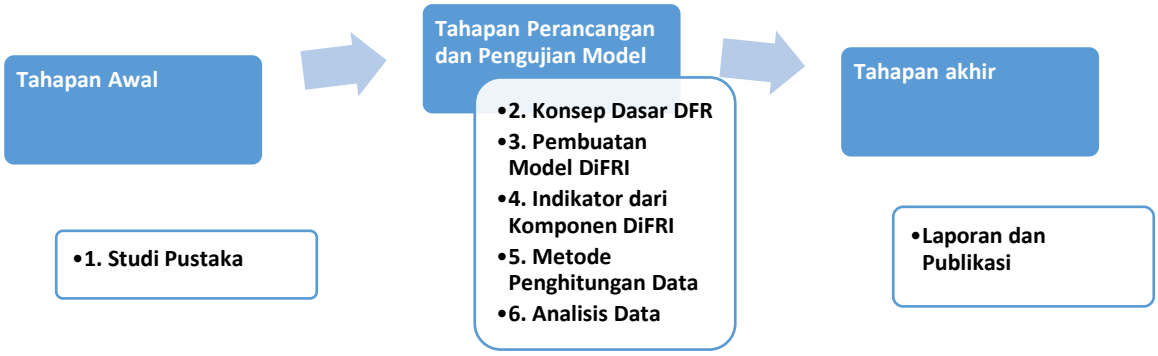
# BAB 3
# Metodologi Penelitian

Bab ini menjelaskan metode-metode yang dilakukan sehingga diketahui dengan jelas dan rinci tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan penelitian ini, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Langkah-langkah tersebut dapat dilihat pada **Gambar 3.1**




Gambar 3.1 Bagan Proses Metodologi Penelitian

## 3.1 Studi Pustaka

Studi pustaka dilakukan terhadap penelitian yang terkait dengan kebijakan keamanan, *digital forensic*, *digital forensic readiness*, tahapan *digital forensic readiness* dan DiFRI agar dapat menunjang tujuan akhir dari penelitian ini.

## 3.2 Konsep Dasar Digital Forensic Readiness (DFR)

Berdasarkan hasil dari *review* beberapa penelitian-penelitian terdahulu yang dapat dilihat pada Tabel 1.1 dan berdasarkan fenomena yang terjadi saat ini, maka komponen utama pada DiFRI mengalami perubahan. Dimana pada model DiFRI yang sebelumnya terdapat 6 komponen utama berubah menjadi 5 komponen utama. Terjadi penggabungan antara komponen *control(Risk)* dan *legality*. Hal ini disebabkan komponen ini merupakan komponen yang sangat penting dan saling terkait, terutama untuk kasus serangan *penanganan insident forensic digital*. 5 komponen utama dari *digital forensic readiness* tersebut, sebagai berikut :

a. *Strategy*. Kesiapan pengguna internet dalam menghadapi *digital forensic* dapat dilihat dari strategi dan rencana yang dibuat pengguna internet karena tanpa strategi dan rencana yang baik, pengguna internet akan mengalami kesulitan dalam menangani masalah serangan penanganan insident forensic digital dan aktifitas-aktifitas lainnya yang berkaitan dengan *digital forensic*. Hal ini dipaparkan oleh (Robert Rowlingson, 2004) dan (Barske et al., 2010).

b. *Policy & Procedure*. Aktifitas yang dilakukan oleh pengguna internet harus berdasarkan pada aturan dan prosedur yang telah ditetapkan. Prosedur ini akan menjadi petunjuk bagi pengguna internet dalam beraktifitas dan berkegiatan di dunia internet. Hal ini dipaparkan oleh (Barske et al., 2010)

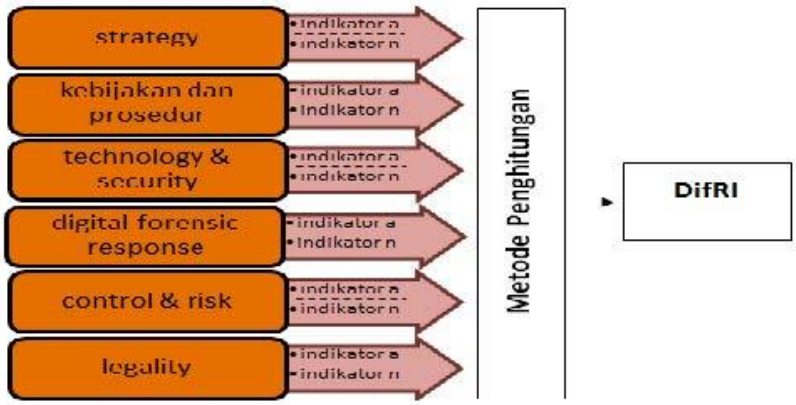
c. *Technology & Security*. Hal ini adalah bagian paling penting ketika akan menerapkan *digital forensic*. Setiap pengguna internet seharusnya memiliki perangkat keras maupun perangkat lunak untuk mencari, mengambil dan melindungi barang bukti digital. Hal ini dipaparkan oleh (Grobler & Louwrens, 2007), (Barske et al., 2010) dan (Mouhtaropoulos et al., 2014).

d. *Digital Forensic Response.* Ketika melakukan aktifitas *digital forensic*, dibutuhkan keahlian dan pengetahuan di bidang *digital forensic*. Hal ini dipaparkan oleh (Barske et al., 2010).

e. *Control(Risk) & Legality*. Dalam hal ini *control* dibutuhkan saat proses penanganan *digital forensic*, dimana dibutuhkan pengawasan atas resiko-resiko yang akan ditimbulkan, agar program *digital forensic readiness* dapat berjalan dengan baik. Hal ini dipaparkan oleh (Robert Rowlingson, 2004) dan (Barske et al., 2010). Dan ini harus diimbangi atau dilengkapi dengan aspek lain, yaitu *legality*, dimana komponen ini menjadi yang paling penting karena semua aktifitas penanganan data digital harus sesuai dengan undang-undang terkait dalam hal ini undang- undang ITE. Agar setiap data dapat digunakan secara sah dimata hukum sebagai barang bukti. Hal ini dipaparkan oleh (Robert Rowlingson, 2004) dan (Mouhtaropoulos et al., 2014).

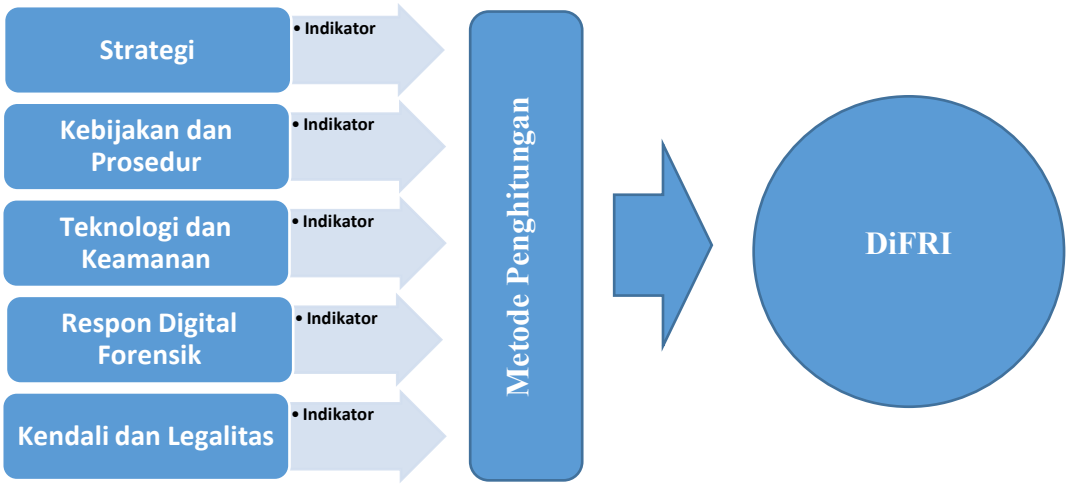
### 3.3 Pembuatan Model DiFRI terhadap Perusahaan PT Waditra Reka Cipta Bandung

Model DiFRI yang akan dibuat ini sebelumnya merupakan pengembangan dari model DiFRI yang dipaparkan oleh (Widodo, 2016) dalam penelitiannya dapat dilihat seperti berikut :




Gambar 3.2 Model DiFRI (Widodo, 2016)

Pengembangan dilakukan berdasarkan telaah dari peneletian-penelitian yang telah ada dan fenomena-fenomena yang terjadi saat ini. Hasil dari pengembangan model DiFRI terlihat dari komponen utama, pada model DiFRI yang dipaparkan oleh (Widodo, 2016) terdapat 6 komponen utama. Sementara berdasarkan telaah penelitian-penelitian yang telah ada sebelumnya dan berdasarkan fenomena yang terjadi saat ini, ada komponen utama yang harus digabung, yaitu penggabungan antara komponen *control* dan *legality*. Hal ini disebabkan komponen ini merupakan komponen yang sejalan dan saling terkait dan tak bisa dipisahkan. Model pengembangan DiFRI terhadap PT Waditra Reka Cipta Bandung dapat dilihat pada gambar 3.3.




Gambar 3.3 Model DiFRI PT Waditra Reka Cipta Bandung

### 3.4 Indikator dari komponen DiFRI

Dari komponen-komponen utama *digital forensic readiness* yang dirumuskan sebelumnya, maka akan disusun indikator-indikator berdasarkan setiap komponen yang ada.

#### 3.4.1 Komponen Strategi

- Program-program Digital Forensic Readiness
- Aturan, regulasi dan kewajiban menyimpan dokumen, file dan rekaman (CCTV, Log, dokumen)
- Ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital
- Identifikasi sumber-sumber dan tipe-tipe yang berbeda dari barang bukti digital organisasi
- Identifikasi teknologi dan Sumber Daya manusia untuk menjamin Digital Forensic Readiness
- Jaminan ketersediaan dana untuk menjalankan dan merawat program Digital Forensic Readiness

#### 3.4.2 Komponen Kebijakan dan Prosedur

- Kebijakan dan prosedur sebagai petunjuk aktifitas dan kegiatan anggota organisasi yang mengunakan TIK
- Sangsi bagi pelanggar kebijakan dan prosedur Digital Forensic Readiness

#### 3.4.3 Komponen Teknologi dan Keamanan

- Jaminan manajemen log dari masing-masing sistem, pemeliharaan, dan pengelolaan
- Manajemen media penyimpanan (CD, hardisk, falshdisk) dari masing-masing komputer dan server
- Ketersediaan perangkat akuisisi dan analisis barang bukti digital, baik berupa hardware (write block protector, dll) maupun software (analisys tool)
- Jaminan keamanan barang bukti, baik secara online maupun offline, melalui imaging maupun penggandaan fisik
- Ketersediaan perangkat pendukung digital forensic seperti cctv, finger print, dan autentikasi sistem
- Ketersediaan perangkat pengamanan sistem seperti firewall, anti virus
- Ketersediaan perangkat pendukung keamanan seperti enkripsi dan kriptografi

### 3.4.4 Komponen Respon Digital Forensik

- Ketersediaan SOP (standard operating procedure) penanganan insiden maupun tindakan digital forensic
- Ketersediaan SDM yang memiliki sertifikasi/keahlian bidang digital forensic
- Tim penanganan cyber crime dan digital forensic response
- Pelatihan-pelatihan SDM mengenai penanganan cyber crime dan digital forensic
- Petunjuk teknis pengaduan maupun pelaporan insiden
- Alat peraga, petunjuk dan arahan mengenai cyber crime berupa poster, banner, dan alat peraga lainya
- Ketersediaan sekretariat pengaduan, informasi dan pelaporan cyber crime

### 3.4.5 Komponen Kendali dan Legalitas

- Sosialisasi tentang digital forensic kepada pegawai instansi.
- Sosialisasi tentang bahaya penanganan insident forensic digital kepada pegawai instansi.
- Pengawasan program digital forensic readiness.
- Pemahaman kepada setiap pegawai mengenai setiap proses digital forensic dan resiko kegagalan setiap prosesnya.
- Pembaharuan perangkat, tool dan sistem secara berkala.
- Kebijakan aspek hukum setiap proses investigasi digital forensic.
- Pemahaman setiap pegawai instansi akan undang-undang ITE.
- Sosialisasi peraturan dan undang-undang ITE.
- Pelatihan penanganan terhadap serangan penanganan insident forensic digital dan proses hukumnya.

## 3.5 Metode Pengumpulan dan Penghitungan Data

Pada penelitian ini, data didapatkan melalui kuesioner yang disebar secara pribadi kepada seluruh karyawan beserta jajaran pimpinan PT Waditra Reka Cipta Bandung yang berjumlah 22 orang dan selanjutnya disebut populasi. Sementara itu sampel yang akan digunakan diperoleh dengan teknik pengambilan *sampling* jenuh karena jumlah populasi yang relatif kecil, kurang dari 30 orang, maka sampel yang digunakan adalah seluruh pegawai beserta jajaran pimpinan dari PT Waditra Reka Cipta Bandung.

Metode penghitungan pada kuesioner ini akan menggunakan skala Linkert dalam proses penghitungan datanya. Skala Linkert adalah skala yang biasa digunakan untuk mengukur persepsi atau pendapat seseorang mengenai sebuah peristiwa atau fenomena sosial. Skala Linkert dipilih karena memiliki interval dalam penilaiannya, hal ini akan membuat nilai yang didapat lebih mendekati dengan keadaan sesungguhnya sehingga pengguna internet dapat melakukan pembenahan dan perbaikan secara baik dan tepat sasaran. Kemudian dari komponen-komponen utama yang ada, akan dilakukan *scoring* untuk menilai aspek DiFRI secara keseluruhan untuk mengetahui *Digital Forensic Readiness Index* terhadap serangan *penanganan insident forensic digital* bagi individu-individu pengguna internet. Rancangan kuesioner pengukuran DiFRI dapat dilihat pada tabel 3.1.

Tabel 3.1 Rancangan Kuesioner

Nama Lengkap : …….

Jabatan/ Jobdesk : …….

*1.* Komponen *Strategy*

| **No.** | **Indikator** | **SS** | **S** | **RG** | **TS** | **STS** |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| n | | | | | | |

*2.* Komponen *Policy & Procedure*

| **No.** | **Indikator** | **SS** | **S** | **RG** | **TS** | **STS** |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| n | | | | | | |

*3.* Komponen *Technology & Security*

| **No.** | **Indikator** | **SS** | **S** | **RG** | **TS** | **STS** |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| N | | | | | | |

*4.* Komponen *Digital Forensic Response*

| No. | Indikator | SS | S | RG | TS | STS |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| N | | | | | | |

*5.* Komponen *Control & Legality*

| No. | Indikator | SS | S | RG | TS | STS |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| n | | | | | | |

Keterangan :

- SS : Sangat Sesuai
- S : Sesuai
- RG : Ragu-ragu
- TS : Tidak Sesuai
- STS : Sangat Tidak Sesuai

Berdasarkan tabel 3.1 akan dilakukan penghitungan atas jawaban-jawaban yang diberikan, kemudian dilakukan *scoring* pada masing-masing komponen dengan menggunakan rumus pada skala Likert. Hasil *scoring* setiap komponen dapat dilihat pada table 3.2 dan hasil *scoring* keseluruhan DiFRI dapat dilihat seperti pada tabel 3.3.

Tabel 3.2 *Scoring* setiap komponen

| No | Indikator | Total Skor | | | | | Jumlah Total Skor | Indeks (%) |
|---|---|---|---|---|---|---|---|---|
| | | SS | S | RG | TS | STS | | |
| 1 | | | | | | | | |
| N | | | | | | | | |
| **Indeks (%) Komponen** | | | | | | | | |

Total skor untuk setiap jawaban dapat dihitung dengan rumus :

$$Total\ Skor = T \times Pn$$

Keterangan :

T : Jumlah Responden.

Pn : Skor Pilihan.

Jumlah Total Skor untuk setiap indikator dapat dihitung dengan rumus :

$$Jumlah\,Total\,Skor = \sum Total\,Skor\,Setiap\,Pilihan$$

Indeks (%) untuk setiap indikator dapat dihitung dengan rumus :

$$Indeks\ (\%)\ Indikator = \frac{Jumlah\ Total\ Skor}{Skor\ Maksimum} \times 100$$

Keterangan :

Skor Maksimum : Nilai tertinggi pilihan dikali jumlah responden.

Indeks (%) setiap komponen dapat dihitung dengan rumus :

$$Indeks\ (\%)\ Komponen = \frac{\sum Indeks\ Indikator}{Jumlah\ Indikator}$$

Tabel 3.3 *Scoring* DiFRI

| No. | Komponen | Indeks (%) |
|---|---|---|
| 1 | | |
| n | | |
| **Nilai DiFRI (%)** | | |

DiFRI akan dihitung berdasarkan besar nilai dari setiap komponen-komponen yang dimiliki, sehingga dapat dirumuskan :

$$DiFRI = \frac{Jumlah\ Indeks\ Semua\ Komponen}{Jumlah\ Komponen}$$

Selanjutnya peneliti membuat skala dan status dari hasil nilai DiFRI (d) yang diperoleh. Hal ini untuk memperjelas hasil dari kesiapan para individu-individu pengguna *internet*. Peneliti membuat 3 kriteria berdasarkan skala tertentu. Ini dapat dilihat pada tabel 3.4.

Tabel 3.4 Skala Kesiapan berdasarkan DIFRI

| No. | Skala | Status |
|---|---|---|
| 1. | $0\% < d \leq 30\%$ | Tidak Siap |
| 2. | $30\% < d \leq 60\%$ | Kurang Siap |
| 3. | $60\% < d \leq 100\%$ | Siap |