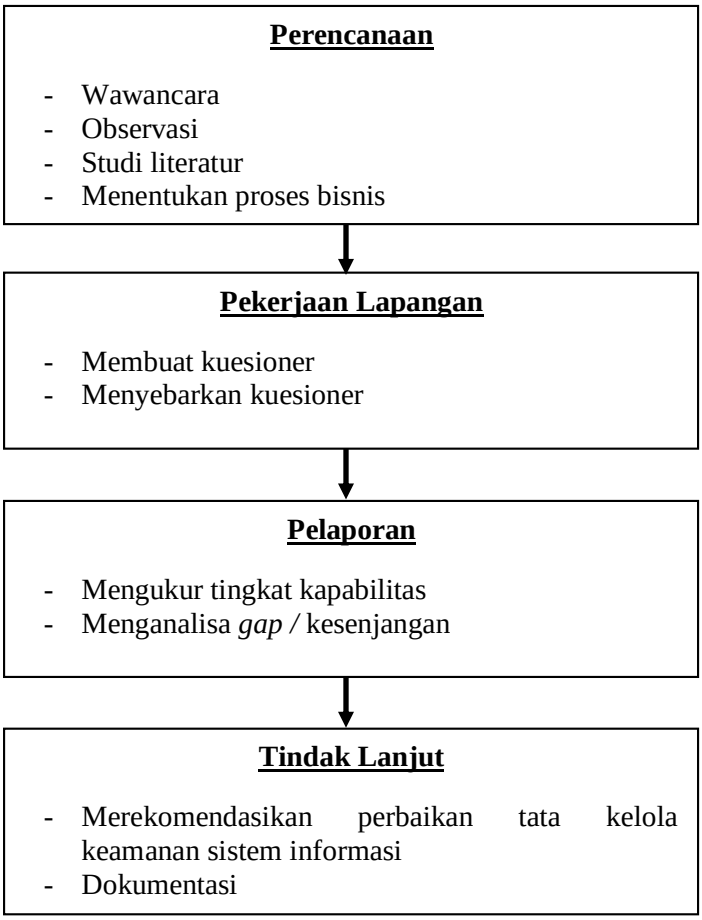
BAB III. METODOLOGI PENELITIAN

Bab ini membahas tentang pelaksanaan setiap tahapan pada metodologi penelitian audit operasional. Metodologi audit operasional berkaitan dengan penggunaan secara ekonomis dan efisien atas sumber daya pencapaian tujuan serta sasaran yang diterapkan. Audit operasional memiliki 4 tahapan, yaitu perencanaan (*planning*), pekerjaan lapangan (*fieldwork*), pelaporan (*reporting*), dan tindak lanjut (*follow up*).

Tahapan audit operasional juga disajikan dalam bentuk bagan penelitian yang dapat dilihat pada gambar 3.1.



Gambar 3.1 Bagan Penelitian

3.1 Perencanaan (*Planning*)

Tahap perencanaan dilakukan dengan mengumpulkan data berikut.

1. Wawancara

   Mewawancarai staf IT untuk mengidentifikasi masalah khususnya tentang tindakan *cracking* yang pernah terjadi pada sistem informasi Lampost.

2. Observasi

   Mengamati tata kelola sistem informasi Lampost.

3. Studi literatur

   Mengumpulkan bahan referensi berupa teori yang berasal dari buku dan jurnal serta data sekunder berupa dokumen yang mendukung hasil penelitian.

4. Menentukan proses bisnis

   Metode yang digunakan untuk menganalisis tata kelola keamanan informasi, yaitu *Framework* COBIT 5. *Framework* COBIT 5 merupakan standar kontrol yang umum terhadap teknologi informasi, dengan memberikan kerangka kerja dan kontrol terhadap teknologi informasi yang dapat diterima dan diterapkan secara internasional. *Framework* COBIT berupa kerangka kerja yang harus digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum panduan pada lingkungan yang lebih spesifik. *Framework* COBIT bermanfaat untuk membantu menyeimbangkan antara resiko dan investasi pengendalian dalam sebuah lingkungan IT yang sering tidak dapat diprediksi. Tujuan utama COBIT adalah memberikan kebijaksanaan yang jelas dan latihan yang bagus bagi IT Governance bagi organisasi di seluruh dunia untuk membantu memahami dan mengatur

risiko–risiko yang berhubungan dengan TI. *Framework* COBIT 5 dirancang dengan 5 domain yang masing-masing mencakup penjelasan rinci dan termasuk panduan secara luas dan bertujuan sebagai tata kelola dan manajemen TI perusahaan. 5 domain yang ada pada COBIT 5 adalah sebagai berikut.

a. EDM (*Evaluate, Direct and Monitor*)
b. APO (*Align, Plan and Organise*)
c. BAI (*Build, Acquire and Implement*)
d. DSS (*Deliver, Service, and Support*)
e. MEA (*Monitor, Evaluate and Assess*)

3.2 Pekerjaan Lapangan (*Fieldwork*)

Pada tahapan pekerjaan lapangan, kegiatan yang dilakukan peneliti adalah sebagai berikut.

1. Membuat kuesioner

   Peneliti membuat pernyataan pada kuesioner berdasarkan pedoman pada *framework* COBIT 5 yang terkait dengan tata kelola keamanan sistem informasi untuk mencegah terjadinya tindakan *cracking* pada Lampost.

2. Menyebarkan kuesioner

   Peneliti menyebarkan kuesioner kepada bagian IT Lampost sebanyak 6 orang dan redaksi Lampost sebanyak 24 orang yang dilakukan pada tanggal 3-31 Desember 2018 yang digunakan untuk mengukur kapabilitas tata kelola keamanan sistem informasi perusahaan.

3.3 Pelaporan (*Reporting*)

Kegiatan yang dilakukan peneliti pada tahap pelaporan adalah sebagai berikut.

1. Mengukur tingkat kapabilitas

   Merekap pengisian kuesioner untuk menghitung dan mengukur tingkat kapabilitas tata kelola keamanan sistem informasi untuk dijadilan laporan hasil analisis. Tingkat kapabilitas setiap proses yang dinilai dinyatakan dalam level 0 sampai 5.

   a. Level 0 : *incomplete*
   b. Level 1 : *performed*
   c. Level 2 : *managed*
   d. Level 3 : *established*
   e. Level 4 : *predictable*
   f. Level 5 : *optimizing* (ISACA, 2013).

2. Menganalisa *gap /* kesenjangan

   Peneliti menganalisa *gap/*kesenjangan tingkat kapabilitas untuk menemukan permasalahan yang terjadi pada tata kelola keamanan sistem informasi perusahaan.

3.4 Tindak Lanjut (*Follow Up*)

Kegiatan yang dilakukan peneliti pada tahap tindak lanjut adalah sebagai berikut.

1. Merekomendasikan perbaikan tata kelola keamanan sistem informasi

   Dari hasil *gap/*kesenjangan yang terjadi pada tingkat kapabilitas saat ini dan yang diharapkan perusahaan didapatkan temuan masalah yang kemudian akan diberikan rekomendasi perbaikan untuk meningkatkan kapabilitas tata kelola

keamanan sistem informasi perusahaan guna mencegah terjadinya tindakan *cracking* pada *website* Lampost.co.

2. Dokumentasi

   Peneliti melakukan dokumentasi kegiatan penelitian tata kelola keamanan sistem informasi pada Lampost.