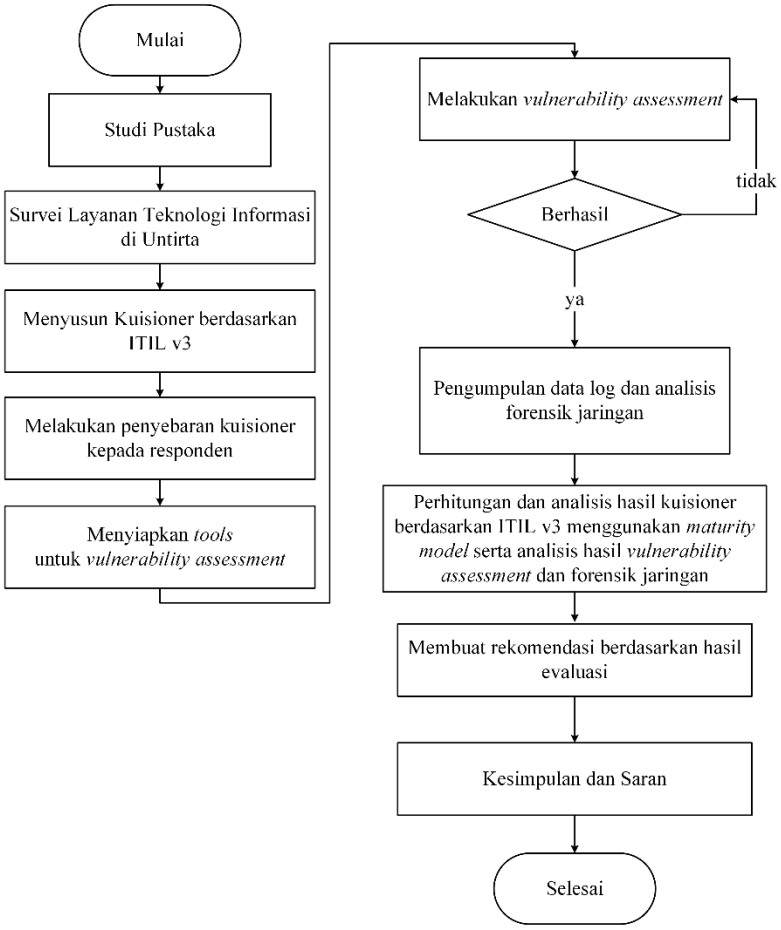
BAB III
METODOLOGI PENELITIAN

3.1 Alur Penelitian

Alur penelitian berisikan diagram alir yang menjelaskan setiap langkah atau metode penelitian dari awal dimulai penelitian hingga akhir. Adapun alur penelitian dalam evaluasi menggunakan *framework* ITIL v3 *service operation* seperti pada Gambar 3.1:



Gambar 3.1 Alur Penelitian

Alur dalam menyelesaikan penelitian ini adalah sebagai berikut:

1. Studi literatur dengan mencari referensi dari jurnal maupun buku yang berkaitan dengan permasalahan pada penelitian. Referensi tersebut berikaitan dengan keamanan IT, *vulnerability assessment*, ITSM, dan kerangka kerja ITIL v3 domain *service operation*.

2. Melakukan survei ke lokasi untuk mengetahui proses layanan teknologi informasi yang terdapat pada UPT Data dan Informasi Untirta.
3. Menyusun kuesioner ITIL v3 menggunakan *template* UCISA *Service Operation*.
4. Menyebar kuesioner ITIL v3 kepada responden UPT Data dan Informasi yang ahli dibidangnya.
5. Menyiapkan *tools* yang akan digunakan untuk *vulnerability assessment*.
6. Melakukan *vulnerability assessment* pada layanan yang telah ditentukan.
7. Mengumpulkan data *log* jaringan dari UPT Data dan Informasi Untirta.
8. Menganalisis hasil dari kuesioner berdasarkan ITIL v3 menggunakan *maturity model*, serta hasil dari *vulnerability assessment* dan forensik jaringan.
9. Membuat rekomendasi berdasarkan hasil dari kuesioner ITIL v3 serta hasil dari *vulnerability assessment* dan forensik jaringan.
10. Membuat kesimpulan, saran, serta rekomendasi dari hasil evaluasi yang telah didapatkan.

3.2 Analisis Forensik Jaringan

Pada analisis forensik jaringan, dilakukan analisis terhadap *log* yang didapatkan saat keadaan normal dan saat serangan terjadi. Analisis *log* juga dilakukan sebagai informasi awal sebelum melakukan *vulnerability assessment* yang akan dilakukan. Analisis *log* dapat memberikan beberapa informasi diantaranya adalah IP a*ddress* penyerang, lokasi penyerang, jenis paket yang terkirim, dan beban CPU.

3.3 *Vulnerability Assessment*

Pada *vulnerability assessment*, dilakukan uji kerentanan terhadap layanan yang terdapat pada UPT Data dan Informasi Untirta. Layanan yang akan dilakukan uji *Vulnerability* adalah SIAKAD Untirta, SPADA Untirta, *website* Untirta, *website* FT Untirta, dan e-Administrasi Untirta. Layanan-layanan tersebut dipilih karena sering digunakan baik sebagai layanan akademik, maupun sebagai layanan penyampaian informasi terkini yang ada di Untirta. *Vulnerability assessment*

menggunakan sebuah laptop dengan sistem operasi Kali Linux. Kali linux merupakan salah satu sistem operasi yang sering digunakan dalam *ethical hacking*. Sistem operasi ini memiliki beberapa *tool* yang berguna untuk mencari informasi dan celah kerentanan pada sebuah jaringan komputer.

Tools yang digunakan untuk *vulnerability assessment* yaitu Nmap dan *Nessus*. Nmap digunakan untuk *network mapping*, mengetahui informasi terkait IP *address server*, *port* yang terbuka, jenis sistem operasi yang digunakan oleh *server*, dan lain sebagainya. Sedangkan Nessus digunakan sebagai alat untuk uji *vulnerability*. Penggunaan aplikasi Nessus dapat memberikan informasi kerentanan yang ada pada layanan teknologi informasi Untirta berdasarkan tingkat kerentanannya. Tingkat kerentanan pada nessus dibagi menjadi 4 level, yaitu *low* yang paling rendah, diikuti *medium, high,* dan *critical* yang paling tinggi.

3.4 Kuesioner ITIL v3 *Service Operation*

Kuesioner dilakukan menggunakan template UCISA ITIL v3 *service operation readiness*. Tingkat maturitas didasarkan pada level yang telah dijelaskan ITIL *maturity model* pada subbab 2.6. Pada penelitian ini hanya difokuskan pada dua sub-domain yaitu *service operation processes,* dan *common service operation activities*. Pertanyaan yang diberikan berjumlah 53 pertanyaan pada sub-domain *service operation processes* dan 28 pertanyaan pada sub-domain *common service operation activities.*

Sub-domain *service operation processes* berisi pernyataan yang berkaitan dengan manajemen seluruh proses yang ada pada *service operation*, yaitu *event management, incident management, request fullfilment, problem management,* dan *access management*. Sementara itu, sub-domain *common service operation activities* berisi pernyataan yang berkaitan dengan aktivitas umum pada penerapan proses dan fungsi yang ada pada *service operation*. Rancangan tabel kuesioner yang akan digunakan dijelaskan pada Tabel 3.1.

Tabel 3.1 Rancangan Kuesioner ITIL *Service Operation*

Sub-Domain							
No.	**Pernyataan**	**Jawaban**					**Keterangan**
		1	**2**	**3**	**4**	**5**	
1.							
2.							
3.							

Rancangan kuesioner pada Tabel 3.1 diberikan beberapa pernyataan terkait domain *service operation*. Kemudian responden akan memberikan nilai 1-5 terhadap pernyataan yang diberikan sesuai dengan keadaan yang dialami saat ini. Setelah itu dilakukan perhitungan *maturity* model untuk menentukan nilai kematangan terhadap layanan operasional UPT Data dan Informasi.

Berdasarkan penelitian sebelumnya, jumlah responden untuk kuesioner ITIL v3 dapat dilakukan serta dinyatakan valid dengan minimal 3 responden yang ahli di bidangya [14]. Pada penelitian ini, kuesioner dilakukan kepada 4 responden ahli di bidangnya. Responden dipilih berdasarkan keahlian mereka di bidang IT serta posisi yang mereka tempati di UPT Data dan Informasi Untirta. Responden kuesioner pada penelitian ini diantaranya adalah

1. Bapak Arry Setiyadi sebagai Kepala Subkoor Jaringan
2. Bapak Permadi sebagai Admin *Server* Untirta
3. Bapak Ramdhan J sebagai Kepala Subkoor Pengembangan Sistem
4. Bapak Firman Riyadhi sebagai Spv. *Engineering* PT. MMD

3.5 Analisis *Maturity Model* dan Kesenjangan

Analisis *maturity* model dilakukan untuk menghitung nilai kematangan manajemen layanan teknologi informasi. Sementara itu, Analisis kesenjangan dilakukan untuk menghitung nilai kesenjangan terhadap nilai yang diharapkan dengan keadaan saat ini.