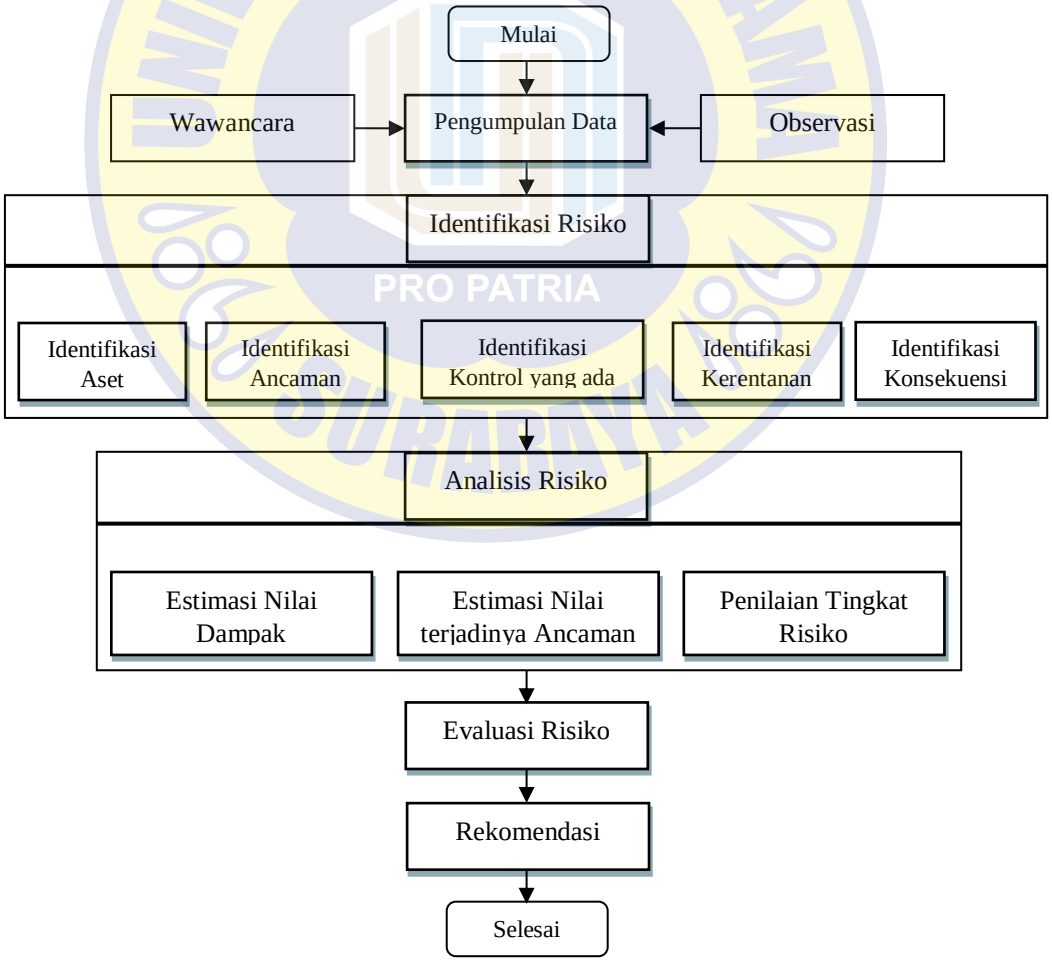
BAB III

METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Penelitian ini untuk memahami, menganalisis, serta memecahkan masalah berdasarkan risiko yang ada dan juga merupakan rangkaian proses yang panjang serta sistematis. Agar penelitian berjalan dengan baik maka diperlukan kerangka kerja ISO 27005:2018 yang didalamnya berisi tahapan yang harus dilakukan dalam melakukan penelitian yang dapat dilihat dalam bentuk gambar 3.1.



Gambar 3.1 Alur Diagram

3.1.1 Pengumpulan Data

Pada tahap ini penelitian melakukan pengumpulan data pada PT. Sunrise Steel dengan cara wawancara pada salah satu pihak yang bertanggung jawab pada aset TI kemudian melakukan pengamatan secara cermat dan mengumpulkan data-data aset TI yang rawan terkenanya ancaman risiko, dengan tahapan pengumpulan data ini diharapkan mampu mengetahui keseluruhan kondisi yang terjadi saat ini di PT. Sunrise Steel untuk membuktikan kebenaran dari sebuah kejadian. Pada pengamatan data ini juga mencari informasi sumber daya manusia dan juga teknologi yang akan diperlukan dalam proses pengelolahan risiko.

3.1.2 Identifikasi Risiko

Dalam tahap penelitian identifikasi risiko ini terdapat beberapa hal-hal yang dilakukan untuk menentukan penyebab risiko yang berpotensi 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, identifikasi kontrol yang ada, identifikasi kerentanan, dan identifikasi konsekuensi terhadap aset TI untuk mendapatkan hasil yang lebih rinci.

3.1.2.1 Identifikasi Aset

Dalam identifikasi aset akan dilakukan penelitian terhadap semua ruang lingkup perusahaan PT. Sunrise Steel yang berhubungan dengan teknologi informasi (TI) baik *hardware*, *software* dan orang yang bertanggung jawab

terhadap aset TI tersebut. Dalam aset TI terdapat beberapa jenis seperti aset utama dan aset pendukung. Aset utama didefinisikan sebagai aset yang dirahasiakan dan sangat dijaga dalam perusahaan seperti server dan juga aplikasi utama untuk berjalannya sebuah perusahaan, namun aset pendukung didefinisikan sebagai pendukung dalam membangun sebuah organisasi dan perusahaan seperti perangkat keras dan perangkat lunak yang bersifat pendukung untuk berjalannya organisasi.

3.1.2.2 Identifikasi Ancaman

Melakukan tahap identifikasi ancaman terhadap aset-aset TI pada PT. Sunrise Steel ini membutuhkan identifikasi aset terlebih dahulu, setelah melakukan identifikasi aset akan dilanjutkan dalam proses identifikasi ancaman yang pernah terjadi dan yang akan terjadi terhadap aset TI mengetahui dengan rinci jenis sumber ancaman apa saja yang bisa membuat kerugian sekala kecil ataupun besar nantinya. Sumber ancaman mempunyai beberapa jenis seperti sumber ancaman dari karyawan, lingkungan kerja, hacker, dan juga dari faktor teknis ataupun faktor alam.

3.1.2.3 Identifikasi Kontrol yang ada

Pada tahap penelitian ini mencari tahu kondisi identifikasi kontrol yang ada pada perusahaan PT. Surise Steel yang nanti akan dikembangkan dengan rekomendasi kontrol penelitian. Maka perlu identifikasi kontrol yang sudah

berjalan agar tidak tumpang tindih dengan kontrol yang baru sebagai rekomendasi.

3.1.2.4 Identifikasi Kerentanan

Setelah melakukan tahap identifikasi kontrol yang ada selanjutnya ketahap identifikasi kerentanan terhadap aset TI yang kemungkinan masih bisa dapat dieksploitasi oleh orang yang tidak bertanggung jawab. Kerentanan terjadi disebabkan kontrol yang ada belum memenuhi kebutuhan kemanan terhadap aset TI yang berakibat rentan terkena risiko dalam sekala kecil sampai besar.

3.1.2.5 Identifikasi Konsekuensi

Dalam tahap identifikasi konsekuensi atau dampak terjadi disebabkan adanya kerentanan yang tidak bisa terkontrol dengan baik sehingga timbul konsekuensi yang mengakibatkan kehilangan atau kerusakan data-data kerahasiaan perusahaan yang ada pada aset TI tersebut.

3.1.3 Analisis Risiko.

Pada tahap ini analisis risiko bertujuan untuk menentukan nilai kriteria risiko seperti penilaian kemungkinan terjadinya ancaman atau insiden, penilaian dampak yang akan terjadi dan menentukan nilai kriteria tingkat level risiko. Masing-masing dari nilai dampak dan kemungkinan akan terjadi ancaman nantinya akan dikalikan sehingga menghasilkan nilai tingkatan risiko. Kriteria risiko kemungkinan terjadinya ancaman dan dampak tidak memiliki tujuan yang

khusus, namun dapat disesuaikan dengan kebutuhan dari organisasi yang diamati. Berikut kriteria kemungkinan terjadinya ancaman dan kriteria dampak terjadinya risiko pada Tabel 3.1 dan Tabel 3.2.

Tabel 3.1 Kriteria kemungkinan terjadinya ancaman/insiden[11]

Kemungkinan Terjadinya Ancaman	**Keterangan**
Rare	Tidak terjadi ancaman
Unlikely	Kecenderungan kejadian jarang
Possible	Kecenderungan kejadian cukup sering
Likely	Kecenderungan kejadian sering
Almost Certain	Kecenderungan kejadian sangat sering

Tabel 3.2 Kriteria dampak terjadinya risiko[11]

Kriteria Dampak	Keterangan
Tidak Kritis (1)	1. Tidak terjadi gangguan produktifitas yang disebabkan pada aset TI, batas toleransi gangguan < 30 menit.
Rendah (2)	1. Menimbulkan gangguan kecil yang disebabkan aset TI, batas toleransi gangguan 1 jam sampai 2 jam. 2. *Backup* data masih bisa dilakukan.
Sedang (3)	1. Menimbulkan gangguan kegiatan produktifitas pada aset TI, batas toleransi gangguan < 12 jam. 2. *Backup* data masih bisa dilakukan. 3. Listrik padam.
Tinggi (4)	1. Menimbulkan gangguan kegiatan produktifitas pada aset utama TI, batas toleransi gangguan < 1 hari. 2. Penggunaan aset IT yang tidak berwenang. 3. Pengaksesan sistem tanpa izin dari pengelola sistem. 4. Terdapat kesalahan Input data, dikarenakan kelalaian karyawan.
Sangat Tinggi (5)	1. Menimbulkan gangguan pada kegiatan produktifitas aset utama TI, batas toleransi gangguan 1hari sampai 2 hari. 2. Kerusakan salah satu perangkat keras aset TI dan tidak terdapat cadangan 3. Tersebarnya data informasi rahasia kepada pihak yang tidak berwenang. 4. Proses tidak dapat dilakukan karena data hilang atau rusak dan tidak terdapat *backup* data. 5. Akses yang dilakukan oleh pihak yang tidak berwenang.

3.1.4 Evaluasi Risiko

Tahap evaluasi risiko ini bertujuan untuk mencari tingkatan peringkingan level risiko dari sumber ancaman terhadap aset TI pada perusahan PT. Sunrise steel. Dalam menentukan peringkingan risiko ini dibutuhkah dari hasil identifikasi aset TI dan ancaman apa saja yang membuat kerusakan atau kehancuran pada aset TI. Maka untuk menentukan tingkat peringkingan risiko ini terdapat peringkat dari yang tertinggi sampai risiko terendah. Hasil dari evaluasi risiko akan dijadikan sebagai hasil akhir yaitu recomedasi untuk menjadi pertimbangan bagi perusahaan.

3.1.5 Rekomendasi

Pada tahap ini akan dilakukan sebuah keputusan dan penetapan terhadap risiko-risiko yang sudah diketahui dari identifikasi ancaman, kontrol yang ada, kerentanan, dan konsekuensi serta hasil dari evaluasi kemudian untuk dijadikan pertimbangan rekomendasi dalam bentuk *blueprint* pada risiko aset TI perusahaan.