BAB IV
HASIL DAN PEMBAHASAN

4.1 Pengumpulan Data

Pada tahap awal penelitian ini melakukan pengumpulan data untuk mencari tahu keadaan informasi-informasi dan data aset TI yang berada di PT. Sunrise Steel. Pengumpulan data ini dilakukan dengan cara wawancara kepada pihak yang bertanggung jawab dibagian TI untuk mencari keseluruhan aset TI mana saja yang perlu di identifikasi dari aset pendukung dan aset utama. Namun, tidak hanya dengan melakukan wawancara, penelitian ini juga melakukan observasi untuk mengidentifikasi data-data aset TI dari *Hardware* dan *Software*, juga mencari tahu *control* seperti apa yang dilakukan perusahaan untuk mengatasi ancaman, kerentanan, dan dampak yang pernah terjadi.

4.2 Identifikasi Risiko

Tujuan dari dilakukannya identifikasi risiko ini adalah untuk menentukan risiko penyebab potensi kerugian dari yang pernah terjadi atau yang akan terjadi dan bagaimana cara mengontrol dari risiko tersebut. Untuk mendapatkan identifikasi risiko tersebut, akan dilakukan penelitian identifikasi aset, identifikasi ancaman, kontrol yang ada, identifikasi kerentanan, dan identifikasi konsekuensi dari aset TI untuk mendapatkan hasil yang rinci. Kemudian dilanjutkan ke tahap penilaian risiko untuk mengetahui tingkatan risiko. Tingkatan tersebut dapat disempurnakan pada tahap lebih lanjut dari penilaian risiko.

4.2.1 Identifikasi Aset

Dalam setiap instasi atau perusahaan memiliki aset untuk menjalankan sebuah bisnisnya, demi keamanan aset pada sebuah perusahaan perlu pemeliharaan dan perlindungan. Namun, untuk melindungi dan memelihara aset tersebut harus memiliki penaggung jawab atau kepala aset yang ditugaskan khusus untuk menangani aset untuk menentukan nilai aset dalam sebuah perusahaan. Jenis aset dapat dibedakan menjadi dua, yaitu aset utama dan aset pendukung.

Dalam penelitian ini akan dilakukan identifikasi aset yang berada di perusahaan PT. Sunrise Steel dengan mencangkup *hardware* dan *software* serta aset utama dan aset pendukung. Berikut adalah rincian aset pada PT. Sunrise Steel yang disajikan pada Tabel 4.1.

Tabel 4.1 Identifikasi Aset TI

Kode Aset	Nama aset dan Unit aset	Jenis Aset	Penanggung Jawab Aset	Penjelasan
AS1	PC Sepaket (30) Ket: Monitor : Dell Mouse : Dell Keyboard: Dell	Aset Pendukung	Ka. IT Teknis	Masing-masing PC mempunyai spesifikasi yang sama rata.
AS2	Proyektor (7) Ket: GP-9 Proyektor LCD 2000 Lumens	Aset pendukung	Ka. IT Teknis	Merupakan perangkat keras aset pendukung kebutuhan yang diperlukan pada PT. Sunrise steel
AS3	LCD TV (6) Ket: Panasonic 40” Hitam TH-40D302	Aset pendukung	Ka. IT Teknis	Merupakan perangkat keras aset pendukung kebutuhan yang diperlukan pada PT. Sunrise steel
AS4	Printer (10) Ket: EPSON LaserJet AL-M200dn	Aset pendukung	Ka. IT Teknis	Merupakan perangkat keras aset pendukung kebutuhan yang diperlukan pada PT. Sunrise steel

(Sumber: hasil penelitian diolah kembali)

Tabel 4.1 Identifikasi Aset TI (Lanjutan)

Kode Aset	Nama aset dan Unit aset	Jenis Aset	Penanggung Jawab Aset	Penjelasan
AS5	Laptop (12) Ket: Lenovo x270	Aset pendukung	PT. Sunrise Steel	Masing-masing laptop perusahaan mempunyai spesifikasi : - Processor core i5-7300U CPU 2.60 GHz 2.71GHz - Ram 8 GB
AS6	Komputer *Server* (3) Ket: Dell PowerEdge T30	Aset utama	Ka. IT Support	Merupakan aset utama perangkat keras *computer server* tempat penyimpanan data yang digunakan perusahaan. Pada saat ini terdapat tiga komputer *server*.
AS7	UPS *(Uninterruptible Power Supply)*	Aset pendukung	Ka. IT Teknis	Merupakan aset tenaga listrik cadangan uang digunakan ketika listrik mendadak padam.
AS8	Perangkat jaringan Ket: Router Cisco Aironet 1852i F-K9	Aset pendukung	Ka. IT Teknis (Network Enginering)	Perangkas keras jaringan seperti Router,switch, kabel UTP, fiber optic.
AS9	Aplikasi launcher PT.Sunrise Steel	Aset utama	Ka. IT Teknis (Aplikasi Devlopment)	Aplikasi utama dari PT. Sunrise steel, yang digunakan untuk pengolahan data.
AS10	Microsoft Visual Studio	Aset pendukung	Ka. IT Support	*Software* yang digunakan untuk pengembangan pada aplikasi launcher.
AS11	Microsoft Windows 7 dan 10	Aset pendukung	Ka. IT Support	Perangkat lunak *operation sistem* yang digunakan pada komputer atau laptop perusahaan.
AS12	Microsoft Office Processing	Aset pendukung	Ka. IT Support	*Software* yang digunakan mendokumen data-data yang tersimpan di media penyimpanan komputer yang berupa word, excel, gambar, video.

(Sumber: hasil penelitian diolah kembali)

4.2.2 Identifikasi Ancaman

Sebuah perusahaan atau organisasi yang besar selalu memiliki jenis ancaman-ancaman tersendiri pada masing-masing aset TI yang nantinya akan mengakibatkan kerugian dalam jumlah besar maupun kecil dalam bisnisnya. Sebuah perusahaan harus sangat teliti dan mengetahui dengan rinci jenis sumber ancaman apa saja yang bisa membuat kerugian sekala kecil ataupun besar nantinya. Namun, sebuah perusahaan bisa mengontrol ancaman tersebut dengan mengetahui terlebih dahulu sumber ancaman dari mana dan jenis ancaman apa saja, sumber ancaman biasanya datang pada faktor dalam lingkungan kerja, faktor teknis atau juga datang dari faktor alam dan juga bisa datang dari hacker atau cracker yang berupaya masuk kedalam data penting perusahaan.

Dalam penelitian ini setelah mengidentifikasi aset utama dan aset pendukung pada PT. Sunrise Steel, selanjutnya dilakukan identifikasi ancaman dan sumber ancaman dan nantinya akan dinilai dari tingkatan ancaman, tingkatan tersebut dapat dijelaskan pada tahap lebih lanjut dari analisis risiko dalam penilaian ancaman. Berikut penjelasan sumber dan jenis ancaman apa saja yang dapat teridentifikasi dalam penelitian ini dapat disajikan pada Tabel 4.2.

Tabel 4.2 Identifikasi Ancaman

Sumber Ancaman	Kode Ancaman	Jenis Ancaman
Sumber ancaman dari Hacker / Cracker	AN1	Upaya login illegal.
	AN2	Terkenanya infeksi malware atau virus.
	AN3	Penyadapan.
	AN4	Penebakan password.
Sumber ancaman dari lingkungan karyawan	AN5	Salah Input tidak sengaja kedalam aplikasi launcher.
	AN6	Pencurian data informasi aplikasi dan perangkat keras.
	AN7	Menyebarkan data penting kepada orang lain.
	AN8	Penyalahgunaan hak akses sistem dan perangkat keras.
	AN9	Penggunaan internet selain diwaktu jam kerja.
	AN10	Memberitahu hak akses login kepada orang yang tidak berhak.
	AN11	Kesalahan oprasional disebabkan karyawan.
Sumber ancaman dari faktor teknis dan lingkungan alam	AN12	Gangguan tegangan listrik.
	AN13	Kegagalan jaringan dari pusat.
	AN14	Gangguan hubungan internet.
	AN15	Bencana alam (banjir, kebakaran) dan lain-lain.
	AN16	Aplikasi launcher atau software error .
	AN17	Kerusakan pada *hardware* akibat debu kotoran.

(Sumber: hasil penelitian diolah kembali)

4.2.3 Identifikasi Kontrol yang ada

Setelah melakukan identifikasi ancaman, selanjutnya akan mengidentifikasi kontrol yang sudah ada atau yang sudah berjalan di PT. Sunrise Steel untuk mengurangi ancaman-ancaman yang mungkin terjadi. Maka kontrol untuk mengurangi ancaman sangat penting bagi sebuah perusahaan atau organisasi untuk menjaga kemamananya. Identifikasi kontrol yang sudah ada dibuat agar rekomendasi kontrol yang diberikan pada perusahaan tidak tumpang tindih dengan kontrol yang ada saat ini di PT. Sunrise Steel untuk aset TI. Berikut identifikasi kontrol yang ada dapat dilihat pada Tabel 4.3.

Tabel 4.3 Idenitfikasi Kontrol yang ada

No	Nama aset	Jenis Aset	Kontrol yang ada
1	PC	Aset Pendukung	1. Instal Antivirus 2. Antivirus selalu update 3. Menempatkan di ruang ber AC dan jauh dari debu
2	Proyektor	Aset pendukung	1. Penggunaan yang cukup, dimatikan bila tidak diperlukan
3	LCD TV	Aset pendukung	1. Penggunaan yang cukup,dimatikan bila tidak diperlukan
4	Printer	Aset pendukung	1. Penggunaan yang cukup,dimatikan bila tidak diperlukan
5	Laptop	Aset pendukung	1. Install antivirus 2. Update antivirus 3. Memberi password
6	Komputer *Server*	Aset utama	1. Penempatan ruangan yang aman 2. Di tempatkan data center yang sudah memenuhi standart keamanan.
7	UPS *(Uninterruptible Power Supply)*	Aset pendukung	1. Memperhatikan tegangan daya listrik 2. Melakukan pengecekan terhadap bateray UPS

(Sumber: hasil penelitian diolah kembali)

Tabel 4.3 Identifikasi Kontrol yang ada (Lanjutan)

No	Nama aset	Jenis Aset	Kontrol yang ada
8	Perangkat jaringan	Aset pendukung	1. Mengimplementasikan IPS *(Intrusion Prevention System)* 2. Melakukan konfigurasi jaringan jika diperlukan 3. Melakukan pengecekan dan perawatan
9	Aplikasi launcher PT.Sunrise Steel	Aset utama	1. Melakukann *maintenance* pada aplikasi 2. Melakukan pengembangan terhadap keamanan aplikasi.
10	Microsoft visual studio	Aset pendukung	Update *software*
11	Microsoft windows 7 dan 10	Aset pendukung	Update windows secara rutin Install antivirus
12	Microsoft Office processimg	Aset pendukung	Back-up data secara rutin Update *software*

(Sumber: hasil penelitian diolah kembali)

4.2.4 Identifikasi Kerentanan

Langkah selanjutnya akan dilakukan identifikasi kerentanan yang ada pada aset TI dari aset utama dan pendukung. Pada sebuah perusahaan akan kemungkinan terdapat masalah kerentanan pada aset TI, kerentanan disebabkan karena kontrol yang ada belum bisa mengurangi ancaman tersebut dengan baik, berikut tabel identifikasi kerentanan yang terjadi dapat dilihat pada Tabel 4.4.

Tabel 4.4 Identifikasi Kerentanan

No	**Nama aset**	**Kontrol yang ada**	**Kerentanan**
1	PC	1. Install anti virus 2. Update anti virus jika terdapat notifikasi update 3. Melakukan pemeliharaan terhadap setiap PC secara berkala.	1. Anti virus yang tidak terupdate 2. Software yang digunakan terdapat malware atau virus 3. banyak debu masuk ke komponen *hardware*.

(Sumber: hasil penelitian diolah kembali)

Tabel 4.4 Identifikasi Kerentanan (Lanjutan)

No	Nama aset	Kontrol yang ada	Kerentanan
2	Proyektor	1. Penggunaan yang cukup dimatikan bila tidak terpakai. 2. Melakukan pembersihan pada lensa secara berkala	1. Hasil gambar yang dimunculkan buram 2. kemasukan debu kotor pada lensa.
3	LCD TV	1. Penggunaan yang cukup dimatikan bila tidak terpakai.	1. Penggunaan yang terlalu berlebihan atau lama. Rentan panas
4	Printer	1. Melakukan pengisian secara rutin. 2. Melakukan *maintenance* pada printer 3. Melakukan proses *cleaning* secara rutin.	1. Kehabisan tinta 2. Keluarnya garis-garis pada hasil printer. 3. Tersumbatnya tinta di catridge
5	Laptop	1. Install anti virus 2. Update anti virus jika terdapat notifikasi update 3. Melakukan pemeliharaan terhadap laptop secara berkala. 4. Mengecek kondisi bateray	1. Anti virus yang belum diperbarui 2. Software yang digunakan terdapat malware atau virus 3. banyak debu masuk ke komponen *hardware*. 4. Bateray rusak atau error
6	Komputer *Server*	1. Ditempatkan di data center yang sudah memenuhi standard keamanan. 2. Menerapkan standar konfigurasi kemanan diatas standar yang ada	1. Sharing password
7	UPS *(Uninterruptible Power Supply)*	1. Memperhatikan terhadap suplai dan daya tegangan listrik 2. Melakukan pemeliharaan pada UPS	1. Tegangan listrik yang tidak setabil. 2. Debu masuk ke komponen.
8	Perangkat jaringan (Switch, router, kabel UTP, fiber optic)	1. Melakukan konfigurasi pada jaringan. 2. Melakukan pengecekan secara berkala	1. Jaringan yang terhubung dalam perangkat mengalami gangguan. 2. Terputusnya kabel UTP

(Sumber: hasil penelitian diolah kembali)

Tabel 4.4 Identifikasi Kerentanan (Lanjutan)

No	Nama aset	Kontrol yang ada	Kerentanan
9	Aplikasi launcher PT.Sunrise Steel	1. Melakukann *maintenance* pada aplikasi 2. Melakukan pengembangan terhadap keamanan aplikasi.	1. Pengendalian data belum diterapkan dengan baik. 2. Aplikasi error 3. Serangan hacker
10	Microsoft visual studio	1. Melakukan update ketika terdapat *notifikasi update*.	1. Software eror meminta *update* tidak bisa dibuka
11	Microsoft windows 7 dan 10	1. Melakukan *update* windows secara rutin 2. Melakukan *update* anti virus secara berkala	1. Windows terdapat pemberitahuan error. 2. Windows terkena virus
12	Microsoft Office processing	1. Instal anti virus 2. Melakukan *backup* data file secara rutin	1. File error dikarenakan virus 2. File data hilang terhapus karna kelalaian admin.

(Sumber: hasil penelitian diolah kembali)

4.2.5 Identifikasi Konsekuensi

Setelah dilakukan identifikasi kerentanan, pada langkah selanjutnya akan melakukan identifikasi konsekuensi yang ada pada aset TI dari aset utama dan pendukung. Pada sebuah perusahaan atau organisasi akan kemungkinan terjadi konsekuensi. Konsekuensi datang disebabkan karena adanya kerentanan yang terdapat pada aset TI tersebut. Berikut tabel identifikasi konsekuensi yang terjadi dapat dilihat pada Tabel 4.5.

Tabel 4.5 Identifikasi Konsekuensi

No	Nama aset	Kerentanan	Konsekuensi
1	PC	1. Operation Sistem bajakan. 2. Anti virus yang tidak terupdate 3. banyak debu masuk	1. OS terkadang error atau meminta verifikasi aktivasi 2. Sering terjadinya error pada software. 3. Rusaknya piranti *hardware* pada pc
2	Proyektor	1. komponen cepat panas 2. kemasukan debu kotor.	1. menyebabkan rusak pada komponen proyektor. 2. hasil gambar proyektor buram tidak jelas.

Tabel 4.5 Identifikasi Konsekuensi (Lanjutan)

No	Nama aset	Kerentanan	Konsekuensi
3	LCD TV	1. Komponen cepat panas 2. Kemasukan debu kotor pada komponen.	1. Menyebabkan meledak pada komponen. 2. Hasil tidak jelas
4	Printer	1. Kehabisan tinta 2. Keluarnya garis garis pada hasil printer. 3. Tersumbatnya tinta di catridge	1. Hasil cetakan tidak jelas. 2. Kerusakan pada catridge printer.
5	Laptop	1. Operation sistem bajakan. 2. Software yang digunakan terdapat malware atau virus. 3. Banyak debu yang masuk.	1. OS terkadang error atau meminta verifikasi aktivasi 2. Sering terjadinya error pada software. 3. Rusaknya piranti komponen *hardware* pada laptop.
6	Komputer *Server*	1. *Sharing password*	1. Kendala terhadap akun, contoh akun terkunci oleh sistem. 2. Akses orang lain tanpa sepengetahuan admin.
7	UPS *(Uninterruptible Power Supply)*	1. Tegangan listrik yang tidak setabil. 2. Debu masuk ke komponen.	1. UPS rusak tidak dapat menyimpan daya listrik cadangan. 2. UPS rusak karena kotoran debu yang mengendap. 3. UPS meledak.
8	Perangkat jaringan (Switch, router, kabel UTP, fiber optic)	1. Jaringan yang terhubung dalam perangkat mengalami gangguan. 2. Terputusnya kabel UTP	1. Terhentinya pada data layanan atau pelayanan 2. Jaringan internet akan mengalami gangguan seperti *request tine out*
9	Aplikasi launcher PT.Sunrise Steel	1. Pengendalian data belum diterapkan dengan baik. 2. Aplikasi eror 3. Serangan hacker	1. Aplikasi tidak dapat diakses. 2. Akses dari pihak tidak dikenal mengakibatkan pengacakan data penting. 3. Data hilang

(Sumber: hasil penelitian diolah kembali)

Tabel 4.5 Identifikasi Konsekuensi (Lanjutan)

No	Nama aset	Kerentanan	Konsekuensi
10	Microsoft Visual Studio	1. Software error meminta update tidak bisa dibuka	1. Tidak dapat melakukan pengembangan untuk aplikasi launcher
11	Microsoft Windows 7 dan 10	1. Windows terdapat pemberitahuan error 2. Windows terkena virus.	1. Tidak bisa masuk ke sistem 2. Hilangnya data-data penting.
12	Microsoft Office Processing	1. File error dikarenakan virus. 3. File data hilang dikarenakan kelalian admin.	1. File rusak, tidak bisa dibuka. Data dan file terhapus permanen.

(Sumber: hasil penelitian diolah kembali)

4.3 Analisis Risiko

Dalam tahap analisis risiko ini adalah tahap penilaian yang akan menentukan nilai kriteria risiko seperti penilaian kemungkinan terjadinya ancaman atau insiden, penilaian dampak yang akan terjadi dan menentukan nilai kriteria tingkat level risiko. Maka masing-masing dari nilai kemungkinan akan terjadi ancaman dan dampak yang akan terjadi nantinya akan dikalikan sehingga menghasilkan nilai tingkatan risiko, setelah terdapat tingkatan risiko akan dilanjutkan peringkingan tingkatan risiko untuk menentukan level tersebut dengan kategori dari yang tertinggi sampai rsiko terendah.

4.3.1 Estimasi Nilai Dampak

Dalam tahap ini nilai kriteria dampak akan di pertimbangkan dengan ancaman yang telah teridentifikasi, pertimbangan ini dilakukan dengan menggunakan kuesioner untuk mendapatkan tingkatan kriteria nilai dari dampak

yang akan terjadi. Setelah dilakukan proses pertimbangan dan hasil dari kuesioner yang telah dilakukan pada PT. Sunrise Steel, kemudian akan ditentukan Estimasi nilai dampak yang terjadi pada aset TI diperusahaan PT. Surise steel. Berikut adalah hasil lampiran kuesioner dan tabel estimasi nilai dampak yang akan terjadi dapat dilihat pada Tabel 4.6 dan Lampiran 1.

Tabel 4.6 Estimasi Nilai Dampak yang akan terjadi

Kriteria Dampak	Kode ancaman yang mungkin terjadi
Tidak Kritis (1)	
Rendah (2)	AN4, AN9
Sedang (3)	AN2, AN3, AN17
Tinggi (4)	AN1, AN6, AN7, AN8 ,AN10, AN11. AN14
Sangat Tinggi (5)	AN5, AN12, AN13, AN15, AN16

(Sumber: hasil penelitian diolah kembali)

4.3.2 Estimasi Nilai Terjadinya Ancaman

Dalam tahap ini nilai kriteria kemungkinan terjadinya ancaman akan di pertimbangkan dengan ancaman yang telah teridentifikasi, pertimbangan ini dilakukan dengan menggunakan kuesioner untuk mendapatkan tingkatan kriteria nilai dari sebuah terjadinya ancaman/insiden. Setelah proses pertimbangan dan hasil dari kuesioner yang telah dilakukan pada PT. Sunrise Steel, kemudian akan ditentukan estimasi nilai terjadinya ancaman pada aset TI diperusahaan PT. Surise steel. Berikut adalah hasil lampiran kuesioner dan tabel estimasi nilai terjadinya ancaman dapat dilihat pada Tabel 4.7 dan Lampiran 2.

Tabel 4.7 Estimasi Nilai Terjadinya Ancaman

Kriteria Kemungkinan Kejadian Ancaman	Kode ancaman yang mungkin terjadi
Rare (1)	AN1, AN3, AN7, AN15
Unlikely (2)	AN4, AN6, AN8, AN10, AN11, AN12, AN13
Possible (3)	AN2, AN5, AN16, AN17
Likely (4)	AN9, AN14
Almost Certain (5)	

(Sumber: hasil penelitian diolah kembali)

4.3.3 Penilaian Tingkat Risiko

Setelah dilakukan estimasi nilai dampak dari ancaman dan estimasi nilai terjadinya ancaman, selanjutnya akan dilakukan penentuan nilai tingkat risiko aset TI. Maka penentuan nilai tingkat risiko ini diambil dari hasil indentifikasi aset dan ancaman untuk menentukan nilai tersebut. Hasil ini telah dipertimbangan sesuai dengan kebutuhan dari pihak PT. Sunrise Steel, berikut tampilan tabel keterangan dari kode aset, kode ancaman dan tabel hasil nilai tingkat risiko dapat dilihat pada Tabel 4.8 dan Tabel 4.9.

Tabel 4.8 Keterangan kode aset dan kode ancaman

Kode	Aset	Kode	Ancaman
AS1	PC	AN1	Upaya Login Ilegal
AS2	Proyektor	AN2	Terkena infeksi malware atau virus
AS3	LCD TV	AN3	Penyadapan
AS4	Printer	AN4	Penebakan password

Tabel 4.8 Keterangan kode aset dan kode ancaman (Lanjutan)

Kode	Aset	Kode	Ancaman
AS5	Laptop	AN5	Salah input data sengaja maupun tidak disengaja kedalam aplikasi launcher
AS6	Komputer Server	AN6	Pencurian data informasi aplikasi dan perangkat keras
AS7	UPS(Uninterruptible power supplay)	AN7	Menyebarkan data penting kepada orang lain
AS8	Perangkat Jaringan	AN8	Penyalahgunaan hak akses sistem dan perangkat keras
AS9	Aplikasi Launcher PT. Sunrise Steel.	AN9	Penggunaan internet untuk kepentingan lain selain diwaktu jam kerja
AS10	Microsoft visual Studio	AN10	Memberitahu hak akses login kepada orang yang tidak berhak
AS11	Microsoft Windows 7 dan 10	AN11	Kesalahan oprasional disebabkan karyawan
AS12	Microsoft Office Processing	AN12	Gangguan tegangan listrik
		AN13	Kegagalan jaringan dari pusat
		AN14	Gangguan hubungan internet
		AN15	Bencana alam (Banjir, kebakaran) dan lain-lain.
		AN16	Aplikasi launcher atau software eror
		AN17	Kerusaka pada hardware akibat debu kotoran

Tabel 4.9 Penilaian Tingkat Risiko

Kode Aset	Kode Ancaman	Nilai Ancaman	Nilai Dampak	Nilai Risiko	Kriteria Peringkat
AS1	AN6	2	4	8	4
	AN11	2	4	8	4
	AN12	2	5	10	2
	AN15	1	5	5	5
	AN17	3	3	9	3
AS2	AN8	2	4	8	4
	AN11	2	4	8	4
	AN12	2	5	10	2
	AN15	1	5	5	5
	AN17	3	3	9	3
AS3	AN8	2	4	8	4
	AN11	2	4	8	4
	AN12	2	5	10	2
	AN15	1	5	5	5
	AN17	3	3	9	3
AS4	AN8	2	4	8	4
	AN11	2	5	10	2
	AN12	2	5	10	2
	AN15	1	5	5	5
	AN17	3	3	9	3
AS5	AN6	2	4	8	4
	AN11	2	5	10	2
	AN12	2	5	10	2
	AN15	1	5	5	5
	AN17	3	3	9	3
AS6	AN10	2	4	8	4
	AN12	2	5	10	2
	AN13	2	5	10	2
	AN15	1	5	5	5
	AN17	3	3	9	3
AS7	AN11	2	4	8	4
	AN12	2	5	10	2
	AN17	3	3	9	3
AS8	AN9	4	2	8	4
	AN10	2	4	8	4
	AN11	2	4	8	4
	AN12	2	5	10	2
	AN13	2	5	10	2
	AN17	3	3	9	3

(Sumber: hasil penelitian diolah kembali)

Tabel 4.9 Penilaian Tingkat Risiko (Lanjutan)

Kode Aset	Kode Ancaman	Nilai Ancaman	Nilai Dampak	Nilai Risiko	Kriteria Peringkat
AS9	AN1	1	4	4	6
	AN3	1	3	3	7
	AN4	2	2	4	6
	AN5	3	5	15	1
	AN6	2	4	8	4
	AN10	2	4	8	4
	AN16	3	5	15	1
AS10	AN2	3	3	9	3
AS11	AN2	3	3	9	3
	AN10	2	4	8	4
AS12	AN2	3	3	9	3
	AN5	3	5	15	1
	AN7	1	4	4	6
	AN16	3	5	15	1

(Sumber: hasil penelitian diolah kembali)

Berdasarkan hasil dari Tabel 4.9 pada penilaian tingkat risiko diatas, telah ditentukan 12 aset TI beserta 17 ancaman yang mengancam aset TI tersebut, dan juga hasil nilai risiko dari perkalian terjadinya ancaman dan nilai dampak yang akan terjadi. Hasil ini menunjukan bahwa terdapat 2 aset TI yang nilai risikonya tertinggi yaitu AS9 dan AS12 dengan ancaman kode AN5 dan AN16. Maka dengan hasil ini nantinya akan dapat diusulkan sebagai rekomendasi untuk meminimalisir risiko dari ancaman yang tertinggi hingga yang terendah. Berikut hasil dari observasi kuesioner penelitian aset TI terhadap ancaman, akan disajikan pada Gambar 4.1.

KUESIONER PENELITIAN

Berikut ini adalah kuesioner yang berkaitan dengan penelitian saya berdasarkan aset teknologi informasi beserta ancaman yang kemungkinan bisa terjadi. Oleh karena itu disela-sela kesibukan bpk/ibu pimpinan, saya memohon dengan hormat kesediaan bpk/ibu untuk mengisi kuesioner yang ada, demikian saya ucapkan terima kasih.

Petunjuk Pengisian :

Mohon untuk memberikan tanda (V) pada setiap pernyataan yang ada pilih.

NAMA ASET	BERDASARKAN KODE ANCAMAN								
PC	AN1	AN2	AN3	AN4	AN5	AN6 ✓	AN7	AN8	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17 ✓	
		✓	✓			✓			
Proyektor	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8 ✓	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
		✓	✓			✓		✓	
LCD TV	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8 ✓	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
		✓	✓			✓		✓	
Printer	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8 ✓	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
		✓	✓			✓		✓	
Laptop	AN1	AN2	AN3	AN4	AN5	AN6 ✓	AN7	AN8	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
		✓	✓			✓		✓	
Komputer Server	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
✓		✓	✓	✓		✓		✓	
UPS *(Uninterruptible Power Supply)*	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
		✓	✓					✓	
Perangkat Jaringan	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9 ✓
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
✓	✓	✓	✓					✓	
Aplikasi Launcher	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9
✓	✓	✓	✓	✓	✓	✓			
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
✓							✓		
Microsoft Visual Studio	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9
	✓								
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
Microsoft Windows 7 dan 10	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9
		✓							
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	
✓									
Microsoft Office Processing	AN1	AN2	AN3	AN4	AN5	AN6	AN7	AN8	AN9
		✓			✓		✓		
	AN10	AN11	AN12	AN13	AN14	AN15	AN16	AN17	

NARASUMBER,

Support Officer
SUNRISE STEEL

Gambar 4.1 Kuesioner Aset TI terhadap Ancaman

4.4 Evaluasi Risiko

Setelah dilakukan penilaian selanjutnya akan dilanjutkan tahap evaluasi risiko yang didalamnya membuat daftar peringkat atau peringkingan agar bisa terlihat urutan ranking risikonya, risiko diberi ranking berdasarkan tingkat risikonya dimulai dari yang tertinggi sampai risiko terendah. Berikut adalah tabel peringkat risiko yang disajikan pada Tabel 4.10.

Tabel 4.10 Peringkat Risiko

Peringkat Risiko	Kode Aset	Kode Ancaman	Deskripsi
1	AS9	AN5	Kurangnya teliti karyawan saat *input* data ke aplikasi launcher
		AN16	aplikasi *error* karena aplikasi launcher yang belum stabil
1	AS12	AN5	Kesalahan input data
		AN16	Terkena virus pada s*oftware* menyebabkan kerusakan data, dan *software error*
2	AS1	AN12	Kehilangan daya listrik, mengakibatkan berhentinya sistem online
2	AS2	AN12	Kehilangan daya listrik, tidak berfungsinya aset teknologi
2	AS3	AN12	Kehilangan daya listrik, tidak berfungsinya aset teknologi
2	AS4	AN11	Karyawan yang kurang waspada atau hati-hati terhadap aset TI
		AN12	Kehilangan daya listrik, tidak berfungsinya aset teknologi
2	AS5	AN11	Kurangnya pe;atihan karyawan terhadap tanggung jawab aset TI yang diberikan
		AN12	Kehilangan daya listrik, mengakibatkan berhentinya sistem online

(Sumber: hasil penelitian diolah kembali)

Tabel 4.10 Peringkat Risiko (Lanjutan)

Peringkat Risiko	Kode Aset	Kode Ancaman	Deskripsi
2	AS6	AN12	Kehilangan daya listrik, mengakibatkan aset utama terhenti atau sistem *offline*
		AN13	Kehilangan jaringan mengakibatkan aset utama terhenti dan tidak bisa simpan data ke server.
2	AS7	AN12	Kehilangan daya listrik mengakibatkan, tidak bisa menyimpan daya saat daya sudah habis.
2	AS8	AN12	Hilangnya daya listrik, berakibat sistem *online* terhenti
		AN13	Putusnya kabel jaringan, mengakibatkan jaringan *offline*
3	AS1	AN17	Rusaknya hardware karena tidak terawat dengan baik
3	AS2	AN17	Rusaknya aset pendukung dikarenakan kurang terwat dengan baik
3	AS3	AN17	Rusaknya aset pendukung dikarenakan kurang terwat dengan baik
3	AS4	AN17	Rusaknya aset pendukung dikarenakan komponen kurang terwat dengan baik
3	AS5	AN17	Komponen rusak mengakibatkan terhentinya memasukan data ke sistem
3	AS6	AN17	Penempatan aset utama kurang baik dan berdebu
3	AS7	AN17	Debu masuk berakibat komponen *error* atau meledak
3	AS8	AN17	Kurangnya pembersihan terhadap aset TI yang sering terkena debu
3	AS10	AN2	Terinfeksi virus menyebabkan kerusakan data, dan eror dikarenakan kurangnya keamanan
3	AS11	AN2	keamanan kurang sehingga mengakibatkan virus merusak sistem windows
3	AS12	AN2	Keamanan yang kurang berakibat rusaknya atau hilangnya data penting karena malware

(Sumber: hasil penelitian diolah kembali)

Tabel 4.10 Peringkat Risiko (Lanjutan)

Peringkat Risiko	Kode Aset	Kode Ancaman	Deskripsi
4	AS1	AN6	Kurangnya kemanan pada aset TI berakibat hilangnya aset TI
		AN11	Kurang pelatihan terhadap karyawan dengan baik
4	AS2	AN8	Penyalahgunaan aset berakibat kerusakan dan hilangnya aset TI
		AN11	Kurang pelatihan terhadap karyawan dengan baik
4	AS3	AN8	Pemakaian diluar jam kerja menyebabkan pemborosan listrik
4	AS4	AN6	Kurangnya kemanan pada aset TI berakibat hilangnya aset TI
4	AS5	AN6	Kurangnya kemanan pada aset TI berakibat hilangnya aset TI
4	AS6	AN10	Memberitahu hak akses login, mengakibatkan kehilangan data penting yang tersimpan.
4	AS7	AN11	Mengakibatkan penyimpanan daya rusak
4	AS8	AN9	kurangnya *limit* pada jaringan internet
		AN10	Berakibat *speed down* pada jaringan internet
		AN11	Tidak fungsi, komponen atau kabel rusak
4	AS9	AN6	Kurangnya keamanan terhadap aplikasi utama.
		AN10	Kesalahan karyawan memberi tahu hak akses yang berakibat kehilangan data
4	AS11	AN10	Memberi tahu hak akses, berakibat kehilangan data-data penting
5	AS1	AN15	Kerusakan salah satu aset TI karena bencana alam namun kejadian minim
5	AS2	AN15	Kerusakan salah satu aset TI karena bencana alam namun kejadian minim
5	AS3	AN15	Kerusakan salah satu aset TI karena bencana alam namun kejadian minim

(Sumber: hasil penelitian diolah kembali)

Tabel 4.10 Peringkat Risiko (Lanjutan)

Peringkat Risiko	Kode Aset	Kode Ancaman	Deskripsi
5	AS4	AN15	Kerusakan salah satu aset TI karena bencana alam namun kejadian minim
5	AS5	AN15	Kerusakan salah satu aset TI karena bencana alam namun kejadian minim
5	AS6	AN15	Kerusakan salah satu aset utama TI karena bencana alam namun kejadian minim
6	AS9	AN1	Keamanan kurang sehingga keamanan asset data memiliki banyak celah kelemahan
		AN4	Tingkat kerumitan password yang kurang, sehingga mudah ditebak.
6	AS12	AN7	Kesalahan dari karyawan, menyebabkan aset TI yang penting terancam hilang.

(Sumber: hasil penelitian diolah kembali)

Berdasarkan hasil dari pemeringkatan risiko pada Tabel 4.10 menunjukan bahwa terdapat 51 risiko ancaman yang mungkin bisa terjadi pada 12 aset TI utama dan pendukung pada perusahaan PT. Sunrise Steel. Maka dari hasil ini akan dijadikan bahan pencegahan maupun pengendalian pada risiko-risiko yang tertinggi sampai yang terendah, selanjutnya penelitian ini akan dijadikan rekomendasi dalam bentuk *blueprint* pada risiko-risiko yang sudah diketahui terhadap aset TI pada perusahaan PT. Sunrise Steel.

4.5 Rekomendasi

Hasil dari rekomendasi ini, akan dijadikan bahan pertimbangan oleh perusahan PT. Sunrise Steel untuk mengontrol masalah-masalah risiko terhadap aset TI tersebut. Berikut adalah hasil rekomendasi yang akan disajikan pada Tabel 4.11.

Tabel 4.11 Rekomendasi

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS1	PC	AN12	Gangguan tegangan listrik	1. Anti virus yang belum diperbarui 2. Software yang digunakan terdapat malware atau virus 3. banyak debu masuk ke komponen *hardware*.	1. Instal Antivirus 2. Antivirus update 3. Menempatkan di ruang ber AC dan jauh dari debu	2	1. Melakukan Update Antivirus secara terjadwal. 2. Menginstal *software* antivirus. 3. Membuat jadwal khusus pelatihan untuk karyawan baru. 4. Melakukan perawatan secara berkala dan terjadwal.
		AN17	Hardware rusak disebabkan debu kotoran			3	
		AN6	Pencurian perangkat keras			4	
		AN11	Kesalahan operasional karyawan			4	
		AN15	Bencana alam (Banjir,Kebakaran, dan lain-lain)			5	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS2	Proyektor	AN12	Gangguan tegangan Listrik	1. Hasil gambar yang dimunculkan buram 2. kemasukan debu kotor pada lensa.	1. Penggunaan yang cukup, dimatikan bila tidak diperlukan	2	1. Membuat jadwal pelatihan pada karyawan baru. 2. Membuat jadwal perwatan secara berkala.
		AN17	Hardware rusak akibat debu kotoran			3	
		AN8	Penyalahgunaan perangkat keras			4	
		AN11	Kesalahan operasional disebabkan karyawan			4	
		AN15	Bencana alam (Kebakaran, banjir, dan lain-lain)			5	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS3	LCD TV	AN12	Gangguan tegangan Listrik	1. Penggunaan yang terlalu berlebihan atau lama berakibat rentan panas	1. Penggunaan yang cukup dimatikan bila tidak terpakai.	2	1. Membuat jadwal pelatihan pada karyawan baru. 2. Membuat jadwal perawatan secara berkala. 3. Member sanksi peringatan pada karyawan yang menyalahgunakan tanpa seizin perusahaan
		AN17	Hardware rusak akibat debu kotoran			3	
		AN8	Penyalahgunaan perangkat keras			4	
		AN11	Kesalahan operasional disebabkan karyawan			4	
		AN15	Bencana alam (Kebakaran, banjir, dan lain-lain)			5	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS4	Printer	AN12	Gangguan tegangan Listrik	1. Kehabisan tinta 2. Keluarnya garis-garis pada hasil printer. 3. Tersumbatnya tinta di cartridge	1. Penggunaan yang cukup,dimatikan bila tidak diperlukan	2	1. Melakukan pengecekan secara terjadwal. 2. Melakukan pembersihan secara terjadwal 3. Membuat pelatihan untuk karyawan baru. 4. Member sanksi peringatan pada karyawan yang menyalahgunakan tanpa seizin perusahaan.
		AN17	Hardware rusak akibat debu kotoran			3	
		AN8	Penyalahgunaan perangkat keras			4	
		AN11	Kesalahan operasional disebabkan karyawan			4	
		AN15	Bencana alam (Kebakaran, banjir, dan lain-lain)			5	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS5	Laptop	AN11	Gangguan tegangan Listrik	1. Anti virus yang belum diperbarui 2. Software yang digunakan terdapat malware atau virus 3. banyak debu masuk ke komponen *hardware*. 4. Bateray rusak atau eror	1. Install antivirus 2. Update antivirus	2	1. Melakukan update antivirus secara terjadwal. 2. Melakukan pengecekan kondisi kelayakan *hardware*. 3. Membatasi akses yang diberikan hanya untuk mengakses ke aplikasi launcher. 4. Membuat jadwal khusus pelatihan untuk karyawan baru.
		AN12	Hardware rusak akibat debu kotoran			2	
		AN17	Penyalahgunaan perangkat keras			3	
		AN6	Kesalahan operasional disebabkan karyawan			4	
		AN15	Bencana alam (Kebakaran, banjir, dan lain-lain)			5	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS6	Komputer Server	AN12	Gangguan tegangan Listrik	1. Sharing password	1. Ditempatkan data center yang sudah memenuhi standart keamanan	2	1. Melakukan (SMKI) Sistem manajemen keamanan informasi. 2. Membuat listrik cadangan, untuk sementara. 3. Melakukan pelatihan khusus pada karyawan baru. 4. Melakukan perawatan pada server secara terjadwal.
		AN13	Kegagalan jaringan dari pusat			2	
		AN17	Rusak dikarnakan debu kotor			3	
		AN10	Memberi tahu hak akses login pada orang lain			4	
		AN15	Bencana alam (Kebakaran, banjir, dan lain-lain)			5	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS7	UPS (Uninterr uptible power supplay)	AN12	Gangguan tegangan Listrik	1. Tegangan listrik yang tidak setabil. 2. Debu masuk ke komponen.	1. Memperhatikan tegangan daya listrik 2. Melakukan pengecekan terhadap bateray UPS	2	1. Membuat listrik cadangan, untuk sementara. 2. Melakukan perawatan secara terjadwal. 3. Membuat jadwal pelatihan khusus karyawan baru. 4. Melakukan pengecekan kelayakan UPS
		AN17	Rusak dikarnakan debu kotor			3	
		AN11	Kesalahan operasional disebabkan karyawan			4	

Tabel 4.11 Rekomendasi Lanjutan

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS8	Perangkat Jaringan	AN12	Gangguan Tegangan Listrik	1. Jaringan yang terhubung dalam perangkat mengalami gangguan. 2. Terputusnya kabel UTP	1. Melakukan konfigurasi jaringan jika diperlukan 2. Melakukan pengecekan	2	1. Membuat listrik cadangan, untuk sementara. 2. Membuat jaringan cadangan, seperti modem jika sangat diperlukan. 3. Melakukan perawatan secara terjadwal. 4. Membuat jadwal pelatihan untuk karyawan.
		AN13	Kegagalan jaringan dari pusat			2	
		AN17	Hardware rusak akibat debu			3	
		AN9	Penggunaan internet selain diwaktu jam kerja			4	
		AN10	Memberitahu akses login kepada orang lain			4	
		AN11	Kesalahan operasional disebabkan karyawan			4	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS9	Aplikasi Launcher	AN5	Salah input data disengaja maupun tidak sengaja	1. Pengendalian data belum diterapkan dengan baik. 2. Aplikasi eror 3. Serangan hacker	1. Melakukann *maintenance* pada aplikasi 2. Melakukan pengembangan terhadap keamanan aplikasi.	1	1. Melakukan penerapan (SMKI) Sistem Manajemen Keamanan Informasi 2. Melakukan *maintenance* pada aplikasi secara terjadwal. 3. Membatasi Akses yang diberikan hanya untuk mengakses ke aplikasi launcher
		AN16	Aplikasi Launcher atau *software* eror			1	
		AN6	Pencurian data informasi aplikasi			4	
		AN10	Memberitahu akses login pada orang lain kerja			4	
		AN1	Upaya login ilegal			6	
		AN4	Penebakan password			6	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS10	Microsoft Visual Studio	AN2	Terkenanya malware atau virus.	1. Software error meminta *update* tidak bisa dibuka	1. Update *software*	3	1. Instal antivirus 2. Update antivirus

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS11	Microsoft Windows 7 dan 10	AN2	Terkena infeksi malware atau virus	1. Windows terdapat pemberitahuan error. 2. Windows terkena virus.	1. Update windows secara rutin. 2. Install antivirus.	3	1. Melakukan update windows secara rutin. 2. Install antivirus 3. Melakukan update antivus untuk keamanan lebih baik. 4. Membatasi akses yang diberikan hanya untuk mengakses ke sistem
		AN10	Memberitahu akses login pada orang lain			4	

Tabel 4.11 Rekomendasi (Lanjutan)

Kode	Aset	Kode	Ancaman	Kerentanan	Kontrol yang ada	Peringkat Risiko	Rekomendasi Kontrol
AS12	Microsoft Office Processing	AN5	Salah input data sengaja maupun tidak sengaja	1. File error dikarenakan virus 2. File data hilang terhapus karna kelalaian admin.	1. Back-up data secara rutin. 2. Update *software*	1	1. Melakukan pelatihan terhadap karyawan. 2. Melakukan back-up data secara terjadwal. 3. Install antivirus terbaru. 4. Melakukan pembatasan pada hak akses sistem
		AN16	*Software* eror			1	
		AN2	Terkenanya infeksi malware atau virus			3	
		AN7	Menyebarkan data penting pada orang lain			6	