalan	0.081936513	0.02398	0.03119	0.02755906

20	Terserang virus/malware	0.024098974	0.00959	0.00891	0.00787402
21	Tidak kompatible dengan server	0.004819795	0.0048	0.00446	0.01574803
22	Tidak mendapat daya listrik	0.250629333	0.11032	0.11586	0.23228346
23	Tidak terkoneksi dengan jaringan	0.053017744	0.02878	0.03119	0.05905512
24	Tidak terkoneksi dengan sensor	0.004819795	0.0048	0.01782	0.01574803
25	User tidak bisa melakukan otentikasi	0.024098974	0.00959	0.00891	0.00787402
26	User tidak bisa terkoneksi	0.033738564	0.0048	0.00891	0.00393701
27	User tidak mendapatkan IP Address	0.024098974	0.0048	0.00446	0.00393701

g. Matriks normalisasi terbobot

Menentukan matriks normalisasi terbobot dengan cara mengalikan setiap elemen pada matriks ternormalisasi dengan bobot yang diperoleh pada proses AHP. Sebagai contoh perhitungan, pada risiko AC tidak dingin pada kriteria KT, maka nilai normalisasi terbobotnya 0.024098974x0.21875 = 0.005271651 Berikut ini adalah tabel hasil matriks normalisasi terbobot

Tabel 4. 16 Matriks Normalisasi Terbobot

No	Risiko	KT	R	F	P
1	AC tidak dingin	0.005271651	0.00285	0.00042	0.00147638
2	Access dari orang yang tidak berkepentingan	0.095944042	0.31897	0.05097	0.04835138
3	Adanya kerusakan Hardware	0.041118875	0.06835	0.01462	0.02066929
4	Adanya kerusakan Scan Kartu untuk masuk	0.00105433	0.00285	0.00042	0.00036909
5	Aplikasi tidak bisa diakses	0.064314138	0.22214	0.03133	0.03137303
6	Baterai tidak dapat menyimpan daya	0.00316299	0.0057	0.00084	0.00073819
7	Data pada aplikasi hilang	0.062205478	0.25916	0.04219	0.04096949
8	Data rusak	0.126519615	0.01994	0.00292	0.00332185
9	Data yang ditampilkan tidak sesuai (kalibrasi)	0.00105433	0.00285	0.00084	0.00295276
10	Database access hilang	0.00105433	0.00285	0.00042	0.00036909
11	Gas Habis	0.00105433	0.00285	0.00084	0.00147638

12	Hilangnya Access Card	0.00316299	0.00285	0.00042	0.00036909
13	Kapasitas lisensi melebihi batas	0.00316299	0.00285	0.00042	0.00036909
14	Kapasitas melebihi batas / penuh	0.026358253	0.03702	0.0071	0.01254921
15	Kesalahan dalam input data	0.059042487	0.17372	0.03008	0.0332185
16	Kesalahan konfigurasi	0.034792894	0.05696	0.01044	0.01291831
17	Lisensi expired	0.004217321	0.0057	0.00125	0.00110728
18	Pencurian Data	0.062205478	0.29903	0.0447	0.03727854
19	Service tidak berjalan	0.017923612	0.01424	0.00292	0.00258366
20	Terserang virus/malware	0.005271651	0.0057	0.00084	0.00073819
21	Tidak kompatible dengan server	0.00105433	0.00285	0.00042	0.00147638
22	Tidak mendapat daya listrik	0.054825167	0.0655	0.01086	0.02177657
23	Tidak terkoneksi dengan jaringan	0.011597631	0.01709	0.00292	0.00553642
24	Tidak terkoneksi dengan sensor	0.00105433	0.00285	0.00167	0.00147638
25	User tidak bisa melakukan otentikasi	0.005271651	0.0057	0.00084	0.00073819
26	User tidak bisa terkoneksi	0.007380311	0.00285	0.00084	0.00036909
27	User tidak mendapatkan IP Address	0.005271651	0.00285	0.00042	0.00036909

h. Menentukan Solusi Ideal Positif (A+) dan Solusi Ideal Negatif (A-)

Tahap ini adalah mencari nilai minimum dan maksimun dari setiap kriteri yang ditunjukkan pada Tabel 4.16

Tabel 4. 17 Solusi Ideal Positif dan Solusi Ideal Negatif

	KT	**R**	**F**	**P**
A+	0.126519615	0.318968	0.050966	0.048351378
A-	0.00105433	0.002848	0.000418	0.000369094

i. Menghitung *separation measure* (D)

Merupakan pengukuran jarak dari suatu alternatif ke solusi ideal positif (D+) dan solusi ideal negative (D-).

Separation measure untuk solusi ideal positif

$$D_1^+ = \sqrt{\sum_{j=1}^{n}(v_{ij} - v_{j1}^+)^2} \text{ , dengan } i = 1,2,3,\ldots,n \qquad (4.1)$$

Separation measure untuk solusi ideal negatif

$$D_1^- = \sqrt{\sum_{j=1}^{n}(v_{ij} - v_{j1}^-)^2}$$, dengan i = 1,2,3,…,n (4.2)

Berikut ini adalah hasil perhitungan reparation measure

Tabel 4.18 Separation Measure

No	Risiko	D+	D-
1	AC tidak dingin	0.345521718	0.00436
2	Access dari orang yang tidak berkepentingan	0.030575574	0.33733
3	Adanya kerusakan Hardware	0.268681382	0.08068
4	Adanya kerusakan Scan Kartu untuk masuk	0.347175403	0
5	Aplikasi tidak bisa diakses	0.117979895	0.23239
6	Baterai tidak dapat menyimpan daya	0.343709579	0.00359
7	Data pada aplikasi hilang	0.088569616	0.26987
8	Data rusak	0.306196033	0.12668
9	Data yang ditampilkan tidak sesuai (kalibrasi)	0.346767121	0.00262
10	Database access hilang	0.347175403	0
11	Gas Habis	0.346963495	0.00118
12	Hilangnya Access Card	0.346418936	0.00211
13	Kapasitas lisensi melebihi batas	0.346418936	0.00211
14	Kapasitas melebihi batas / penuh	0.304517684	0.04474
15	Kesalahan dalam input data	0.162217025	0.1858
16	Kesalahan konfigurasi	0.282772359	0.06576
17	Lisensi expired	0.343220843	0.0044
18	Pencurian Data	0.068524498	0.30788
19	Service tidak berjalan	0.330234854	0.02063
20	Terserang virus/malware	0.342958433	0.00512
21	Tidak kompatible dengan server	0.3470241	0.00111
22	Tidak mendapat daya listrik	0.267767516	0.08593
23	Tidak terkoneksi dengan jaringan	0.329362855	0.01863
24	Tidak terkoneksi dengan sensor	0.346843761	0.00167
25	User tidak bisa melakukan otentikasi	0.342958433	0.00512
26	User tidak bisa terkoneksi	0.344878727	0.00634
27	User tidak mendapatkan IP Address	0.345673678	0.00422

j. Menghitung Kedekatan Relatif dengan Solusi Ideal Positif (V)

Cara menghitung kedekatan relatif dengan solusi ideal positif (V) adalah membagi antara solusi ideal negatif (D-) dengan penjumlahan antara solusi ideal negatif (D-) dengan positif (D+).

$V_i = \frac{D_1^-}{D_1^- + D_1^+}$, dengan $0 < Vi < 1$ dan $i = 1,2,3,\ldots,m$ (4.3)

Sebagai contoh untuk $V_{AC\ tidak\ dingin}$ = 0.00436 / (0.00436+0.345521718) = 0.012462089

Berikut ini adalah hasil perhitungan kedekatan relative dengan solusi iseal positif

Tabel 4.19 Kedekatan Relatif dengan Solusi Ideal Positif

No	Risiko	V
1	AC tidak dingin	0.012462089
2	Access dari orang yang tidak berkepentingan	0.916893463
3	Adanya kerusakan Hardware	0.230939784
4	Adanya kerusakan Scan Kartu untuk masuk	0
5	Aplikasi tidak bisa diakses	0.66327432
6	Baterai tidak dapat menyimpan daya	0.010328871
7	Data pada aplikasi hilang	0.752902018
8	Data rusak	0.29265182
9	Data yang ditampilkan tidak sesuai (kalibrasi)	0.007490941
10	Database access hilang	0
11	Gas Habis	0.003399336
12	Hilangnya Access Card	0.006050196
13	Kapasitas lisensi melebihi batas	0.006050196
14	Kapasitas melebihi batas / penuh	0.128088886
15	Kesalahan dalam input data	0.5338758
16	Kesalahan konfigurasi	0.188674718
17	Lisensi expired	0.012656888
18	Pencurian Data	0.817948093
19	Service tidak berjalan	0.058793265
20	Terserang virus/malware	0.014707346
21	Tidak kompatible dengan server	0.003180648
22	Tidak mendapat daya listrik	0.242951016
23	Tidak terkoneksi dengan jaringan	0.053523568
24	Tidak terkoneksi dengan sensor	0.004798498

25	User tidak bisa melakukan otentikasi	0.014707346
26	User tidak bisa terkoneksi	0.018050758
27	User tidak mendapatkan IP Address	0.012053241

k. Mengurutkan Pilihan Alternatif

Alternatif dapat dirangking berdasarkan hasil perhitungan V pada tahap sebelumnya. Perangkingan dengan cara mengurutkan hasil V dari yang terbesar ke terkecil. Berikut ini hasil perangkingan alternatif yang telah dilakukan.

Tabel 4. 20 Hasil Pengurutan Pilihan Alternatif

No	Risiko	V
1	Access dari orang yang tidak berkepentingan	0.916893463
2	Pencurian Data	0.817948093
3	Data pada aplikasi hilang	0.752902018
4	Aplikasi tidak bisa diakses	0.66327432
5	Kesalahan dalam input data	0.5338758
6	Data rusak	0.29265182
7	Tidak mendapat daya listrik	0.242951016
8	Adanya kerusakan Hardware	0.230939784
9	Kesalahan konfigurasi	0.188674718
10	Kapasitas melebihi batas / penuh	0.128088886
11	Service tidak berjalan	0.058793265
12	Tidak terkoneksi dengan jaringan	0.053523568
13	User tidak bisa terkoneksi	0.018050758
14	Terserang virus/malware	0.014707346
15	User tidak bisa melakukan otentikasi	0.014707346
16	Lisensi expired	0.012656888
17	AC tidak dingin	0.012462089
18	User tidak mendapatkan IP Address	0.012053241
19	Baterai tidak dapat menyimpan daya	0.010328871
20	Data yang ditampilkan tidak sesuai (kalibrasi)	0.007490941
21	Hilangnya Access Card	0.006050196
22	Kapasitas lisensi melebihi batas	0.006050196
23	Tidak terkoneksi dengan sensor	0.004798498
24	Gas Habis	0.003399336
25	Tidak kompatible dengan server	0.003180648
26	Adanya kerusakan Scan Kartu untuk masuk	0
27	Database access hilang	0

Adapun contoh kesimpulan yang dapat diambil dari hasil perangkingan diatas adalah bahwa kontrol yang yang harus didahulukan adalah yang berhubungan dengan “Access dari orang yang tidak berkepentingan”.

4.11 Penyusunan dan Pemberian Rekomendasi

Tahap terakhir yaitu penyususnan dan pemberian rekomendasi berdasarkan tahapan sebelumnya. Kontrol keamanan informasi yang harus dilakukan terlebih dahulu berdasarkan urutan dari risiko yang harus diminimalisir atau diselesaikan pada tahap sebelumnya. Berikut ini kontrol keamanan informasi yang telah disesuaikan dengan perangkingan adalah sebagai berikut:

Tabel 4. 21 Urutan Rekomendasi Kontrol

No	Kontrol
A.5	*Security Policy*
A.6	*Organization of Information Security*
A.8	*Human Resource Policy*
A.9	*Physical and Environmental Security*
A.10	*Communications and Operations Management*
A.11	*Access Control*
A.13	*Information Security Incident Management*
A.7	*Asset Management*
A.12	*Information System Acquisition Development and Maintenance*

Adapun detail lengkap pemberian rekomendasi ada pada Lampiran I – Rekomendasi Sistem Manajemen Keamanan Informasi.

(Halaman ini sengaja dikosongkan)

BAB 5
KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan yang didapatkan dalam penelitian ini, serta saran yang bisa dikembangkan untuk penyempurnaan dari penelitian ini.

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian thesis perancangan sistem manajemen keamanan informasi ini adalah sebagai berikut :

1. Aset-aset informasi Divisi Teknologi Informasi PT PJB Services yang diidentifikasi melaui penelitian ini berjumlah 45 (empat puluh lima) yang terdiri dari 9 (sembilan) aset informasi dimiliki oleh Bagian *Data Center & Storage*, 11 (sebelas) asset informasi dimiliki oleh Bagian *Network & Security*, 10 (sepuluh) asset informasi dimiliki oleh Bagian *Core Businees Application*, 3 (tiga) asset informasi dimiliki oleh Bagian *Enterprise Asset Management (EAM) Application*, dan 12 (dua belas) asset informasi dimiliki oleh Bagian *Supporting Application*.
2. Risiko-risiko terkait asset informasi yang telah diidentifikasi melaui penelitian ini berjumlah 224 (dua ratus dua puluh empat) risiko yang terdiri dari 45 (empat puluh lima) risiko dimiliki oleh Bagian *Data Center & Storage*, 54 (lima puluh empat) risiko dimiliki oleh Bagian *Network & Security*, 50 (lima puluh) risiko dimiliki oleh Bagian *Core Businees Application*, 15 (lima belas) risiko dimiliki oleh Bagian *Enterprise Asset Management (EAM) Application*, dan 60 (enam puluh) risiko dimiliki oleh Bagian *Supporting Application*. Risiko yang terdapat pada semua Bagian Divisi Teknologi Informasi PT PJB Services adalah Access dari orang yang tidak berkepentingan.
3. Urutan implementasi kontrol yang direkomendasikan sesuai dari hasil penelitian ini adalah *Security Policy, Organization of Information Security, Human Resource Policy, Phy sical and Environmental Security, Communications and Operations Management, Access Control, Information*

Security Incident Management, Asset Management, Information System Acquisition Development and Maintenance

4. Terdapat 3 (tiga) proses utama dalam penelitian ini. Pertama, melakukan assessment untuk menentukan kontrol yang sesuai terhadap risiko – risiko yang dimiliki oleh masing-masing aset berdasarkan ISO 27001:2005. Kedua, melakukan proses pengurutan prioritas kontrol apa saja yang harus dilakukan terlebih dahulu menggunakan metode AHP-TOPSIS. Terakhir, penyusunan dokumen terkait rekomendasi Sistem Manajemen Keamanan Informasi dalam bentuk Pernyataan Pemberlakuan

5.2 Saran

Berikut ini adalah saran setelah penelitian thesis perancangan sistem manajemen keamanan informasi ini:

1. Penelitian selanjutnya diharapakan melakukan assessment secara konferehensif atau dilakukan terhadap seluruh asset informasi yang dimiliki oleh Perusahaan agar semua risiko dapat diidentifikasi dan diberikan kontrol yang sesui dengan kondisi perusahaan.
2. Penelitian selanjutnya diharapkan identifikasi risiko dapat dijabarkan lebih detail agar kontrol beserta rekomendasi implementasi yang diberikan dapat lebih spesifik. Dalam penelitian ini identifikasi risiko dijabarkan secara umum dikarenakan kebijakan internal Divisi Teknologi Informasi PT PJB Services.
3. Penelitian selanjutnya diharapkan dapat menggunakan metode SPK lain dalam proses perangkingan kontrol serta membandingkannya, hal ini bertujuan agar dapat mengetahui kelebihan dan kekurangan masing-masing SPK jika diterapkan dalam perangkingan rekomendasi kontrol risiko.
4. Sebagai perusahaan yang bergerak di bidang jasa dengan menggunakan Teknologi Informasi. Maka PT PJB Services harus memiliki suatu framework berupa Sistem Manajemen Keamanan Informasi (SMKI) yang digunakan sebagai acuan dalam melakukan mengimplementasi, mengoperasikan, memantau, mengkaji, menjaga dan meningkatkan keamanan informasi agar proses bisnis tetap berjalan sesuai dengan visi misi perusahaan.

DAFTAR PUSTAKA

Purnomo, Eka Pramudita. (2017). *Perancangan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001 (Studi Kasus: PT SENTRA VIDYA UTAMA).*Surabaya: Institut Teknologi Sepuluh Nopember.

Purnomo, Estining Nur Sejati, Sari Widya Sihwi, Rini Anggrainingsih. (2013). *Analisis Perbandingan Menggunakan Metode AHP, TOPSIS, dan AHP-TOPSIS dalam Studi Kasus Sistem Pendukung Keputusan Penerimaan Siswa Program Akselerasi*. Surakarta: Universitas Negeri Sebelas Maret.

Juliyanti, Mohammad Isa Irawan, Imam Mukhlash. (2011). *Pemilihan Guru Berprestasi Menggunakan Metode AHP dan TOPSIS*. Prosiding Seminar Nasional Penelitian, Pendidikan dan Penerapan MIPA. Universitas Negeri Yogyakarta.

Aginsa, Andre, Ian Yosef Matheus Edward, Wervyan Shalannanda. (2016). Enhanced Information Security Management System Framework Design Using ISO 27001 And Zachman Framework A Study Case of XYZ Company. *IEEE*, 62-66.

Manurung, Pangeran. (2010). *Sistem Pendukung Keputusan Seleksi Penerima Beasiswa Dengan Metode AHP dan TOPSIS (Studi Kasus: FMIPA USU)*. Medan: Universitas Sumatera Utara.

PT PJB Services. (2016). *SK DIREKSI PT PJB Services Nomor: 136.K/010/DIR-PJBS/2017*. Sidoarjo: PT PJB Services

Kamus Besar Bahasa Indonesia (KBBI), (2017), https://kbbi.web.id/informasi.

Annual Report PT PJB Services. (2016). *Sustainable Performance for The Best O&M Company*. Sidoarjo: PT PJB SERVICES

ISO/IEC. (2009). *ISO/IEC 27000 - Information technology — Security Techniques - Information security management systems - Overview and vocabulary*. Switzerland: ISO/IEC.

Badan Standarisasi Nasional. (2009). *ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirement*. Jakarta: BSN.

Badan Standarisasi Nasional. (2014). *ISO/IEC 27002:2014 - Information Security - Security Techniques - Code of Practice for Information Security Controls*. Jakarta: BSN.

ISO/IEC. (2010). *ISO/IEC 27003:2010 - Information Technology - Security Techniques - Information Security Management System Implementation Guidance*. Switzerland: ISO/IEC.

ISO/IEC, (2011). *ISO/IEC 27005:2011 - Information Technology - Security Technique - Information Security Risk Management*. Switzerland: ISO/IEC.

Jogiyanto. (2003:34). *Analisis dan Desain Sistem Informasi*. Bandung: Penerbit Informatika

Williams dan Sawyer. (2003). *Using Information Technology: A Practical Introduction to Computers and Communications*. London: Career Education.

O'Brien dan Marakas, (2010). *Management System Information*. New York.

HM, Jogiyanto. (1999). *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*. ANDI Yogyakarta: Yogyakarta.

Peltier, T. R. (2014). *Information Security Fundamentals*. Boca Raton: CRC PRess.

Turban, E dan Jay E. (2001). *Decision Support Systems and Intelligent Systems*. Upper Saddle River: Prentice Hall.

Sprague, Jr., Ralph H., dan Hugh J. Watson. 1996. *Decision Support for Management*. Upper Saddle River: Prentice Hall.

Marimin. (2004).*Teknik dan Aplikasi Pengambil Keputusan Kriteria Majemuk*. Jakarta: PT.Gramedia Widiasarana Indonesia

Kusrini. (2007). *Konsep dan Aplikasi Sistem Pendukung Keputusan*. Yogyakarta: Penerbit Andi

Tzeng, G., & Huang, J. (2011). *Multiple Atribut Decision Making: Methods and Applications*.Florida: CRC Press.

LAMPIRAN A

Dokumen Ruang Lingkup SMKI

PT PJB Services

Ruang Lingkup Sistem Manajemen Keamanan Informasi (SMKI)

Nama Dokumen : Dokumen Ruang Lingkup SMKI
Versi : 1
Tanggal : 18 Juni 2018

1. Tujuan

Tujuan dari dokumen ini adalah untuk memberikan penjelasan mengenai lingkup dan batasan *assessment* untuk pembuatan rekomendasi Sistem Manajemen Keamanan Informasi (SMKI) pada PT PJB Services

2. Ruang Lingkup SMKI

Ruang Lingkup SMKI ditetapkan sebagai berikut:

2.1 Karakteristik Bisnis

Berikut ini adalah karakteristik bisnis PT PJB Services

a. PT PJB Services merupakan perusahaan yang berkecimpung dalam jasa operasi dan pemeliharaan pembangkit listrik.
b. Layanan atau produk utama dari PT PJB Services antara lain O&M Power Plant, O&M Balance Of Plant, O&M Coal And Ash Handling Plant, Routine Maintenance, HSE Management, Setup Management, Overhaul Power Plant, dan Project Services
c. Karyawan PT PJB Services mencapai lebih dari 3600 orang yang tersebar di seluruh unit kerja di seluruh Indonesia.

2.2 Bagian/Unit Organisasi

Ruang lingkup *assessment* untuk pembuatan rekomendasi Sistem Manajemen Keamanan Informasi pada PT PJB Services mencakup seluruh asset baik hardware maupun aplikasi

production yang berada di Data Center Divisi Teknologi Informasi PT PJB Services meliputi bagian – bagian sebagai berikut:

a. Bagian *Data Center & Storage*
b. Bagian *Network & Security*
c. Bagian *Core Business Application*
d. Bagian *Enterprise Asset Management (EAM) Application*
e. Bagian *Supporting Application*

3. Lokasi

Lokasi penerapan SMKI terletak di Jalan Raya Juanda No 17, Sidoarjo, Jawa Timur Indonesia

4. Komitmen dan Sumber Daya

Manajemen Divisi Teknologi Informasi PT PJB Services berkomitmen dan mendukung *assessment* untuk pembuatan rekomendasi Sistem Manajemen Keamanan Informasi (SMKI). Dukungan dapat berupa dukungan keuangan, tambahan sumber daya manusia atau sumber daya lainnya yang dibutuhkan menyesuaikan antara kebutuhan dan kemampuan Divisi Teknologi Informasi PT PJB Services dalam menerapkannya.

5. Pengecualian

Disaster Recovery Center milik Divisi Teknologi Informasi PT PJB Services yang berlokasi di Jakarta, unit-unit dari PT PJB Services dan Aplikasi yang masih berstatus pengembangan.

Menyetujui,
Manajer Divisi Teknologi Informasi

Habib Amaluddin Mahfudz
NIP : 8308132JA

(Halaman ini sengaja dikosongkan)

LAMPIRAN B

Kebijakan Sistem Manajemen Keamanan Informasi

PT PJB Services

Kebijakan Sistem Manajemen Keamanan Informasi (SMKI)

Nama Dokumen : Kebijakan Sistem Manajemen Keamanan Informasi
Versi : 1
Tanggal : 18 Juni 2018

1. Pendahuluan

Kebijakan Sistem Manajemen Keamanan Informasi (SMKI) adalah untuk menunjang tujuan bisnis, dengan memastikan kerahasiaan, integritas dan kesediaan dari asset-aset informasi yang penting pada organisasi

2. Ruang Lingkup SMKI

Ruang lingkup *assessment* untuk pembuatan rekomendasi Sistem Manajemen Keamanan Informasi pada PT PJB Services mencakup seluruh asset baik hardware maupun aplikasi *production* yang berada di Data Center Divisi Teknologi Informasi PT PJB Services meliputi bagian – bagian sebagai berikut:

a. Bagian *Data Center & Storage*
b. Bagian *Network & Security*
c. Bagian *Core Business Application*
d. Bagian *Enterprise Asset Management (EAM) Application*
e. Bagian *Supporting Application*

3. Tujuan

Tujuan utama dari *assessment* untuk pembuatan rekomendasi SMKI ini adalah untuk mengetahui risiko-risiko beserta kontrol prosedur apa yang harus dilakukan untuk meminimalisasi risiko terkait keamanan informasi dan sekaligus sebagai bahan masukan jika perusahaan akan mengimplementasikan SMKI.

4. Hasil Yang Diharapkan

Hasil yang diharapkan melalui *assessment* ini adalah dokumen daftar risiko beserta kontrolnya sesuai dengan kondisi perusahaan.

5. Tanggung Jawab

Tanggung jawab pada Sistem Manajemen Keamanan Informasi di Divisi Teknologi Informasi PT PJB Services dibagi pada 3 (tiga) peran yaitu manajer sebagai penanggung jawab utama, asisten manajer sebagai penanggung jawab pelaksana SMKI, dan masing-masing pemilik aset informasi sebagai pelaksana perlindungan terhadap aset informasinya.

6. Kebijakan Terkait

Saat ini belum ada kebijakan terkait yang di dokumentasikan.

Menyetujui,

Manajer Divisi Teknologi Informasi

Habib Amaluddin Mahfudz

NIP : 8308132JA

(Halaman ini sengaja dikosongkan)

LAMPIRAN C

Kuesioner Identifikasi Aset dan Risiko

PT PJB Services

Kuesioner Identifikasi Aset dan Risiko

Bagian : Core Business Application
Surveyor : Purnomo Dwi D
Nama Responden : M. Rendra Suryadi
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 20 Juni 2018

1. Apa saja asset informasi yang harus dijaga pada bagian saudara/ri serta langkah apa saja pengamanan yang sudah diterapkan untuk menjaga asset informasi tersebut?

No	Nama	Langkah Pengamanan	Keterangan
1	Aplikasi Pengelolaan Pelanggan	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
2	Aplikasi Monitoring Proyek	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
3	Aplikasi SDM	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
4	Aplikasi Knowledge Management	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
5	Aplikasi Forum Diskusi Karyawan	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
6	Aplikasi Audit Internal	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-

7	Aplikasi Recruitment	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
8	Aplikasi Presensi	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
9	Aplikasi Keuangan	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
10	Aplikasi Penilaian Kinerja Karyawan	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-

2. Selain bagian / divisi ini siapa yang dapat mengakses asset informasi ini?

Tidak ada, bagian/divisi lain bisa mengakses asset informasi jika mendapat persetujuan dari Manajeman Divisi Teknologi Informasi (Asisten Manajer atau Manajer) dan pendampingan dari bagian *Core Business Application*.

3. Apa saja insiden keamanan informasi yang pernah terjadi dan membuat asset informasi tersebut berubah, rusak, tidak dapat diakses atau diakses oleh pihak yang tidak berkepentingan?

Penah terjadi kapasitas storage melebihi daya tampungnya sehingga menyebabkan aplikasi tidak bisa diakses.

4. Bagaimana prosedur atau tindakan ketika salah satu anggota bagian dipindah atau dikeluarkan?

Manajemen akan menunjuk staff baru untuk dilakukan transfer knowledge dari staff lama kemuadian akan dilakukan penghapusan akses terhadap asset informasi yang dimiliki oleh staff lama serta semua fasilitas kerja yang melekat pada staff lama akan ditarik seperti laptop.

5. Apa ada sosialisasi berkala dari IT atau semacamnya terkait kemanan informasi?

Sangat jarang, tidak ada sosialisasi berkala

6. Catatan atau Keterangan Lain

Tidak ada

Surveyor

Purnomo Dwi D

Responden

M. Rendra Suryadi

(NIP. 9014140KP)

PT PJB Services

Kuesioner Identifikasi Aset dan Risiko

Bagian : Data Center & Storage
Surveyor : Purnomo Dwi D
Nama Responden : Bagus Dahono Putro
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 20 Juni 2018

1. Apa saja asset informasi yang harus dijaga pada bagian saudara/ri serta langkah apa saja pengamanan yang sudah diterapkan untuk menjaga asset informasi tersebut?

No	Nama	Langkah Pengamanan	Keterangan
1	Access Data Center	Membuat suatu access card untuk user tertentu	-
2	Server Aplikasi	Mengimplementasikan monitoring sistem untuk melihat kondisi perangkat server serta melakukan maintenance rutin	-
3	Virtualisasi Server	Melakukan update dan monitoring	-
4	Storage	Mengimplementasikan monitoring sistem untuk melihat kondisi perangkat server serta melakukan maintenance rutin	-
5	Media Backup	Mengimplementasikan monitoring sistem untuk melihat kondisi perangkat server serta melakukan maintenance rutin	-
6	UPS Data Center	Melakukan maintenance rutin setiap tahun	-
7	Precision AC	Melakukan maintenance rutin setiap tahun	-
8	Monitoring Kelembapan dan Suhu	Melakukan maintenance rutin setiap tahun	-
9	Fire Protection	Melakukan maintenance rutin setiap tahun	-

2. Selain bagian / divisi ini siapa yang dapat mengakses asset informasi ini?

Tidak ada, bagian/divisi lain bisa mengakses asset informasi jika mendapat persetujuan dari Manajeman Divisi Teknologi Informasi (Asisten Manajer atau Manajer) dan pendampingan dari bagian *Data Center* dan *Storage*.

3. Apa saja insiden keamanan informasi yang pernah terjadi dan membuat asset informasi tersebut berubah, rusak, tidak dapat diakses atau diakses oleh pihak yang tidak berkepentingan?

- Penah terjadi kapasitas storage melebihi daya tampungnya sehingga menyebabkan banyak aplikasi yang menggunakan storage tersebut tidak dapat diakses.
- Ada merk dari server yang sering mengalami gangguan pada perangkat
- Ada server dan storage yang tidak bisa melakukan sinkronisasi dengan VMWare dikarenakan versi VMWare tersebut sudah lama

4. Bagaimana prosedur atau tindakan ketika salah satu anggota bagian dipindah atau dikeluarkan?

Manajemen akan menunjuk staff baru untuk dilakukan transfer knowledge dari staff lama kemuadian akan dilakukan penghapusan akses terhadap asset informasi yang dimiliki oleh staff lama serta semua fasilitas kerja yang melekat pada staff lama akan ditarik seperti laptop.

5. Apa ada sosialisasi berkala dari IT atau semacamnya terkait kemanan informasi?

Sangat jarang, tidak ada sosialisasi berkala

6. Catatan atau Keterangan Lain

Tidak ada

Surveyor	Responden
Purnomo Dwi D	Bagus Dahono Putro
	(NIP. 9414120KP)

PT PJB Services

Kuesioner Identifikasi Aset dan Risiko

Bagian : Enterprise Asset Management (EAM) Application
Surveyor : Purnomo Dwi D
Nama Responden : Slamet Fajar Suryadi
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 20 Juni 2018

1. Apa saja asset informasi yang harus dijaga pada bagian saudara/ri serta langkah apa saja pengamanan yang sudah diterapkan untuk menjaga asset informasi tersebut?

No	Nama	Langkah Pengamanan	Keterangan
1	Aplikasi Manajemen Asset Pembangkit	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
2	Aplikasi LK3	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
3	Aplikasi Dashboard Pembangkit	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-

2. Selain bagian / divisi ini siapa yang dapat mengakses asset informasi ini?

Tidak ada, bagian/divisi lain bisa mengakses asset informasi jika mendapat persetujuan dari Manajeman Divisi Teknologi Informasi (Asisten Manajer atau Manajer) dan pendampingan dari bagian Enterprise Asset Management (EAM) Application.

3. **Apa saja insiden keamanan informasi yang pernah terjadi dan membuat asset informasi tersebut berubah, rusak, tidak dapat diakses atau diakses oleh pihak yang tidak berkepentingan?**

Penah terjadi kapasitas storage melebihi daya tampungnya sehingga menyebabkan aplikasi tidak bisa diakses.

4. **Bagaimana prosedur atau tindakan ketika salah satu anggota bagian dipindah atau dikeluarkan?**

Manajemen akan menunjuk staff baru untuk dilakukan transfer knowledge dari staff lama kemuadian akan dilakukan penghapusan akses terhadap asset informasi yang dimiliki oleh staff lama serta semua fasilitas kerja yang melekat pada staff lama akan ditarik seperti laptop.

5. **Apa ada sosialisasi berkala dari IT atau semacamnya terkait kemanan informasi?**

Sangat jarang, tidak ada sosialisasi berkala

6. **Catatan atau Keterangan Lain**

Tidak ada

Surveyor	Responden
Purnomo Dwi D	Slamet Fajar Suryadi
	(NIP. 9514119KP)

6	Access Switch	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
7	Load Balancer	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
8	Access Point	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
9	DNS	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
10	DHCP Server	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
11	Active Directory	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-

2. Selain bagian / divisi ini siapa yang dapat mengakses asset informasi ini?

Tidak ada, bagian/divisi lain bisa mengakses asset informasi jika mendapat persetujuan dari Manajeman Divisi Teknologi Informasi (Asisten Manajer atau Manajer) dan pendampingan dari bagian Network & Security.

3. Apa saja insiden keamanan informasi yang pernah terjadi dan membuat asset informasi tersebut berubah, rusak, tidak dapat diakses atau diakses oleh pihak yang tidak berkepentingan?

- Penah terjadi kapasitas storage melebihi daya tampungnya sehingga menyebabkan server yang berhubungan dengan Network tidak bisa diakses seperti DNS Server dan Active Directory.
- Data user di active directory tidak terupdate sehingga user ada yang tidak bisa login ke aplikasi maupun internet
- Koneksi internetdan akses ke aplikasi internal lambat

PT PJB Services

Kuesioner Identifikasi Aset dan Risiko

Bagian : Network & Security
Surveyor : Purnomo Dwi D
Nama Responden : Rahmat Sudrajat
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 20 Juni 2018

1. Apa saja asset informasi yang harus dijaga pada bagian saudara/ri serta langkah apa saja pengamanan yang sudah diterapkan untuk menjaga asset informasi tersebut?

No	Nama	Langkah Pengamanan	Keterangan
1	Router Agregator	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
2	Firewall Server Farm	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
3	Proxy Internet	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
4	Endpoint Protection	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-
5	Core Switch	Hanya user yang berwenang yang memiliki akses untuk masuk ke perangkat Monitoring kondisi perangkat lewat aplikasi monitoring Melakukan backup konfigurasi perangkat	-

- Router Agregator tidak bisa diakses

4. Bagaimana prosedur atau tindakan ketika salah satu anggota bagian dipindah atau dikeluarkan?

Manajemen akan menunjuk staff baru untuk dilakukan transfer knowledge dari staff lama kemuadian akan dilakukan penghapusan akses terhadap asset informasi yang dimiliki oleh staff lama serta semua fasilitas kerja yang melekat pada staff lama akan ditarik seperti laptop.

5. Apa ada sosialisasi berkala dari IT atau semacamnya terkait kemanan informasi?

Sangat jarang, tidak ada sosialisasi berkala

6. Catatan atau Keterangan Lain

Tidak ada

Surveyor

Purnomo Dwi D

Responden

Rahmat Sudrajat

(NIP. 8714142KP)

PT PJB Services

Kuesioner Identifikasi Aset dan Risiko

Bagian : Supporting Application
Surveyor : Purnomo Dwi D
Nama Responden : Roynther Ayub Djami
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 20 Juni 2018

1. Apa saja asset informasi yang harus dijaga pada bagian saudara/ri serta langkah apa saja pengamanan yang sudah diterapkan untuk menjaga asset informasi tersebut?

No	Nama	Langkah Pengamanan	Keterangan
1	Aplikasi Helpdesk IT	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
2	Aplikasi Dokumen Center	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
3	Aplikasi Event	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
4	Aplikasi Manajemen Resiko	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
5	Aplikasi Inventaris	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
6	Aplikasi Good Corporate Governance	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-

7	Aplikasi Pemesanan Kendaraan	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
8	Aplikasi Portal Berita	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
9	Website Perusahaan	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
10	Email	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
11	Aplikasi Pengadaan / SCM	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-
12	Aplikasi Dokumentasi Proyek	Melakukan backup aplikasi dan database secara berkala Hanya user yang berwenang yang memiliki akses untuk masuk ke aplikasi	-

2. Selain bagian / divisi ini siapa yang dapat mengakses asset informasi ini?

Tidak ada, bagian/divisi lain bisa mengakses asset informasi jika mendapat persetujuan dari Manajeman Divisi Teknologi Informasi (Asisten Manajer atau Manajer) dan pendampingan dari bagian Supporting Application.

3. Apa saja insiden keamanan informasi yang pernah terjadi dan membuat asset informasi tersebut berubah, rusak, tidak dapat diakses atau diakses oleh pihak yang tidak berkepentingan?

Penah terjadi kapasitas storage melebihi daya tampungnya sehingga menyebabkan aplikasi tidak bisa diakses.

4. Bagaimana prosedur atau tindakan ketika salah satu anggota bagian dipindah atau dikeluarkan?

Manajemen akan menunjuk staff baru untuk dilakukan transfer knowledge dari staff lama kemuadian akan dilakukan penghapusan akses terhadap asset informasi yang dimiliki oleh staff lama serta semua fasilitas kerja yang melekat pada staff lama akan ditarik seperti laptop.

5. Apa ada sosialisasi berkala dari IT atau semacamnya terkait kemanan informasi?

Sangat jarang, tidak ada sosialisasi berkala

6. Catatan atau Keterangan Lain

Tidak ada

Surveyor

Purnomo Dwi D

Responden

Roynther Ayub Djami

(NIP. 9014143KP)

LAMPIRAN D

Proses Penilaian Risiko

PT PJB Services

Proses Penanganan Risiko

Nama Dokumen : Proses Penanganan Risiko
Versi : 1
Tanggal : 20 Juni 2018

1. Pendahuluan

Tujuan dari dokumen ini adalah mendefinisikan proses atau metodologi dari penanganan risiko kemanan informasi dan menetapkan kontrol risiko yang diterima sesuai dengan standar ISO 27001:2005

2. Langkah-langkah Penanganan Risiko Keamanan Informasi

Berikut ini adalah langkah-langkah penanganan risiko keamanan informasi

a. Dapatkan daftar risiko dari tahap penilaian risiko.
b. Buat mapping atau hubungan antara tujuan kontrol pada ISO/IEC 27001:2005 dengan risiko yang ada.
c. Dari tujuan kontrol yang terkumpul, lakukan pemilihan apakah kontrol-kontrol yang ada pada tujuan kontrol tersebut diterapkan oleh perusahaan atau tidak.
d. Bila kontrol tersebut dapat diterapkan dan disetujui, maka pilih siapa yang akan bertanggung jawab dalam pelaksanaan kontrol tersebut
e. Bila pemilihan kontrol pada tujuan kontrol sudah selesai, maka buat daftar pernyataan pemberlakuan (*statement of applicability*) yang berisi keseluruhan kontrol pada ISO/IEC 27001:2005 dengan informasi seperti
    - Apakah kontrol tersebut disetujui untuk diterapkan atau tidak
    - Siapa yang bertanggung jawab dalam mengawasi implementasi kontrol tersebut
    - Implementasi yang disarankan pada kontrol tersebut

3. Kaji Ulang Berkala Terhadap Penanganan Risiko Keamanan Informasi

Manajemen Divisi Teknologi Informasi harus melakukan kaji ulang terhadap penanganan risiko yang ada saat ini dan memperbarui pernyataan pemberlakuan *(statement of applicability)* dengan kontrol yang baru. Kaji ulang setidaknya dilakukan satu tahun sekali atau lebih bilamana terjadi perubahan signifikan pada organisasi, teknologi, tujuan bisnis atau lingkungan bisnis.

4. Laporan Hasil Penilaian Risiko Keamanan Informasi

Laporan hasil penanganan risiko berupa pernyataan pemberlakuan harus di dokumentasikan dan disimpan pada aplikasi Manajemen Risiko

Menyetujui,

Manajer Divisi Teknologi Informasi

Habib Amaluddin Mahfudz

NIP : 8308132JA

(Halaman ini sengaja dikosongkan)

LAMPIRAN E

Kuesioner Penilaian Risiko

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Core Business Application
Surveyor : Purnomo Dwi D
Nama Responden : M. Rendra Suryadi
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Kriteria penilaian risiko aspek dampak:

No Kriteria	Tingkat Risiko	Nilai	Dampak Reputasi	Dampak Finansial	Dampak Produktivitas / Operasional
1	Tidak Signifikan	0.05	Tidak berdampak terhadap reputasi	Tidak berdampak pada kerugian finansial	Kegiatan perusahaan terganggu, tidak memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak tidak dirasakan secara lokal maupun keseluruhan sistem.
2	Minor	0.1	Reputasi perusahaan menurun, upaya atau biaya yang dibutuhkan untuk memperbaiki minimal	Kerugian finansial tidak mengganggu kegiatan operasional	Kegiatan perusahaan terganggu, tidak signifikan memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan secara lokal (pada alat tersebut saja).
3	Medium	0.2	Reputasi perusahaan terganggu dan diperlukan upaya dan biaya untuk memperbaiki reputasi perusahaan	Kerugian finansial dapat mengganggu kegiatan operasional	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada satu entitas Unit Pembangkit.
4	Signifikan	0.4	Reputasi perusahaan rusak namun bisa diperbaiki dengan upaya dan biaya yang besar	Kerugian finansial dapat menyebabkan kegiatan operasional berhenti sementara	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada Unit Kerja/ Pembangkit PJBS.
5	Malapetaka	0.8	Reputasi perusahaan rusak dan tidak bisa diperbaiki	Kerugian finansial dapat menyebabkan kebangkrutan	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada keseluruhan sistem PJBS.

- Contoh Pengisian

No	Asset	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
1	Access Data Center	Access dari orang yang tidak berkepentingan	1	2	1	1
		Adanya kerusakan Scan Kartu untuk masuk	1	1	1	1

Hasil konversi penilaian kriteria risiko

No	Asset	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
1	Access Data Center	Access dari orang yang tidak berkepentingan	0.1	0.1	0.05	0.05
		Adanya kerusakan Scan Kartu untuk masuk	0.1	0.05	0.05	0.05

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Aplikasi Pengelolaan Pelanggan	C1	Access dari orang yang tidak berkepentingan	2	2	3	1
	C2	Pencurian Data	2	2	3	1
	C3	Data pada aplikasi hilang	2	2	3	1
	C4	Aplikasi tidak bisa diakses	3	2	3	1
	C5	Kesalahan dalam input data	3	2	3	1
Aplikasi Monitoring Proyek	C6	Access dari orang yang tidak berkepentingan	2	2	3	2
	C7	Pencurian Data	2	2	3	2
	C8	Data pada aplikasi hilang	2	2	3	2
	C9	Aplikasi tidak bisa diakses	2	2	3	2
	C10	Kesalahan dalam input data	2	2	3	2
Aplikasi SDM	C11	Access dari orang yang tidak berkepentingan	1	4	4	5
	C12	Pencurian Data	1	5	5	5
	C13	Data pada aplikasi hilang	1	5	5	5
	C14	Aplikasi tidak bisa diakses	1	4	4	5
	C15	Kesalahan dalam input data	2	4	4	5
Aplikasi Knowledge Management	C16	Access dari orang yang tidak berkepentingan	1	2	3	2
	C17	Pencurian Data	1	2	3	2
	C18	Data pada aplikasi hilang	1	2	3	2
	C19	Aplikasi tidak bisa diakses	1	2	3	2
	C20	Kesalahan dalam input data	1	2	3	2
Aplikasi Forum Diskusi Karyawan	C21	Access dari orang yang tidak berkepentingan	1	1	2	2
	C22	Pencurian Data	1	1	2	2
	C23	Data pada aplikasi hilang	1	1	2	2
	C24	Aplikasi tidak bisa diakses	1	1	2	2
	C25	Kesalahan dalam input data	1	1	2	2
Aplikasi Audit Internal	C26	Access dari orang yang tidak berkepentingan	1	2	3	2
	C27	Pencurian Data	1	2	3	2
	C28	Data pada aplikasi hilang	1	2	3	2
	C29	Aplikasi tidak bisa diakses	1	2	3	2
	C30	Kesalahan dalam input data	1	2	3	2
Aplikasi Recruitment	C31	Access dari orang yang tidak berkepentingan	1	4	4	2
	C32	Pencurian Data	1	4	4	2
	C33	Data pada aplikasi hilang	1	4	4	2

	C34	Aplikasi tidak bisa diakses	1	4	4	2
	C35	Kesalahan dalam input data	1	4	4	2
Aplikasi Presensi	C36	Access dari orang yang tidak berkepentingan	1	1	3	4
	C37	Pencurian Data	1	1	3	4
	C38	Data pada aplikasi hilang	1	1	3	4
	C39	Aplikasi tidak bisa diakses	1	1	3	4
	C40	Kesalahan dalam input data	1	1	3	4
Aplikasi Keuangan	C41	Access dari orang yang tidak berkepentingan	1	4	4	5
	C42	Pencurian Data	1	4	4	5
	C43	Data pada aplikasi hilang	1	4	4	5
	C44	Aplikasi tidak bisa diakses	1	4	4	5
	C45	Kesalahan dalam input data	1	4	4	5
Aplikasi Penilaian Kinerja Karyawan	C46	Access dari orang yang tidak berkepentingan	1	1	2	2
	C47	Pencurian Data	1	1	2	2
	C48	Data pada aplikasi hilang	1	1	2	2
	C49	Aplikasi tidak bisa diakses	1	1	2	2
	C50	Kesalahan dalam input data	1	1	2	2

Surveyor

Purnomo Dwi D

Responden

M. Rendra Suryadi

(NIP. 9014140KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Data Center & Storage
Surveyor : Purnomo Dwi D
Nama Responden : Bagus Dahono Putro
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Access Data Center	A1	Access dari orang yang tidak berkepentingan	2	1	3	3
	A2	Adanya kerusakan Scan Kartu untuk masuk	1	1	1	1
	A3	Hilangnya Access Card	2	1	1	1
	A4	Tidak mendapat daya listrik	1	3	3	3
	A5	Database access hilang	1	1	3 1	1
Server	A6	Access dari orang yang tidak berkepentingan	3	2	3	3
	A7	Adanya kerusakan Hardware	1	1	2	2
	A8	Terserang virus/malware	3	2	2	2
	A9	Tidak terkoneksi dengan jaringan	2	2	2	3
	A10	Tidak mendapat daya listrik	3	2	3	4
	A11	Kesalahan konfigurasi	3	1	2	3
Server Virtualisasi	A12	Access dari orang yang tidak berkepentingan	3	2	3	3
	A13	Adanya kerusakan Hardware	1	1	2	2
	A14	Kesalahan konfigurasi	1	1	1	1
	A15	Lisensi Expired	1	1	2	2
	A16	Tidak terkoneksi dengan jaringan	1	1	1	1
Storage	A17	Kapasitas Penuh	2	2	3	4
	A18	Access dari orang yang tidak berkepentingan	2	3	3	3
	A19	Adanya kerusakan Hardware	1	3	3	3
	A20	Kesalahan konfigurasi	2	1	1	3
	A21	Tidak kompatible dengan server	1	1	1	3
	A22	Tidak mendapat daya listrik	2	1	1	4
	A23	Tidak terkoneksi dengan jaringan	1	1	1	1
Media Backup	A24	Kapasitas Penuh	1	1	1	1
	A25	Access dari orang yang tidak berkepentingan	1	1	1	1
	A26	Tidak terkoneksi dengan jaringan	2	1	1	1
	A27	Adanya kerusakan Hardware	2	2	1	1
	A28	Tidak mendapat daya listrik	2	1	2	2
	A29	Kesalahan konfigurasi	1	1	1	1
UPS Data Center	A30	Baterai tidak dapat menyimpan daya	2	2	2	2
	A31	Kesalahan konfigurasi	1	2	2	2
	A32	Tidak mendapat daya listrik	2	1	1	4
	A33	Adanya kerusakan Hardware	2	1	3	3

Precision AC	A34	Kesalahan konfigurasi	1	1	2	3
	A35	Adanya kerusakan Hardware	2	1	1	3
	A36	Tidak mendapat daya listrik	2	1	2	4
	A37	AC tidak dingin	3	1	1	3
Monitoring Kelembapan dan Suhu	A38	Adanya kerusakan Hardware	2	1	1	3
	A39	Tidak terkoneksi dengan jaringan	2	1	2	4
	A40	Tidak mendapat daya listrik	2	1	2	2
	A41	Data yang ditampilkan tidak sesuai (kalibrasi)	1	1	2	4
Fire Protection	A42	Kesalahan konfigurasi	1	1	1	2
	A43	Gas Habis	1	1	2	3
	A44	Adanya kerusakan Hardware	1	1	2	2
	A45	Tidak terkoneksi dengan sensor	1	1	3	3

Surveyor

Purnomo Dwi D

Responden

Bagus Dahono Putro

(NIP. 9414120KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Enterprise Asset Management (EAM) Application
Surveyor : Purnomo Dwi D
Nama Responden : Slamet Fajar Suryadi
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Aplikasi Manajemen Asset Pembangkit	D1	Access dari orang yang tidak berkepentingan	1	3	3	2
	D2	Pencurian Data	2	4	4	3
	D3	Data pada aplikasi hilang	1	3	3	4
	D4	Aplikasi tidak bisa diakses	3	2	3	3
	D5	Kesalahan dalam input data	3	2	3	4
Aplikasi LK3	D6	Access dari orang yang tidak berkepentingan	1	2	2	2
	D7	Pencurian Data	2	3	2	3
	D8	Data pada aplikasi hilang	3	2	2	3
	D9	Aplikasi tidak bisa diakses	2	2	2	2
	D10	Kesalahan dalam input data	2	2	2	3
Aplikasi Dashboard Pembangkit	D11	Access dari orang yang tidak berkepentingan	2	3	2	2
	D12	Pencurian Data	2	4	3	3
	D13	Data pada aplikasi hilang	3	3	3	4
	D14	Aplikasi tidak bisa diakses	2	2	2	3
	D15	Kesalahan dalam input data	1	3	3	4

Surveyor

Purnomo Dwi D

Responden

Slamet Fajar Suryadi

(NIP. 9514119KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Network & Security
Surveyor : Purnomo Dwi D
Nama Responden : Rahmat Sudrajat
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Router Agregator	B1	Access dari orang yang tidak berkepentingan	1	1	1	1
	B2	Tidak mendapat daya listrik	3	1	1	3
	B3	Adanya kerusakan Hardware	1	1	2	3
	B4	Kapasitas melebihi batas	2	1	2	3
	B5	Kesalahan konfigurasi	2	1	2	2
Firewall Server Farm	B6	Access dari orang yang tidak berkepentingan	2	3	3	3
	B7	Tidak mendapat daya listrik	3	3	3	3
	B8	Adanya kerusakan Hardware	3	3	4	5
	B9	Kapasitas melebihi batas	2	2	3	3
	B10	Kesalahan konfigurasi	2	2	3	3
Proxy Internet	B11	Access dari orang yang tidak berkepentingan	3	2	2	3
	B12	Tidak mendapat daya listrik	3	2	1	2
	B13	Adanya kerusakan Hardware	3	2	2	3
	B14	Kapasitas melebihi batas	3	2	2	4
	B15	Kesalahan konfigurasi	2	2	1	2
Endpoint Protection	B16	Access dari orang yang tidak berkepentingan	1	1	1	1
	B17	Lisensi expired	2	1	1	1
	B18	Kapasitas lisensi melebihi batas	2	1	1	1
	B19	Kesalahan konfigurasi	2	1	1	1
Core Switch	B20	Access dari orang yang tidak berkepentingan	1	1	1	3
	B21	Tidak mendapat daya listrik	3	1	1	3
	B22	Adanya kerusakan Hardware	1	1	2	3
	B23	Kapasitas melebihi batas	2	1	1	2
	B24	Kesalahan konfigurasi	1	1	1	1
Access Switch	B25	Access dari orang yang tidak berkepentingan	1	1	1	1
	B26	Tidak mendapat daya listrik	3	1	1	2
	B27	Adanya kerusakan Hardware	2	1	1	2
	B28	Kapasitas melebihi batas	1	1	1	2
	B29	Kesalahan konfigurasi	1	1	1	1
Load Balancer	B30	Access dari orang yang tidak berkepentingan	1	1	1	1
	B31	Tidak mendapat daya listrik	2	1	1	1
	B32	Adanya kerusakan Hardware	2	1	1	1

	B33	Kapasitas melebihi batas	1	1	1	1
	B34	Kesalahan konfigurasi	1	1	1	1
Access Point	B35	Access dari orang yang tidak berkepentingan	1	2	1	1
	B36	Tidak mendapat daya listrik	2	2	1	2
	B37	Adanya kerusakan Hardware	3	2	2	2
	B38	Kapasitas melebihi batas	3	2	1	3
	B39	Kesalahan konfigurasi	1	1	1	2
	B40	User tidak bisa terkoneksi	4	1	2	1
DNS	B41	Kesalahan konfigurasi	2	1	2	2
	B42	Access dari orang yang tidak berkepentingan	1	2	2	2
	B43	Data rusak	3	2	3	3
	B44	Service tidak berjalan	4	2	3	3
DHCP Server	B45	Kesalahan konfigurasi	1	1	1	1
	B46	Access dari orang yang tidak berkepentingan	1	1	1	1
	B47	Data rusak	1	1	1	1
	B48	Service tidak berjalan	3	1	1	1
	B49	User tidak mendapatkan IP Address	3	1	1	1
Active Directory	B50	Kesalahan input	3	2	3	3
	B51	Access dari orang yang tidak berkepentingan	3	3	3	3
	B52	Data rusak	3	3	2	3
	B53	Service tidak berjalan	3	2	2	2
	B54	User tidak bisa melakukan otentikasi	3	2	2	2

Surveyor

Purnomo Dwi D

Responden

Rahmat Sudrajat

(NIP. 8714142KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Supporting Application
Surveyor : Purnomo Dwi D
Nama Responden : Roynther Ayub Djami
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Aplikasi Helpdesk IT	E1	Access dari orang yang tidak berkepentingan	1	1	1	1
	E2	Pencurian Data	1	1	1	1
	E3	Data pada aplikasi hilang	1	1	1	1
	E4	Aplikasi tidak bisa diakses	1	1	1	1
	E5	Kesalahan dalam input data	4	2	1	1
Aplikasi Dokumen Center	E6	Access dari orang yang tidak berkepentingan	1	1	1	1
	E7	Pencurian Data	2	1	1	1
	E8	Data pada aplikasi hilang	2	1	1	1
	E9	Aplikasi tidak bisa diakses	2	1	1	1
	E10	Kesalahan dalam input data	1	1	1	1
Aplikasi Event	E11	Access dari orang yang tidak berkepentingan	1	1	1	1
	E12	Pencurian Data	1	1	1	1
	E13	Data pada aplikasi hilang	1	1	1	1
	E14	Aplikasi tidak bisa diakses	2	1	1	1
	E15	Kesalahan dalam input data	1	1	1	1
Aplikasi Manajemen Resiko	E16	Access dari orang yang tidak berkepentingan	1	2	2	2
	E17	Pencurian Data	1	1	1	1
	E18	Data pada aplikasi hilang	1	1	1	1
	E19	Aplikasi tidak bisa diakses	2	2	1	1
	E20	Kesalahan dalam input data	1	1	1	1
Aplikasi Inventaris	E21	Access dari orang yang tidak berkepentingan	1	1	1	1
	E22	Pencurian Data	1	1	1	1
	E23	Data pada aplikasi hilang	1	1	1	1
	E24	Aplikasi tidak bisa diakses	1	1	1	1
	E25	Kesalahan dalam input data	1	1	1	1
Aplikasi Good Corporate Governance	E26	Access dari orang yang tidak berkepentingan	1	1	1	1
	E27	Pencurian Data	1	1	1	1
	E28	Data pada aplikasi hilang	1	1	1	1
	E29	Aplikasi tidak bisa diakses	1	1	1	1
	E30	Kesalahan dalam input data	1	1	1	1
Aplikasi Pemesanan Kendaraan	E31	Access dari orang yang tidak berkepentingan	1	1	1	1
	E32	Pencurian Data	1	1	1	1
	E33	Data pada aplikasi hilang	1	1	1	1

	E34	Aplikasi tidak bisa diakses	1	1	1	1
	E35	Kesalahan dalam input data	1	1	1	1
Aplikasi Portal Berita	E36	Access dari orang yang tidak berkepentingan	1	1	1	1
	E37	Pencurian Data	1	1	1	1
	E38	Data pada aplikasi hilang	1	1	1	1
	E39	Aplikasi tidak bisa diakses	1	1	1	1
	E40	Kesalahan dalam input data	1	1	1	1
Website Perusahaan	E41	Access dari orang yang tidak berkepentingan	4	4	2	2
	E42	Pencurian Data	4	4	2	2
	E43	Data pada aplikasi hilang	2	2	2	2
	E44	Aplikasi tidak bisa diakses	4	5	2	2
	E45	Kesalahan dalam input data	3	3	2	2
Email	E46	Access dari orang yang tidak berkepentingan	4	4	4	4
	E47	Pencurian Data	5	5	5	5
	E48	Data pada aplikasi hilang	5	5	5	5
	E49	Aplikasi tidak bisa diakses	4	4	4	4
	E50	Kesalahan dalam input data	1	1	1	1
Aplikasi Pengadaan / SCM	E51	Access dari orang yang tidak berkepentingan	4	4	4	4
	E52	Pencurian Data	4	4	4	4
	E53	Data pada aplikasi hilang	4	4	4	4
	E54	Aplikasi tidak bisa diakses	2	2	2	2
	E55	Kesalahan dalam input data	1	1	1	1
Aplikasi Dokumentasi Proyek	E56	Access dari orang yang tidak berkepentingan	3	3	3	3
	E57	Pencurian Data	2	2	2	2
	E58	Data pada aplikasi hilang	3	3	3	3
	E59	Aplikasi tidak bisa diakses	2	2	2	2
	E60	Kesalahan dalam input data	2	1	1	1

Surveyor

Purnomo Dwi D

Responden

Roynther Ayub Djami

(NIP. 9014143KP)

(Halaman ini sengaja dikosongkan)

LAMPIRAN F

Konversi Penilaian Risiko

PT PJB Services

Hasil Konversi Penilaian Risiko

Bagian : Core Business Application
Surveyor : Purnomo Dwi D
Nama Responden : M. Rendra Suryadi
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Kriteria penilaian risiko aspek dampak:

No Kriteria	Tingkat Risiko	Nilai	Dampak Reputasi	Dampak Finansial	Dampak Produktivitas / Operasional
1	Tidak Signifikan	0.05	Tidak berdampak terhadap reputasi	Tidak berdampak pada kerugian finansial	Kegiatan perusahaan terganggu, tidak memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak tidak dirasakan secara lokal maupun keseluruhan sistem.
2	Minor	0.1	Reputasi perusahaan menurun, upaya atau biaya yang dibutuhkan untuk memperbaiki minimal	Kerugian finansial tidak mengganggu kegiatan operasional	Kegiatan perusahaan terganggu, tidak signifikan memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan secara lokal (pada alat tersebut saja).
3	Medium	0.2	Reputasi perusahaan terganggu dan diperlukan upaya dan biaya untuk memperbaiki reputasi perusahaan	Kerugian finansial dapat mengganggu kegiatan operasional	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada satu entitas Unit Pembangkit.
4	Signifikan	0.4	Reputasi perusahaan rusak namun bisa diperbaiki dengan upaya dan biaya yang besar	Kerugian finansial dapat menyebabkan kegiatan operasional berhenti sementara	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada Unit Kerja/ Pembangkit PJBS.
5	Malapetaka	0.8	Reputasi perusahaan rusak dan tidak bisa diperbaiki	Kerugian finansial dapat menyebabkan kebangkrutan	Kegiatan perusahaan terganggu memberikan dampak terhadap keamanan, keandalan, efisien dan operasi. Dampak dirasakan pada keseluruhan sistem PJBS.

- Contoh Pengisian

No	Asset	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
1	Access Data Center	Access dari orang yang tidak berkepentingan	1	2	1	1
		Adanya kerusakan Scan Kartu untuk masuk	1	1	1	1

Hasil konversi penilaian kriteria risiko

No	Asset	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
1	Access Data Center	Access dari orang yang tidak berkepentingan	0.1	0.1	0.05	0.05
		Adanya kerusakan Scan Kartu untuk masuk	0.1	0.05	0.05	0.05

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Aplikasi Pengelolaan Pelanggan	C1	Access dari orang yang tidak berkepentingan	0.3	0.1	0.2	0.05
	C2	Pencurian Data	0.3	0.1	0.2	0.05
	C3	Data pada aplikasi hilang	0.3	0.1	0.2	0.05
	C4	Aplikasi tidak bisa diakses	0.5	0.1	0.2	0.05
	C5	Kesalahan dalam input data	0.5	0.1	0.2	0.05
Aplikasi Monitoring Proyek	C6	Access dari orang yang tidak berkepentingan	0.3	0.1	0.2	0.1
	C7	Pencurian Data	0.3	0.1	0.2	0.1
	C8	Data pada aplikasi hilang	0.3	0.1	0.2	0.1
	C9	Aplikasi tidak bisa diakses	0.3	0.1	0.2	0.1
	C10	Kesalahan dalam input data	0.3	0.1	0.2	0.1
Aplikasi SDM	C11	Access dari orang yang tidak berkepentingan	0.1	0.4	0.4	0.8
	C12	Pencurian Data	0.1	0.8	0.8	0.8
	C13	Data pada aplikasi hilang	0.1	0.8	0.8	0.8
	C14	Aplikasi tidak bisa diakses	0.1	0.4	0.4	0.8
	C15	Kesalahan dalam input data	0.3	0.4	0.4	0.8
Aplikasi Knowledge Management	C16	Access dari orang yang tidak berkepentingan	0.1	0.1	0.2	0.1
	C17	Pencurian Data	0.1	0.1	0.2	0.1
	C18	Data pada aplikasi hilang	0.1	0.1	0.2	0.1
	C19	Aplikasi tidak bisa diakses	0.1	0.1	0.2	0.1
	C20	Kesalahan dalam input data	0.1	0.1	0.2	0.1
Aplikasi Forum Diskusi Karyawan	C21	Access dari orang yang tidak berkepentingan	0.1	0.05	0.1	0.1
	C22	Pencurian Data	0.1	0.05	0.1	0.1
	C23	Data pada aplikasi hilang	0.1	0.05	0.1	0.1
	C24	Aplikasi tidak bisa diakses	0.1	0.05	0.1	0.1
	C25	Kesalahan dalam input data	0.1	0.05	0.1	0.1
Aplikasi Audit Internal	C26	Access dari orang yang tidak berkepentingan	0.1	0.1	0.2	0.1
	C27	Pencurian Data	0.1	0.1	0.2	0.1
	C28	Data pada aplikasi hilang	0.1	0.1	0.2	0.1

	C29	Aplikasi tidak bisa diakses	0.1	0.1	0.2	0.1
	C30	Kesalahan dalam input data	0.1	0.1	0.2	0.1
Aplikasi Recruitment	C31	Access dari orang yang tidak berkepentingan	0.1	0.4	0.4	0.1
	C32	Pencurian Data	0.1	0.4	0.4	0.1
	C33	Data pada aplikasi hilang	0.1	0.4	0.4	0.1
	C34	Aplikasi tidak bisa diakses	0.1	0.4	0.4	0.1
	C35	Kesalahan dalam input data	0.1	0.4	0.4	0.1
Aplikasi Presensi	C36	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.4
	C37	Pencurian Data	0.1	0.05	0.05	0.4
	C38	Data pada aplikasi hilang	0.1	0.05	0.05	0.4
	C39	Aplikasi tidak bisa diakses	0.1	0.05	0.05	0.4
	C40	Kesalahan dalam input data	0.1	0.05	0.05	0.4
Aplikasi Keuangan	C41	Access dari orang yang tidak berkepentingan	0.1	0.4	0.4	0.8
	C42	Pencurian Data	0.1	0.4	0.4	0.8
	C43	Data pada aplikasi hilang	0.1	0.4	0.4	0.8
	C44	Aplikasi tidak bisa diakses	0.1	0.4	0.4	0.8
	C45	Kesalahan dalam input data	0.1	0.4	0.4	0.8
Aplikasi Penilaian Kinerja Karyawan	C46	Access dari orang yang tidak berkepentingan	0.1	0.05	0.1	0.1
	C47	Pencurian Data	0.1	0.05	0.1	0.1
	C48	Data pada aplikasi hilang	0.1	0.05	0.1	0.1
	C49	Aplikasi tidak bisa diakses	0.1	0.05	0.1	0.1
	C50	Kesalahan dalam input data	0.1	0.05	0.1	0.1

Surveyor

Purnomo Dwi D

Responden

M. Rendra Suryadi

(NIP. 9014140KP)

PT PJB Services

Hasil Konversi Penilaian Risiko

Bagian : Data Center & Storage
Surveyor : Purnomo Dwi D
Nama Responden : Bagus Dahono Putro
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Access Data Center	A1	Access dari orang yang tidak berkepentingan	0.3	0.05	0.2	0.2
	A2	Adanya kerusakan Scan Kartu untuk masuk	0.1	0.05	0.05	0.05
	A3	Hilangnya Access Card	0.3	0.05	0.05	0.05
	A4	Tidak mendapat daya listrik	0.1	0.2	0.2	0.2
	A5	Database access hilang	0.1	0.05	0.05	0.05
Server	A6	Access dari orang yang tidak berkepentingan	0.5	0.1	0.2	0.2
	A7	Adanya kerusakan Hardware	0.1	0.05	0.1	0.1
	A8	Terserang virus/malware	0.5	0.1	0.1	0.1
	A9	Tidak terkoneksi dengan jaringan	0.3	0.1	0.1	0.2
	A10	Tidak mendapat daya listrik	0.5	0.1	0.2	0.4
	A11	Kesalahan konfigurasi	0.5	0.05	0.1	0.2
Server Virtualisasi	A12	Access dari orang yang tidak berkepentingan	0.5	0.1	0.2	0.2
	A13	Adanya kerusakan Hardware	0.1	0.05	0.1	0.1
	A14	Kesalahan konfigurasi	0.1	0.05	0.05	0.05
	A15	Lisensi Expired	0.1	0.05	0.1	0.1
	A16	Tidak terkoneksi dengan jaringan	0.1	0.05	0.05	0.05
Storage	A17	Kapasitas Penuh	0.3	0.1	0.2	0.4
	A18	Access dari orang yang tidak berkepentingan	0.3	0.2	0.2	0.2
	A19	Adanya kerusakan Hardware	0.1	0.2	0.2	0.2
	A20	Kesalahan konfigurasi	0.3	0.05	0.05	0.2
	A21	Tidak kompatible dengan server	0.1	0.05	0.05	0.2
	A22	Tidak mendapat daya listrik	0.3	0.05	0.05	0.4
	A23	Tidak terkoneksi dengan jaringan	0.1	0.05	0.05	0.05
Media Backup	A24	Kapasitas Penuh	0.1	0.05	0.05	0.05
	A25	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	A26	Tidak terkoneksi dengan jaringan	0.3	0.05	0.05	0.05

	A27	Adanya kerusakan Hardware	0.3	0.1	0.05	0.05
	A28	Tidak mendapat daya listrik	0.3	0.05	0.1	0.1
	A29	Kesalahan konfigurasi	0.1	0.05	0.05	0.05
UPS Data Center	A30	Baterai tidak dapat menyimpan daya	0.3	0.1	0.1	0.1
	A31	Kesalahan konfigurasi	0.1	0.1	0.1	0.1
	A32	Tidak mendapat daya listrik	0.3	0.05	0.05	0.4
	A33	Adanya kerusakan Hardware	0.3	0.05	0.2	0.2
Precision AC	A34	Kesalahan konfigurasi	0.1	0.05	0.1	0.2
	A35	Adanya kerusakan Hardware	0.3	0.05	0.05	0.2
	A36	Tidak mendapat daya listrik	0.3	0.05	0.1	0.4
	A37	AC tidak dingin	0.5	0.05	0.05	0.2
Monitoring Kelembapan dan Suhu	A38	Adanya kerusakan Hardware	0.3	0.05	0.05	0.2
	A39	Tidak terkoneksi dengan jaringan	0.3	0.05	0.1	0.4
	A40	Tidak mendapat daya listrik	0.3	0.05	0.1	0.1
	A41	Data yang ditampilkan tidak sesuai (kalibrasi)	0.1	0.05	0.1	0.4
Fire Protection	A42	Kesalahan konfigurasi	0.1	0.05	0.05	0.1
	A43	Gas Habis	0.1	0.05	0.1	0.2
	A44	Adanya kerusakan Hardware	0.1	0.05	0.1	0.1
	A45	Tidak terkoneksi dengan sensor	0.1	0.05	0.2	0.2

Surveyor

Purnomo Dwi D

Responden

Bagus Dahono Putro

(NIP. 9414120KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Enterprise Asset Management (EAM) Application
Surveyor : Purnomo Dwi D
Nama Responden : Slamet Fajar Suryadi
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Aplikasi Manajemen Asset Pembangkit	D1	Access dari orang yang tidak berkepentingan	0.1	0.2	0.2	0.1
	D2	Pencurian Data	0.3	0.4	0.4	0.2
	D3	Data pada aplikasi hilang	0.1	0.2	0.2	0.4
	D4	Aplikasi tidak bisa diakses	0.5	0.1	0.2	0.2
	D5	Kesalahan dalam input data	0.5	0.1	0.2	0.4
Aplikasi LK3	D6	Access dari orang yang tidak berkepentingan	0.1	0.1	0.1	0.1
	D7	Pencurian Data	0.3	0.2	0.1	0.2
	D8	Data pada aplikasi hilang	0.5	0.1	0.1	0.2
	D9	Aplikasi tidak bisa diakses	0.3	0.1	0.1	0.1
	D10	Kesalahan dalam input data	0.3	0.1	0.1	0.2
Aplikasi Dashboard Pembangkit	D11	Access dari orang yang tidak berkepentingan	0.3	0.2	0.2	0.1
	D12	Pencurian Data	0.3	0.4	0.4	0.2
	D13	Data pada aplikasi hilang	0.5	0.2	0.2	0.4
	D14	Aplikasi tidak bisa diakses	0.3	0.1	0.1	0.2
	D15	Kesalahan dalam input data	0.1	0.2	0.2	0.4

Surveyor

Purnomo Dwi D

Responden

Slamet Fajar Suryadi

(NIP. 9514119KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Network & Security
Surveyor : Purnomo Dwi D
Nama Responden : Rahmat Sudrajat
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Router Agregator	B1	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	B2	Tidak mendapat daya listrik	0.5	0.05	0.05	0.2
	B3	Adanya kerusakan Hardware	0.1	0.05	0.1	0.2
	B4	Kapasitas melebihi batas	0.3	0.05	0.1	0.2
	B5	Kesalahan konfigurasi	0.3	0.05	0.1	0.1
Firewall Server Farm	B6	Access dari orang yang tidak berkepentingan	0.3	0.2	0.2	0.2
	B7	Tidak mendapat daya listrik	0.5	0.2	0.2	0.2
	B8	Adanya kerusakan Hardware	0.5	0.2	0.4	0.8
	B9	Kapasitas melebihi batas	0.3	0.1	0.2	0.2
	B10	Kesalahan konfigurasi	0.3	0.1	0.2	0.2
Proxy Internet	B11	Access dari orang yang tidak berkepentingan	0.5	0.1	0.1	0.2
	B12	Tidak mendapat daya listrik	0.5	0.1	0.05	0.1
	B13	Adanya kerusakan Hardware	0.5	0.1	0.1	0.2
	B14	Kapasitas melebihi batas	0.5	0.1	0.1	0.4
	B15	Kesalahan konfigurasi	0.3	0.1	0.05	0.1
Endpoint Protection	B16	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	B17	Lisensi expired	0.3	0.05	0.05	0.05
	B18	Kapasitas lisensi melebihi batas	0.3	0.05	0.05	0.05
	B19	Kesalahan konfigurasi	0.3	0.05	0.05	0.05
Core Switch	B20	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.2
	B21	Tidak mendapat daya listrik	0.5	0.05	0.05	0.2
	B22	Adanya kerusakan Hardware	0.1	0.05	0.1	0.2
	B23	Kapasitas melebihi batas	0.3	0.05	0.05	0.1
	B24	Kesalahan konfigurasi	0.1	0.05	0.05	0.05
Access Switch	B25	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	B26	Tidak mendapat daya listrik	0.5	0.05	0.05	0.1
	B27	Adanya kerusakan Hardware	0.3	0.05	0.05	0.1
	B28	Kapasitas melebihi batas	0.1	0.05	0.05	0.1
	B29	Kesalahan konfigurasi	0.1	0.05	0.05	0.05
Load Balancer	B30	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	B31	Tidak mendapat daya listrik	0.3	0.05	0.05	0.05
	B32	Adanya kerusakan Hardware	0.3	0.05	0.05	0.05
	B33	Kapasitas melebihi batas	0.1	0.05	0.05	0.05

	B34	Kesalahan konfigurasi	0.1	0.05	0.05	0.05
Access Point	B35	Access dari orang yang tidak berkepentingan	0.1	0.1	0.05	0.05
	B36	Tidak mendapat daya listrik	0.3	0.1	0.05	0.1
	B37	Adanya kerusakan Hardware	0.5	0.1	0.1	0.1
	B38	Kapasitas melebihi batas	0.5	0.1	0.05	0.2
	B39	Kesalahan konfigurasi	0.1	0.05	0.05	0.1
	B40	User tidak bisa terkoneksi	0.7	0.05	0.1	0.05
DNS	B41	Kesalahan konfigurasi	0.3	0.05	0.1	0.1
	B42	Access dari orang yang tidak berkepentingan	0.1	0.1	0.1	0.1
	B43	Data rusak	0.5	0.1	0.2	0.2
	B44	Service tidak berjalan	0.7	0.1	0.2	0.2
DHCP Server	B45	Kesalahan konfigurasi	0.1	0.05	0.05	0.05
	B46	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	B47	Data rusak	11	0.05	0.05	0.05
	B48	Service tidak berjalan	0.5	0.05	0.05	0.05
	B49	User tidak mendapatkan IP Address	0.5	0.05	0.05	0.05
Active Directory	B50	Kesalahan input	0.5	0.1	0.2	0.2
	B51	Access dari orang yang tidak berkepentingan	0.5	0.2	0.2	0.2
	B52	Data rusak	0.5	0.2	0.1	0.2
	B53	Service tidak berjalan	0.5	0.1	0.1	0.1
	B54	User tidak bisa melakukan otentikasi	0.5	0.1	0.1	0.1

Surveyor

Purnomo Dwi D

Responden

Rahmat Sudrajat

(NIP. 8714142KP)

PT PJB Services

Kuesioner Penilaian Risiko

Bagian : Supporting Application
Surveyor : Purnomo Dwi D
Nama Responden : Roynther Ayub Djami
Lokasi : Kantor Pusat PT PJB Services
Tanggal : 22 Juni 2018

Petunjuk Pengisian

- Pada Daftar Risiko, akan ditampilkan daftar asset informasi beserta risiko keamanan informasi yang ada
- Responden diharapkan dapat memberikan penilaian dengan nilai 1 (paling rendah) hingga 5 (paling tinggi) pada aspek **kemungkinan terjadi** dan **dampak (reputasi, kerugian, dan produktivitas)** untuk masing-masing risiko yang ada. Penilaian ini merupakan representasi dari **nomor kriteria** yang nantinya akan dikonversikan dengan **nilai risiko** sesuai dengan nomor kriteria yang dipilih.
- Penjelasan mengenai penilaian kriteria risiko ada dibawah ini

Kriteria penilaian risiko aspek kemungkinan terjadi:

No Kriteria	Tingkat Kemungkinan	Nilai	Probabilitas	Diskripsi Kualitatif	Insiden Sebelumnya
1	Sangat Kecil	0.1	<10%	Hampir dapat dipastikan tidak akan terjadi.	Tidak pernah terjadi dalam rentang waktu 5 tahun
2	Kecil	0.3	10%-30%	Kemungkinan kecil akan terjadi	Tidak pernah terjadi dalam rentang waktu antara 2 sampai dengan 4 tahun
3	Sedang	0.5	>30%-<70%	Kemungkinan sama antara akan terjadi dan tidak terjadi	Terjadi 1 kali dalam rentang waktu 1 tahun terakhir
4	Besar	0.7	70%-90%	Kemungkinan besar akan terjadi	Terjadi 2 sampai dengan 12 kali dalam rentang waktu 1 tahun
5	Sangat Besar	0.9	>90%	Hampir dapat dipastikan akan terjadi	Terjadi lebih dari 12 kali dalam rentang waktu 1 tahun

Daftar Risiko

Asset	Kode	Risiko	Kemungkinan Terjadi	Dampak		
				Reputasi	Finansial	Produktivitas
Aplikasi Helpdesk IT	E1	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E2	Pencurian Data	0.1	0.05	0.05	0.05
	E3	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E4	Aplikasi tidak bisa diakses	0.1	0.05	0.05	0.05
	E5	Kesalahan dalam input data	0.7	0.1	0.05	0.05
Aplikasi Dokumen Center	E6	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E7	Pencurian Data	0.3	0.05	0.05	0.05
	E8	Data pada aplikasi hilang	0.3	0.05	0.05	0.05
	E9	Aplikasi tidak bisa diakses	0.3	0.05	0.05	0.05
	E10	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Event	E11	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E12	Pencurian Data	0.1	0.05	0.05	0.05
	E13	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E14	Aplikasi tidak bisa diakses	0.3	0.05	0.05	0.05
	E15	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Manajemen Resiko	E16	Access dari orang yang tidak berkepentingan	0.1	0.1	0.1	0.1
	E17	Pencurian Data	0.1	0.05	0.05	0.05
	E18	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E19	Aplikasi tidak bisa diakses	0.3	0.1	0.05	0.05
	E20	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Inventaris	E21	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E22	Pencurian Data	0.1	0.05	0.05	0.05
	E23	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E24	Aplikasi tidak bisa diakses	0.1	0.05	0.05	0.05

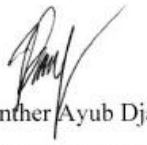
	E25	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Good Corporate Governance	E26	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E27	Pencurian Data	0.1	0.05	0.05	0.05
	E28	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E29	Aplikasi tidak bisa diakses	0.1	0.05	0.05	0.05
	E30	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Pemesanan Kendaraan	E31	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E32	Pencurian Data	0.1	0.05	0.05	0.05
	E33	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E34	Aplikasi tidak bisa diakses	0.1	0.05	0.05	0.05
	E35	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Portal Berita	E36	Access dari orang yang tidak berkepentingan	0.1	0.05	0.05	0.05
	E37	Pencurian Data	0.1	0.05	0.05	0.05
	E38	Data pada aplikasi hilang	0.1	0.05	0.05	0.05
	E39	Aplikasi tidak bisa diakses	0.1	0.05	0.05	0.05
	E40	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Website Perusahaan	E41	Access dari orang yang tidak berkepentingan	0.7	0.4	0.1	0.1
	E42	Pencurian Data	0.7	0.4	0.1	0.1
	E43	Data pada aplikasi hilang	0.3	0.1	0.1	0.1
	E44	Aplikasi tidak bisa diakses	0.7	0.8	0.1	0.1
	E45	Kesalahan dalam input data	0.5	0.2	0.1	0.1
Email	E46	Access dari orang yang tidak berkepentingan	0.7	0.4	0.4	0.4
	E47	Pencurian Data	0.9	0.8	0.8	0.8
	E48	Data pada aplikasi hilang	0.9	0.8	0.8	0.8
	E49	Aplikasi tidak bisa diakses	0.7	0.4	0.4	0.4
	E50	Kesalahan dalam input data	0.1	0.05	0.05	0.05

Aplikasi Pengadaan / SCM	E51	Access dari orang yang tidak berkepentingan	0.7	0.4	0.4	0.4
	E52	Pencurian Data	0.7	0.4	0.4	0.4
	E53	Data pada aplikasi hilang	0.7	0.4	0.4	0.4
	E54	Aplikasi tidak bisa diakses	0.3	0.1	0.1	0.1
	E55	Kesalahan dalam input data	0.1	0.05	0.05	0.05
Aplikasi Dokumentasi Proyek	E56	Access dari orang yang tidak berkepentingan	0.5	0.2	0.2	0.2
	E57	Pencurian Data	0.3	0.1	0.1	0.1
	E58	Data pada aplikasi hilang	0.5	0.2	0.2	0.2
	E59	Aplikasi tidak bisa diakses	0.3	0.1	0.1	0.1
	E60	Kesalahan dalam input data	0.3	0.05	0.05	0.05

Surveyor

Purnomo Dwi D

Responden



Roynther Ayub Djami

(NIP. 9014143KP)

LAMPIRAN G

Proses Penanganan Risiko

PT PJB Services

Proses Penanganan Risiko

Nama Dokumen : Proses Penanganan Risiko
Versi : 1
Tanggal : 20 Juni 2018

1. Pendahuluan

Tujuan dari dokumen ini adalah mendefinisikan proses atau metodologi dari penanganan risiko kemanan informasi dan menetapkan kontrol risiko yang diterima sesuai dengan standar ISO 27001:2005

2. Langkah-langkah Penanganan Risiko Keamanan Informasi

Berikut ini adalah langkah-langkah penanganan risiko keamanan informasi

a. Dapatkan daftar risiko dari tahap penilaian risiko.
b. Buat mapping atau hubungan antara tujuan kontrol pada ISO/IEC 27001:2005 dengan risiko yang ada.
c. Dari tujuan kontrol yang terkumpul, lakukan pemilihan apakah kontrol-kontrol yang ada pada tujuan kontrol tersebut diterapkan oleh perusahaan atau tidak.
d. Bila kontrol tersebut dapat diterapkan dan disetujui, maka pilih siapa yang akan bertanggung jawab dalam pelaksanaan kontrol tersebut
e. Bila pemilihan kontrol pada tujuan kontrol sudah selesai, maka buat daftar pernyataan pemberlakuan (*statement of applicability*) yang berisi keseluruhan kontrol pada ISO/IEC 27001:2005 dengan informasi seperti
    - Apakah kontrol tersebut disetujui untuk diterapkan atau tidak
    - Siapa yang bertanggung jawab dalam mengawasi implementasi kontrol tersebut
    - Implementasi yang disarankan pada kontrol tersebut

3. Kaji Ulang Berkala Terhadap Penanganan Risiko Keamanan Informasi

Manajemen Divisi Teknologi Informasi harus melakukan kaji ulang terhadap penanganan risiko yang ada saat ini dan memperbarui pernyataan pemberlakuan *(statement of applicability)* dengan kontrol yang baru. Kaji ulang setidaknya dilakukan satu tahun sekali atau lebih bilamana terjadi perubahan signifikan pada organisasi, teknologi, tujuan bisnis atau lingkungan bisnis.

4. Laporan Hasil Penilaian Risiko Keamanan Informasi

Laporan hasil penanganan risiko berupa pernyataan pemberlakuan harus di dokumentasikan dan disimpan pada aplikasi Manajemen Risiko

Menyetujui,

Manajer Divisi Teknologi Informasi

Habib Amaluddin Mahfudz

NIP : 8308132JA

(Halaman ini sengaja dikosongkan)

LAMPIRAN H

Pernyataan Pemberlakuan

(Halaman ini sengaja dikosongkan)

Pernyataan Pemberlakuan

No	Kontrol	Diterapkan (Ya/Tidak)	Tanggung Jawab	Rekomendasi Implementasi
A.5	Security Policy			
A.5.1	Information Security Policy			
A.5.1.1	Information Security Policy Document	Ya	(Asisten Manajer Pemeliharaan)	Semua kebijakan sesuai dengan kontrol yang disetujui dibuat dalam bentuk Surat Keputusan atau Nota Dinas dalam kurun waktu maksimal 5 bulan
A.5.1.2	Review of Information Security Policy	Ya	(Asisten Manajer Pemeliharaan)	Review kebijakan keamanan informasi dilakukan berkala setidaknya 1 tahun sekali oleh internal maupun eksternal (pihak ketiga)
A.6	Organization of information security			
A.6.1	Internal Organization			
A.6.1.1	Management Commitment to information security	Ya	(Manajer TI)	Manajemen TI berkomitmen dalam mendukung penyediaan sumber daya manusia, kebijakan, peraturan ataupun finansial sesuai dengan kebutuhan keamanan dan kemampuan perusahaan
A.6.1.2	Information security Co-ordination	Ya	(Manajer TI)	Ada pemisahan fungsi/peran untuk koordinasi keamanan informasi sesuai dengan kebijakan SMKI
A.6.1.3	Allocation of information security Responsibilities	Ya	(Manajer TI)	Setiap peran memiliki tanggung jawab terhadap asset informasi yang dimilikinya

A.6.1.4	Authorization process for Information Processing facilities	Ya	(Manajer TI)	Hardware atau software yang akan diintegrasikan atau diimplementasikan harus melalui pengecekan (UAT) dan setujui oleh penanggung jawab aset dan manajemen
A.6.1.5	Confidentiality agreements	Tidak		
A.6.1.6	Contact with authorities	Tidak		
A.6.1.7	Contact with special interest groups	Tidak		
A.6.1.8	Independent review of information security	Tidak		
A.6.2	External Parties			
A.6.2.1	Identification of risk related to external parties	Tidak		
A.6.2.2	Addressing security when dealing with customers	Ya	(Asisten Manajer Pengembangan)	Pihak ketiga yang membutuhkan akses terhadap sistem, harus mendapat persetujuan dari manajemen TI
A.6.2.3	Addressing security in third party agreements	Tidak		
A.7	Asset management			
A.7.1	Responsibility for Assets			
A.7.1.1	Inventory of assets	Ya	(Asisten Manajer Pengembangan)	1. Pencatatan aset informasi diperbarui berkala (3 bulan sekali) sekaligus dilakukan pengecekan terhadap aset tersebut 2. Pencatatan aset informasi harus mencatat informasi tanggal beli, tanggal garansi habis, nomor seri, asal vendor dan dokumen-dokumen yang terkait dengan aset tersebut
A.7.1.2	Ownership of Assets	Ya	(Asisten Manajer Pengembangan)	Setiap aset informasi yang tercatat harus ditunjuk penangung jawab aset tersebut
A.7.1.3	Acceptable use of assets	Tidak		

A.7.2	Information classification			
A.7.2.1	Classification Guidelines	Ya	(Asisten Manajer Pengembangan)	Setiap aset informasi harus dikelompokkan berdasarkan tingkat risiko
A.7.2.2	Information Labeling and Handling	Tidak		
A.8	Human resources security			
A.8.1	Prior to Employment			
A.8.1.1	Roles and Responsibilities	Tidak		
A.8.1.2	Screening	Tidak		
A.8.1.3	Terms and conditions of employment	Tidak		
A.8.2	During Employment			
A.8.2.1	Management Responsibility			
A.8.2.2	Information security awareness, education and training	Tidak		
A.8.2.3	Disciplinary process	Tidak		
A.8.3	Termination or change of employment			
A.8.3.1	Termination responsibility	Ya	(Asisten Manajer Pemeliharaan)	Staff yang berhenti atau dipindahtugaskan harus memberikan transfer knowledge kepada staff baru yang ditunjuk
A.8.3.2	Return of assets	Ya	(Asisten Manajer Pemeliharaan)	Staff yang berhenti atau dipindahtugaskan harus menyerahkan kembali fasilitas yang ia dapatkan kepada perusahaan
A.8.3.3	Removal of access rights	Ya	(Asisten Manajer Pemeliharaan)	Staff yang berhenti atau dipindahtugaskan akan dihapus akses terhadap aset informasi yang ia pegang sebelumnya
A.9	Physical and environmental security			

A.9.1	Secure Areas			
A.9.1.1	Physical security Perimeter	Tidak		
A.9.1.2	Physical entry controls	Ya	(Asisten Manajer Pemeliharaan)	1. Pengunjung dari luar selalu didampingi oleh staff yang bersangkutan 2. Area-area penting seperti ruang server diberi tambahan autentikasi seperti kartu akses
A.9.1.3	Securing offices, rooms and facilities	Tidak		
A.9.1.4	Protecting against external and environmental threats	Ya	(Asisten Manajer Pemeliharaan)	1. Ada pengamanan fisik dari tindakan pencurian dari luar (kartu akses, cctv) 2. Ada pengamanan khusus untuk menghindari bencana seperti banjir atau kebakaran
A.9.1.5	Working in secure areas	Ya	(Asisten Manajer Pemeliharaan)	1. Pekerjaan yang berhubungan dengan akses fisik, didampingi untuk dipantau pekerjaannya 2. Ketika area sudah tidak digunakan, harus segera dikunci dan dicek berkala apakah sudah dalam keadaan terkunci
A.9.1.6	Public access, delivery and loading areas	Tidak		
A.9.2	Equipment security			
A.9.2.1	Equipment sitting and protection	Ya	(Asisten Manajer Pengembangan)	Penyimpanan peralatan yang tidak digunakan, langsung dikembalikan ke tempat penyimpanan
A.9.2.2	Support utilities	Ya	(Asisten Manajer Pengembangan)	Peralatan pendukung seperti AC, Listrik, Fire Protection harus diinspeksi dan diuji secara berkala untuk memastikan bahwa berfungsi dengan baik (2 bulan sekali)
A.9.2.3	Cabling security	Ya	(Asisten Manajer Pengembangan)	Kabel power listrik atau telekomunikasi berada di bawah lantai (underground) atau telah menggunakan perlindungan khusus (seperti pipa kabel)

A.9.2.4	Equipment Maintenance	Ya	(Asisten Manajer Pengembangan)	1. Peralatan harus dirawat berkala sesuai dengan rekomendasi supplier atau tertera pada spesifikasinya 2. Ada catatan tindakan perawatan atau perbaikan (tanggal, tindakan apa saja, dan oleh siapa) 3. Setelah dilakukan perawatan pada peralatan, langsung dilakukan pengecekan apakah tidak ada kejanggalan atau malfungsi pada peralatan tersebut
A.9.2.5	Security of equipment off-premises	Ya	(Asisten Manajer Pengembangan)	Ketika peralatan berada di luar area perusahaan dipindahtangankan kepada pihak lain (staff atau pihak luar) maka harus ada catatan/bukti dari perpindahan atau penitipan barang tersebut.
A.9.2.6	Secure disposal or reuse of equipment	Ya	(Asisten Manajer Pengembangan)	Ada verifikasi terhadap setiap peralatan yang akan dibuang, dijual atau dihancurkan, apakah sudah tidak mengandung informasi perusahaan yang penting atau rahasia
A.9.2.7	Removal of Property	Ya	(Asisten Manajer Pengembangan)	1. Ada batas waktu, kapan aset bisa disimpan dan dibuang. 2. Aset-aset yang dibuang harus dicatat terlebih dahulu (siapa yang membuang, metode pembuangan / penghancuran, kapan)
A.10	Communications and operations management			
A.10.1	Operational Procedures and responsibilities			
A.10.1.1	Documented operating Procedures	Ya	(Asisten Manajer Pemeliharaan)	Adanya SOP terkait operational semua aset informasi
A.10.1.2	Change Management	Ya	(Asisten Manajer Pemeliharaan)	Setiap akan terjadi perubahan terhadap aset informasi harus mengajukan ijin mengenai aset informasi, penanggung jawab, waktu, dampak jika gagal, dampak jika tidak dilaksanan, dan tanda tangan dari manajemen
A.10.1.3	Segregation of Duties	Ya	(Manajer TI)	Setiap peran memiliki tanggung jawab terhadap asset informasi yang dimilikinya

A.10.1.4	Separation of development and Operations facilities	Ya	(Manajer TI)	1. Adanya pemisahan terhadap aset informasi yang bersifat development maupun operasional /production 2. Testing tidak diperkenankan pada lingkungan operasional/production
A.10.2	Third Party Service Delivery Management			
A.10.2.1	Service Delivery	Tidak		
A.10.2.2	Monitoring and review of third party services	Tidak		
A.10.2.3	Manage changes to the third party services	Tidak		
A.10.3	System Planning and Acceptance			
A.10.3.1	Capacity management	Ya	(Asisten Manajer Pemeliharaan)	1. Adanya pemantauan berkala untuk kapasitas server, storage, dan media backup 2. Adanya review secara berkala mengenai kapasitas server, storage dan media backup sebagai dasar untuk penambahan kapasitas
A.10.3.2	System acceptance	Ya	(Asisten Manajer Pengembangan)	Hardware atau software yang akan diintegrasikan atau diimplementasikan harus melalui pengecekan (UAT) dan setujui oleh penanggung jawab aset dan manajemen
A.10.4	Protection against Malicious and Mobile Code			
A.10.4.1	Controls against malicious code	Ya	(Asisten Manajer Pengembangan)	1. Menetapkan peraturan tertulis mengenai penggunaan software yang diperbolehkan 2. Filter terhadap website dan aplikasi yang tidak berkaitan dengan produktivitas 3. Instalasi dan update berkala dari program antivirus/antimalware 4. Adanya penjadwalan scanning berkala Anti Virus (minimal 1 minggu sekali)
A.10.4.2	Controls against Mobile code	Tidak		

A.10.5	Back-Up			
A.10.5.1	Information Backup	Ya	(Asisten Manajer Pemeliharaan)	1. Langkah-langkah cara backup dan restorasi harus didokumentasikan dengan jelas 2. Backup harus dilakukan berkala (sesuai dengan kebutuhan perusahaan) 3. Media backup harus disimpan pada tempat atau lokasi yang diamankan 4. Media backup harus diuji secara berkala untuk memastikan apakah masih berfungsi dengan baik
A.10.6	Network Security Management			
A.10.6.1	Network controls	Ya	(Asisten Manajer Pengembangan)	1. Ada pencatatan dan pemantauan terkait akses dan traffic jaringan 2. Koneksi terhadap jaringan mengugnakan autentikasi password
A.10.6.2	Security of Network services	Ya	(Asisten Manajer Pengembangan)	Adanya target SLA pada setiap layanan yang ada pada Divisi TI
A.10.7	Media Handling			
A.10.7.1	Management of removable media	Tidak		
A.10.7.2	Disposal of Media	Ya	(Asisten Manajer Pemeliharaan)	Dokumen yang memiliki kerahasiaan dihancurkan dengan aman (dibakar atau dipotong kecil)
A.10.7.3	Information handling procedures	Tidak		
A.10.7.4	Security of system documentation	Tidak		
A.10.8	Exchange of Information			
A.10.8.1	Information exchange policies and procedures	Tidak		
A.10.8.2	Exchange agreements	Tidak		
A.10.8.3	Physical media in transit	Tidak		
A.10.8.4	Electronic Messaging	Ya	(Asisten Manajer Pemeliharaan)	Adanya fitur keamanan seperti antispam pada email korporat perusahaan
A.10.8.5	Business Information systems	Tidak		

A.10.9	Electronic Commerce Services			
A.10.9.1	Electronic Commerce	Tidak		
A.10.9.2	On-Line transactions	Tidak		
A.10.9.3	Publicly available information	Tidak		
A.10.10	Monitoring			
A.10.10.1	Audit logging	Tidak		
A.10.10.2	Monitoring system use	Ya	(Asisten Manajer Pemeliharaan)	Adanya monitoring terkait aktivitas user seperti monitoring traffic internet
A.10.10.3	Protection of log information	Tidak		
A.10.10.4	Administrator and operator logs	Tidak		
A.10.10.5	Fault logging	Tidak		
A.10.10.6	Clock synchronization	Ya	(Asisten Manajer Pengembangan)	Adanya NTP Server internal yang digunakan untuk sinkronisasi waktu perangkat
A.11	Access control			
A.11.1	Business Requirement for Access Control			
A.11.1.1	Access control Policy	Ya	(Asisten Manajer Pengembangan)	Pembuatan kebijakan tertulsi mengenai 1. Pemberian dan penghapusan akses 2. Pemisahan peran kontrol akses 3. Review berkala hak akses
A.11.2	User Access Management			
A.11.2.1	User Registration	Ya	(Asisten Manajer Pengembangan)	1. Penggunaaan kode unik ID User (bisa berupa no karyawan, atau inisial) 2. Adanya tindakan penghapusan/penonaktifan user ID yang meninggalkan perusahaan 3. Secara berkala melakukan identifikasi dan menghapus / menon-aktifkan ID user sudah tidak dipakai (minimal 6 bulan sekali)

A.11.2.2	Privilege Measurement	Ya	(Asisten Manajer Pengembangan)	1. Adanya pencatatan yang berisi identifikasi hak akses istimewa pada setiap sistem atau proses (OS, DBMS, aplikasi, jaringan) dan siapa saja yang memiliki hak akses istimewa tersebut 2. Adanya masa expired untuk setiap hak akses istimewa 3. Adanya pencabutan atau penggantian password segera ketika user yang memiliki hak akses istimewa berpindah atau keluar dari perusahaan
A.11.2.3	User password management	Ya	(Asisten Manajer Pengembangan)	1. Password harus diganti saat pertama kali digunakan 2. Password sementara yang diberikan, harus unik untuk setiap individu dan tidak mudah ditebak 3. Sistem memaksa user agar mengganti password secara berkala minimal 1 tahun sekali 4. Password standar dari VENDOR harus dirubah setelah instalasi 5. Pemberian password kepada pihak lain, harus melalui ijin dan autorisasi dari manajemen
A.11.2.4	Review of user access rights	Ya	(Asisten Manajer Pengembangan)	1. Review hak akses dilakuan secara berkala dan setiap kali adanya perubahan peran atau jabatan (promosi, demosi atau terminasi) 2. Setiap perubahan hak akses harus dicatat
A.11.3	User Responsibilities			
A.11.3.1	Password Use	Ya	(Asisten Manajer Pemeliharaan)	Ada penetapan kualitas password minimal seperti: - mudah diingat - tidak menggunakan informasi yang mudah ditebak seperti (nama, ulang tahun, no telpon, dll) - tidak menggunakan password yang bisa ditebak dengan kata dari kamus - menggunakan campuran antara alfa numerik dan simbol - harus dirubah saat penggunaan pertama kali
A.11.3.2	Unattended user equipment	Tidak		

A.11.3.3	Clear Desk and Clear Screen Policy	Ya	(Asisten Manajer Pemeliharaan)	1. Dokumen penting atau sensitif harus disimpan pada rak atau laci yang dikunci 2. Komputer / laptop harus dalam keadaan logged off bila ditinggalkan, dan login diamankan dengan password 3. Dokumen atau kertas yang berisi informasi yang memiliki informasi penting harus segera dipindahkan dari printer setelah selesai printing
A.11.4	Network Access control			
A.11.4.1	Policy on use of network services	Ya	(Asisten Manajer Pengembangan)	1. Ada proses autentikasi (contoh : permintaan password) setiap kali mengakses layanan jaringan 2. Dilakukan pemantauan dan pencatatan terhadap penggunaan layanan jaringan
A.11.4.2	User authentication for external connections	Ya	(Asisten Manajer Pengembangan)	Penggunaan remote acces pada VPN atau semacamnya, harus memiliki autentikasi (bisa berupa password yang berkualitas)
A.11.4.3	Equipment identification in networks	Ya	(Asisten Manajer Pengembangan)	Ada software monitoring yang digunakna untuk mengetahui seluruh peralatan yang terkoneksi dengan jaringan
A.11.4.4	Remote diagnostic and configuration port protection	Ya	(Asisten Manajer Pengembangan)	Port yang tidak digunakan harus dinonaktifkan
A.11.4.5	Segregation in networks	Tidak		
A.11.4.6	Network connection control	Tidak		
A.11.4.7	Network Routing control	Tidak		
A.11.5	Operating System Access Control			

A.11.5.1	Secure Log-on procedures	Ya	(Asisten Manajer Pemeliharaan)	1. Tidak menampilkan informasi sistem atau aplikasi apapun sebelum berhasi log-on 2. Tidak menyediakan help yang dapat membantu pihak yang tidak berwenang 3. Bila salah input login, notifikasi error tidak boleh memberitahukan letak kesalahan input 4. Ada batasan percobaan login 5. Ada pencatatan terhadap setiap proses login yang gagal maupun berhasil 6. Password yang diinput tidak terlihat 7. Password tidak ditransmisikan berupa clear text 8. Ada batas masa session setelah login, bila melewati batas waktu maka akan dilog out otomatis
A.11.5.2	User identification and authentication	Ya	(Asisten Manajer Pemeliharaan)	Penggunaaan kode unik ID User untuk login ke sistem
A.11.5.3	Password Management system	Ya	(Asisten Manajer Pemeliharaan)	1. Sistem memaksa penggantian password saat login pertama kali 2. Ketika mengganti password, sistem akan meminta konfirmasi password sebelumnya, dan inputan password yang baru sebanyak minimal 2 kali, untuk menghindari kesalahan password 3. Sistem memaksa penggantian password secara berkala 4. Sistem memaksa password harus mengikuti syarat tertentu (cth : minimal panjang password atau penggunaan alfa numerikt) 5. Sistem mencatat password sebelumnya dan melarang penggunaan password yang sama 6. File penyimpanan password dipisahkan dari data sistem aplikasi (cth : disimpan berupa database)
A.11.5.4	Use of system utilities	Tidak		
A.11.5.5	Session Time-out	Tidak		
A.11.5.6	Limitation of connection time	Tidak		

A.11.6	Application and information access control			
A.11.6.1	Information access restriction	Tidak		
A.11.6.2	Sensitive system isolation	Tidak		
A.11.7	Mobile Computing and Teleworking			
A.11.7.1	Mobile computing and communication	Tidak		
A.11.7.2	Teleworking	Tidak		
A.12	Information systems acquisition, development and maintenance			
A.12.1	Security Requirements of Information Systems			
A.12.1.1	Security requirement analysis and specifications	Tidak		
A.12.2	Correct Processing in Applications			
A.12.2.1	Input data validation	Ya	(Asisten Manajer Pengembangan)	Setiap aplikasi ada validasi terhadap inputan (cth: validasi angka untuk inputan uang)
A.12.2.2	Control of internal processing	Tidak		
A.12.2.3	Message integrity	Tidak		
A.12.2.4	Output data validation	Tidak		
A.12.3	Cryptographic controls			
A.12.3.1	Policy on the use of cryptographic controls	Tidak		
A.12.3.2	Key Management	Tidak		
A.12.4	Security of System Files			
A.12.4.1	Control of Operational software	Tidak		
A.12.4.2	Protection of system test data	Tidak		

A.12.4.3	Access control to program source library	Tidak		
A.12.5	Security in Development & Support Processes			
A.12.5.1	Change Control Procedures	Tidak		
A.12.5.2	Technical review of applications after Operating system changes	Tidak		
A.12.5.3	Restrictions on changes to software packages	Tidak		
A.12.5.4	Information Leakage	Tidak		
A.12.5.5	Outsourced Software Development	Tidak		
A.12.6	Technical Vulnerability Management			
A.12.6.1	Control of technical vulnerabilities	Tidak		
A.13	Information security incident management			
A.13.1	Reporting Information Security Events and Weaknesses			
A.13.1.1	Reporting Information security events	Ya	(Asisten Manajer Pemeliharaan)	Semua detail kejadian keamanan informasi harus dilaporkan kepada manajemen
A.13.1.2	Reporting security weaknesses	Tidak		
A.13.2	Management of Information Security Incidents and Improvements			
A.13.2.1	Responsibilities and Procedures	Ya	(Asisten Manajer Pemeliharaan)	Adanya prosedur tertulis mengenai : - Pencatatan kejadian terkait keamanan informasi - Prosedur pemantauan, pendeteksian, analisa dan pelaporan kejadian terkait keamanan informasi

A.13.2.2	Learning for Information security incidents	Ya	(Asisten Manajer Pemeliharaan)	Pengetahuan dari analisa dan penyelesaian insiden keamanan informasi harus dituliskan dan disosialisasikan kepada pihak-pihak terkait dengan tujuan mengurangi dampak atau kemungkinan terjadi di masa depan
A.13.2.3	Collection of evidence	Ya	(Asisten Manajer Pemeliharaan)	Semua detail kejadian keamanan informasi harus didokumentasikan dan disimpan
A.14	Business continuity management			
A.14.1	Information Security Aspects of Business Continuity Management			
A.14.1.1	Including Information Security in Business continuity management process	Tidak		
A.14.1.2	Business continuity and Risk Assessment	Tidak		
A.14.1.3	developing and implementing continuity plans including information security	Tidak		
A.14.1.4	Business continuity planning framework	Tidak		
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	Tidak		
A.15	Compliance			
A.15.1	Compliance with Legal Requirements			
A.15.1.1	Identification of applicable legislations	Tidak		
A.15.1.2	Intellectual Property Rights (IPR)	Tidak		
A.15.1.3	Protection of organizational records	Tidak		

A.15.1.4	Data Protection and privacy of personal information	Tidak		
A.15.1.5	Prevention of misuse of information processing facilities	Tidak		
A.15.1.6	Regulation of cryptographic controls	Tidak		
A.15.2	Compliance with Security Policies and Standards and Technical compliance			
A.15.2.1	Compliance with security policy	Tidak		
A.15.2.2	Technical compliance checking	Tidak		
A.15.3	Information System Audit Considerations			
A.15.3.1	Information System Audit controls	Tidak		
A.15.3.2	Protection of information system audit tools	Tidak		

(Halaman ini sengaja dikosongkan)

LAMPIRAN I

Rekomendasi Sistem Manajemen Keamanan Informasi

(Halaman ini sengaja dikosongkan)

Rekomendasi Kontrol Sistem Manajemen Keamanan Informasi

No	Kontrol	Diterapkan (Ya/Tidak)	Tanggung Jawab	Rekomendasi Implementasi
A.5	Security Policy			
A.5.1	Information Security Policy			
A.5.1.1	Information Security Policy Document	Ya	(Asisten Manajer Pemeliharaan)	Semua kebijakan sesuai dengan kontrol yang disetujui dibuat dalam bentuk Surat Keputusan atau Nota Dinas dalam kurun waktu maksimal 5 bulan
A.5.1.2	Review of Information Security Policy	Ya	(Asisten Manajer Pemeliharaan)	Review kebijakan keamanan informasi dilakukan berkala setidaknya 1 tahun sekali oleh internal maupun eksternal (pihak ketiga)
A.6	Organization of information security			
A.6.1	Internal Organization			
A.6.1.1	Management Commitment to information security	Ya	(Manajer TI)	Manajemen TI berkomitmen dalam mendukung penyediaan sumber daya manusia, kebijakan, peraturan ataupun finansial sesuai dengan kebutuhan keamanan dan kemampuan perusahaan
A.6.1.2	Information security Co-ordination	Ya	(Manajer TI)	Ada pemisahan fungsi/peran untuk koordinasi keamanan informasi sesuai dengan kebijakan SMKI
A.6.1.3	Allocation of information security Responsibilities	Ya	(Manajer TI)	Setiap peran memiliki tanggung jawab terhadap asset informasi yang dimilikinya
A.6.1.4	Authorization process for Information Processing facilities	Ya	(Manajer TI)	Hardware atau software yang akan diintegrasikan atau diimplementasikan harus melalui pengecekan (UAT) dan setujui oleh penanggung jawab aset dan manajemen
A.6.2	External Parties			

A.6.2.2	Addressing security when dealing with customers	Ya	(Asisten Manajer Pengembangan)	Pihak ketiga yang membutuhkan akses terhadap sistem, harus mendapat persetujuan dari manajemen TI
A.8	Human resources security			
A.8.3	Termination or change of employment			
A.8.3.1	Termination responsibility	Ya	(Asisten Manajer Pemeliharaan)	Staff yang berhenti atau dipindahtugaskan harus memberikan transfer knowledge kepada staff baru yang ditunjuk
A.8.3.2	Return of assets	Ya	(Asisten Manajer Pemeliharaan)	Staff yang berhenti atau dipindahtugaskan harus menyerahkan kembali fasilitas yang ia dapatkan kepada perusahaan
A.8.3.3	Removal of access rights	Ya	(Asisten Manajer Pemeliharaan)	Staff yang berhenti atau dipindahtugaskan akan dihapus akses terhadap aset informasi yang ia pegang sebelumnya
A.9	Physical and environmental security			
A.9.1	Secure Areas			
A.9.1.2	Physical entry controls	Ya	(Asisten Manajer Pemeliharaan)	1. Pengunjung dari luar selalu didampingi oleh staff yang bersangkutan 2. Area-area penting seperti ruang server diberi tambahan autentikasi seperti kartu akses
A.9.1.4	Protecting against external and environmental threats	Ya	(Asisten Manajer Pemeliharaan)	1. Ada pengamanan fisik dari tindakan pencurian dari luar (kartu akses, cctv) 2. Ada pengamanan khusus untuk menghindari bencana seperti banjir atau kebakaran

A.9.1.5	Working in secure areas	Ya	(Asisten Manajer Pemeliharaan)	1. Pekerjaan yang berhubungan dengan akses fisik, didampingi untuk dipantau pekerjaannya 2. Ketika area sudah tidak digunakan, harus segera dikunci dan dicek berkala apakah sudah dalam keadaan terkunci
A.9.2	Equipment security			
A.9.2.1	Equipment sitting and protection	Ya	(Asisten Manajer Pengembangan)	Penyimpanan peralatan yang tidak digunakan, langsung dikembalikan ke tempat penyimpanan
A.9.2.2	Support utilities	Ya	(Asisten Manajer Pengembangan)	Peralatan pendukung seperti AC, Listrik, Fire Protection harus diinspeksi dan diuji secara berkala untuk memastikan bahwa berfungsi dengan baik (2 bulan sekali)
A.9.2.3	Cabling security	Ya	(Asisten Manajer Pengembangan)	Kabel power listrik atau telekomunikasi berada di bawah lantai (underground) atau telah menggunakan perlindungan khusus (seperti pipa kabel)
A.9.2.4	Equipment Maintenance	Ya	(Asisten Manajer Pengembangan)	1. Peralatan harus dirawat berkala sesuai dengan rekomendasi supplier atau tertera pada spesifikasinya 2. Ada catatan tindakan perawatan atau perbaikan (tanggal, tindakan apa saja, dan oleh siapa) 3. Setelah dilakukan perawatan pada peralatan, langsung dilakukan pengecekan apakah tidak ada kejanggalan atau malfungsi pada peralatan tersebut
A.9.2.5	Security of equipment off-premises	Ya	(Asisten Manajer Pengembangan)	Ketika peralatan berada di luar area perusahaan dipindahtangankan kepada pihak lain (staff atau pihak luar) maka harus ada catatan/bukti dari perpindahan atau penitipan barang tersebut.

A.9.2.6	Secure disposal or reuse of equipment	Ya	(Asisten Manajer Pengembangan)	Ada verifikasi terhadap setiap peralatan yang akan dibuang, dijual atau dihancurkan, apakah sudah tidak mengandung informasi perusahaan yang penting atau rahasia
A.9.2.7	Removal of Property	Ya	(Asisten Manajer Pengembangan)	1. Ada batas waktu, kapan aset bisa disimpan dan dibuang. 2. Aset-aset yang dibuang harus dicatat terlebih dahulu (siapa yang membuang, metode pembuangan / penghancuran, kapan)
A.10	Communications and operations management			
A.10.1	Operational Procedures and responsibilities			
A.10.1.1	Documented operating Procedures	Ya	(Asisten Manajer Pemeliharaan)	Adanya SOP terkait operational semua aset informasi
A.10.1.2	Change Management	Ya	(Asisten Manajer Pemeliharaan)	Setiap akan terjadi perubahan terhadap aset informasi harus mengajukan ijin mengenai aset informasi, penanggung jawab, waktu, dampak jika gagal, dampak jika tidak dilaksanan, dan tanda tangan dari manajemen
A.10.1.3	Segregation of Duties	Ya	(Manajer TI)	Setiap peran memiliki tanggung jawab terhadap asset informasi yang dimilikinya
A.10.1.4	Separation of development and Operations facilities	Ya	(Manajer TI)	1. Adanya pemisahan terhadap aset informasi yang bersifat development maupun operasional /production 2. Testing tidak diperkenankan pada lingkungan operasional/production
A.10.3	System Planning and Acceptance			

A.10.3.1	Capacity management	Ya	(Asisten Manajer Pemeliharaan)	1. Adanya pemantauan berkala untuk kapasitas server, storage, dan media backup 2. Adanya review secara berkala mengenai kapasitas server, storage dan media backup sebagai dasar untuk penambahan kapasitas
A.10.3.2	System acceptance	Ya	(Asisten Manajer Pengembangan)	Hardware atau software yang akan diintegrasikan atau diimplementasikan harus melalui pengecekan (UAT) dan setujui oleh penanggung jawab aset dan manajemen
A.10.4	Protection against Malicious and Mobile Code			
A.10.4.1	Controls against malicious code	Ya	(Asisten Manajer Pengembangan)	1. Menetapkan peraturan tertulis mengenai penggunaan software yang diperbolehkan 2. Filter terhadap website dan aplikasi yang tidak berkaitan dengan produktivitas 3. Instalasi dan update berkala dari program antivirus/antimalware 4. Adanya penjadwalan scanning berkala Anti Virus (minimal 1 minggu sekali)
A.10.4.2	Controls against Mobile code	Tidak		
A.10.5	Back-Up			
A.10.5.1	Information Backup	Ya	(Asisten Manajer Pemeliharaan)	1. Langkah-langkah cara backup dan restorasi harus didokumentasikan dengan jelas 2. Backup harus dilakukan berkala (sesuai dengan kebutuhan perusahaan) 3. Media backup harus disimpan pada tempat atau lokasi yang diamankan 4. Media backup harus diuji secara berkala untuk memastikan apakah masih berfungsi dengan baik
A.10.6	Network Security Management			

A.10.6.1	Network controls	Ya	(Asisten Manajer Pengembangan)	1. Ada pencatatan dan pemantauan terkait akses dan traffic jaringan 2. Koneksi terhadap jaringan mengugnakan autentikasi password
A.10.6.2	Security of Network services	Ya	(Asisten Manajer Pengembangan)	Adanya target SLA pada setiap layanan yang ada pada Divisi TI
A.10.7	Media Handling			
A.10.7.2	Disposal of Media	Ya	(Asisten Manajer Pemeliharaan)	Dokumen yang memiliki kerahasiaan dihancurkan dengan aman (dibakar atau dipotong kecil)
A.10.8	Exchange of Information			
A.10.8.4	Electronic Messaging	Ya	(Asisten Manajer Pemeliharaan)	Adanya fitur keamanan seperti antispam pada email korporat perusahaan
A.10.10	Monitoring			
A.10.10.2	Monitoring system use	Ya	(Asisten Manajer Pemeliharaan)	Adanya monitoring terkait aktivitas user seperti monitoring traffic internet
A.10.10.6	Clock synchronization	Ya	(Asisten Manajer Pengembangan)	Adanya NTP Server internal yang digunakan untuk sinkronisasi waktu perangkat
A.11	Access control			
A.11.1	Business Requirement for Access Control			
A.11.1.1	Access control Policy	Ya	(Asisten Manajer Pengembangan)	Pembuatan kebijakan tertulsi mengenai 1. Pemberian dan penghapusan akses 2. Pemisahan peran kontrol akses 3. Review berkala hak akses
A.11.2	User Access Management			

A.11.2.1	User Registration	Ya	(Asisten Manajer Pengembangan)	1. Penggunaaan kode unik ID User (bisa berupa no karyawan, atau inisial) 2. Adanya tindakan penghapusan/penonaktifan user ID yang meninggalkan perusahaan 3. Secara berkala melakukan identifikasi dan menghapus / menon-aktifkan ID user sudah tidak dipakai (minimal 6 bulan sekali)
A.11.2.2	Privilege Measurement	Ya	(Asisten Manajer Pengembangan)	1. Adanya pencatatan yang berisi identifikasi hak akses istimewa pada setiap sistem atau proses (OS, DBMS, aplikasi, jaringan) dan siapa saja yang memiliki hak akses istimewa tersebut 2. Adanya masa expired untuk setiap hak akses istimewa 3. Adanya pencabutan atau penggantian password segera ketika user yang memiliki hak akses istimewa berpindah atau keluar dari perusahaan
A.11.2.3	User password management	Ya	(Asisten Manajer Pengembangan)	1. Password harus diganti saat pertama kali digunakan 2. Password sementara yang diberikan, harus unik untuk setiap individu dan tidak mudah ditebak 3. Sistem memaksa user agar mengganti password secara berkala minimal 1 tahun sekali 4. Password standar dari VENDOR harus dirubah setelah instalasi 5. Pemberian password kepada pihak lain, harus melalui ijin dan autorisasi dari manajemen
A.11.2.4	Review of user access rights	Ya	(Asisten Manajer Pengembangan)	1. Review hak akses dilakuan secara berkala dan setiap kali adanya perubahan peran atau jabatan (promosi, demosi atau terminasi) 2. Setiap perubahan hak akses harus dicatat

A.11.3	User Responsibilities			
A.11.3.1	Password Use	Ya	(Asisten Manajer Pemeliharaan)	Ada penetapan kualitas password minimal seperti: - mudah diingat - tidak menggunakan informasi yang mudah ditebak seperti (nama, ulang tahun, no telpon, dll) - tidak menggunakan password yang bisa ditebak dengan kata dari kamus - menggunakan campuran antara alfa numerik dan simbol - harus dirubah saat penggunaan pertama kali
A.11.3.3	Clear Desk and Clear Screen Policy	Ya	(Asisten Manajer Pemeliharaan)	1. Dokumen penting atau sensitif harus disimpan pada rak atau laci yang dikunci 2. Komputer / laptop harus dalam keadaan logged off bila ditinggalkan, dan login diamankan dengan password 3. Dokumen atau kertas yang berisi informasi yang memiliki informasi penting harus segera dipindahkan dari printer setelah selesai printing
A.11.4	Network Access control			
A.11.4.1	Policy on use of network services	Ya	(Asisten Manajer Pengembangan)	1. Ada proses autentikasi (contoh : permintaan password) setiap kali mengakses layanan jaringan 2. Dilakukan pemantauan dan pencatatan terhadap penggunaan layanan jaringan
A.11.4.2	User authentication for external connections	Ya	(Asisten Manajer Pengembangan)	Penggunaan remote acces pada VPN atau semacamnya, harus memiliki autentikasi (bisa berupa password yang berkualitas)
A.11.4.3	Equipment identification in networks	Ya	(Asisten Manajer Pengembangan)	Ada software monitoring yang digunakna untuk mengetahui seluruh peralatan yang terkoneksi dengan jaringan

A.11.4.4	Remote diagnostic and configuration port protection	Ya	(Asisten Manajer Pengembangan)	Port yang tidak digunakan harus dinonaktifkan
A.11.5	Operating System Access Control			
A.11.5.1	Secure Log-on procedures	Ya	(Asisten Manajer Pemeliharaan)	1. Tidak menampilkan informasi sistem atau aplikasi apapun sebelum berhasi log-on 2. Tidak menyediakan help yang dapat membantu pihak yang tidak berwenang 3. Bila salah input login, notifikasi error tidak boleh memberitahukan letak kesalahan input 4. Ada batasan percobaan login 5. Ada pencatatan terhadap setiap proses login yang gagal maupun berhasil 6. Password yang diinput tidak terlihat 7. Password tidak ditransmisikan berupa clear text 8. Ada batas masa session setelah login, bila melewati batas waktu maka akan dilog out otomatis
A.11.5.2	User identification and authentication	Ya	(Asisten Manajer Pemeliharaan)	Penggunaaan kode unik ID User untuk login ke sistem

A.11.5.3	Password Management system	Ya	(Asisten Manajer Pemeliharaan)	1. Sistem memaksa penggantian password saat login pertama kali 2. Ketika mengganti password, sistem akan meminta konfirmasi password sebelumnya, dan inputan password yang baru sebanyak minimal 2 kali, untuk menghindari kesalahan password 3. Sistem memaksa penggantian password secara berkala 4. Sistem memaksa password harus mengikuti syarat tertentu (cth : minimal panjang password atau penggunaan alfa numerikt) 5. Sistem mencatat password sebelumnya dan melarang penggunaan password yang sama 6. File penyimpanan password dipisahkan dari data sistem aplikasi (cth : disimpan berupa database)
A.13	Information security incident management			
A.13.1	Reporting Information Security Events and Weaknesses			
A.13.1.1	Reporting Information security events	Ya	(Asisten Manajer Pemeliharaan)	Semua detail kejadian keamanan informasi harus dilaporkan kepada manajemen
A.13.2	Management of Information Security Incidents and Improvements			
A.13.2.1	Responsibilities and Procedures	Ya	(Asisten Manajer Pemeliharaan)	Adanya prosedur tertulis mengenai : - Pencatatan kejadian terkait keamanan informasi - Prosedur pemantauan, pendeteksian, analisa dan pelaporan kejadian terkait keamanan informasi
A.13.2.2	Learning for Information security incidents	Ya	(Asisten Manajer Pemeliharaan)	Pengetahuan dari analisa dan penyelesaian insiden keamanan informasi harus dituliskan dan disosialisasikan kepada pihak-pihak terkait dengan tujuan mengurangi dampak atau kemungkinan terjadi di masa depan

A.13.2.3	Collection of evidence	Ya	(Asisten Manajer Pemeliharaan)	Semua detail kejadian keamanan informasi harus didokumentasikan dan disimpan
A.7	Asset management			
A.7.1	Responsibility for Assets			
A.7.1.1	Inventory of assets	Ya	(Asisten Manajer Pengembangan)	1. Pencatatan aset informasi diperbarui berkala (3 bulan sekali) sekaligus dilakukan pengecekan terhadap aset tersebut 2. Pencatatan aset informasi harus mencatat informasi tanggal beli, tanggal garansi habis, nomor seri, asal vendor dan dokumen-dokumen yang terkait dengan aset tersebut
A.7.1.2	Ownership of Assets	Ya	(Asisten Manajer Pengembangan)	Setiap aset informasi yang tercatat harus ditunjuk penangung jawab aset tersebut
A.7.2	Information classification			
A.7.2.1	Classification Guidelines	Ya	(Asisten Manajer Pengembangan)	Setiap aset informasi harus dikelompokkan berdasarkan tingkat risiko
A.12	Information systems acquisition, development and maintenance			
A.12.2	Correct Processing in Applications			
A.12.2.1	Input data validation	Ya	(Asisten Manajer Pengembangan)	Setiap aplikasi ada validasi terhadap inputan (cth: validasi angka untuk inputan uang)

(Halaman ini sengaja dikosongkan)

BIOGRAFI PENULIS

Purnomo Dwi Djajanto. Lahir di Lumajang pada tanggal 8 April 1989. Merupakan anak kedua dari tiga bersaudara. Penulis menempuh pendidikan formal dari tahun 1995-2001 di SDN Kutorenon 1 Sukodono Lumajang, 2001-2004 di SMPN 1 Lumajang, dan 2004-2007 di SMK TELKOM SANDHY PUTRA Malang. Tahun 2008 penulis melanjutkan jenjang pendidikan S1 di jurusan Teknik Informatika, Institut Teknologi Adhi Tama Surabaya hingga tahun 2013. Setelah itu penulis bekerja di perusahaan yang bergerak di bidang *Operation & Maintenance* Pembangkit Listrik. Kemudian pada pertengahan tahun 2016, penulis melanjutkan studi S2 di Program Manajemen Teknologi Imformasi yang berada dalam Fakultas Bisnis dan Manajemen Teknologi, Institut Teknologi Sepuluh November, Surabaya. Adapun kritik dan saran dapat menghubungi penulis melalui Email: si.ipung@gmail.com

(Halaman ini sengaja dikosongkan)