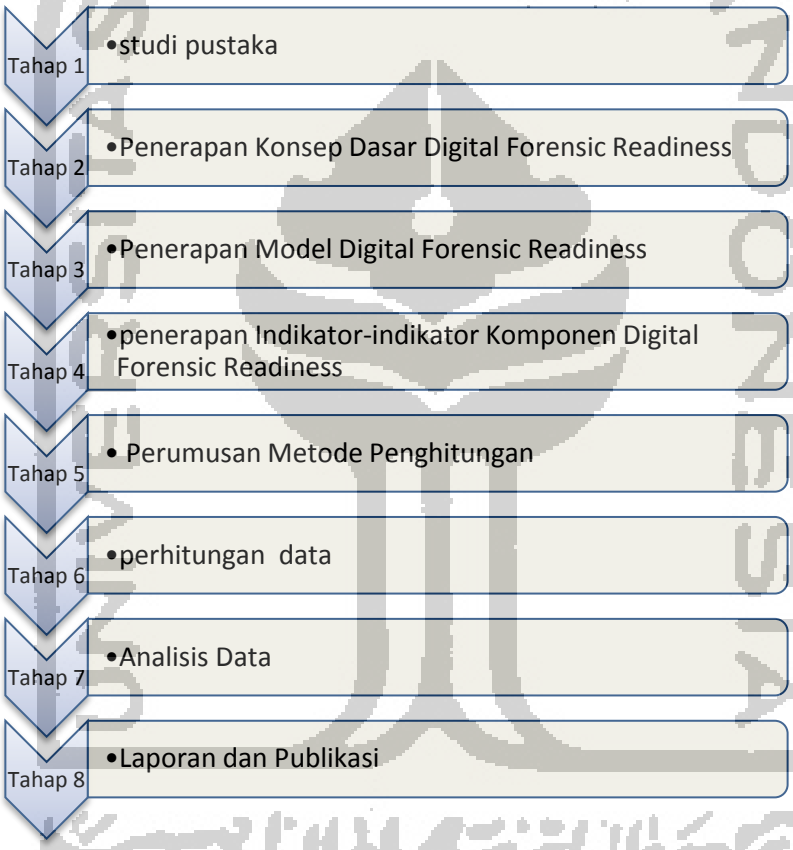
BAB III
METODOLOGI PENELITIAN

Dalam penelitian ini digunakan langkah-langkah dalam menyelesaikan permasalahan. Pembuatan model *Digital forensic readinessIndex* dan pengukuran *Digital forensic readiness*Index menggunakan tahapan-tahapan yang dapat dilihat pada Gambar 5



Gambar 6 Langkah-langkah Penelitian

3.1. Studi Pustaka

Studi pustaka dilakukan untuk memahami teori-teori dan penelitian-penelitian terdahulu mengenai *digital forensic*, *digital forensic readiness*, keamanan sistem informasi, dan aspek hukum dari Digital Forensik untuk menilai*Digital forensic readiness*pada suatu institusi.

3.2. Konsep Dasar Digital *Forensic readiness*

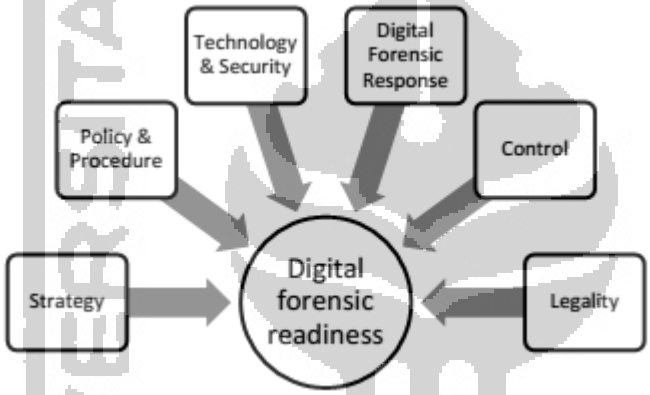
Berdasar studi pustaka dan *review* beberapa penelitian-penelitian sebelumnya, dapat disimpulkan bahwa kriteria utama *digital forensic readiness*tidak dapat terlepas dari beberapa hal, antaralain:

1. *Strategy*. Kesiapan organisasi dalam digital forensik terlihat dari strategi dan perencanaan sebuah organisasi, tanpa rencana dan strategi yang matang, organisasi akan kesulitan menangani kejahatan siber dan aktivitas digital forensik lainya. Pentingnya komponen strategi ini dikemukakan oleh Rowlingson (2004), Bates (2011), dan Barske et al. (2010).
2. *Policy & procedure*. Setiap aktivitas organisasi harus dilandaskan pada kebijakan dan prosedur tertentu yang telah ditetapkan. Prosedur ini akan menjadi dasar dan petunjuk bagi anggota organisasi untuk menjalankan aktivitas dan kegiatan. Untuk menjamin kesiapan organisasi dalam digital forensic, harus ada prosedur yang ditetapkan. Pentingnya komponen *policy & procedure* ini dikemukakan oleh Tan (2001), Bates (2011), Barske et al. (2010), dan Sommer (2012).
3. *Technology & security*, infrastruktur dan keamanan TIK. Untuk mengimplementasikan digital forensik, organisasi harus didukung oleh *hardware* maupun *software* yang digunakan untuk mencari, mengambil, dan melindungi barang bukti digital. Pentingnya komponen *technology & security* ini dikemukakan oleh Grobbler & Lowrens (2007) dan Barske et al. (2010)
4. *Digital forensic response*. Dalam menjalankan tugas maupun aktivitas *digital forensic*, dibutuhkan tenaga-tenaga ahli dan memiliki ketrampilan di bidang digital forensik. Pentingnya Aspek *digitalforensic response* ini dikemukakan oleh Barske et al. (2010).
5. *Control*. Ketika program dan aktivitas pendukung maupun penanganan digital forensik, dibutuhkan pengawasan dan kendali akan resiko-resiko yang ditimbulkan, agar program-program *digitalforensic readiness*dilaksanakan oleh setiap anggota organisasi. Pentingnya

komponen Control ini dikemukakan oleh Rowlingson (2004), dan Barske et al. (2010).

6. *Legality*, yaitu aspek kesesuaian setiap aktivitas/penanganan data digital yang sesuai dengan undang-undang transaksi elektronik. Agar setiap data dapat digunakan secara sah sebagai barang bukti. Pentingnya komponen *legality* ini dikemukakan oleh Tan (2001), dan Rowlingson (2004).

Keenam kriteria tersebut akan mempengaruhi tingkat d*igital forensic readiness* suatu institusi, seperti terlihat pada gambar 6



Gambar 7. Komponen Utama Digital *Forensic readiness*

Selanjutnya detail aspek penilaian masing-masing komponen dapat diketahui pada Tabel 3.1.

Tabel 1 Aspek Masing-masing Digital *Forensic readiness*

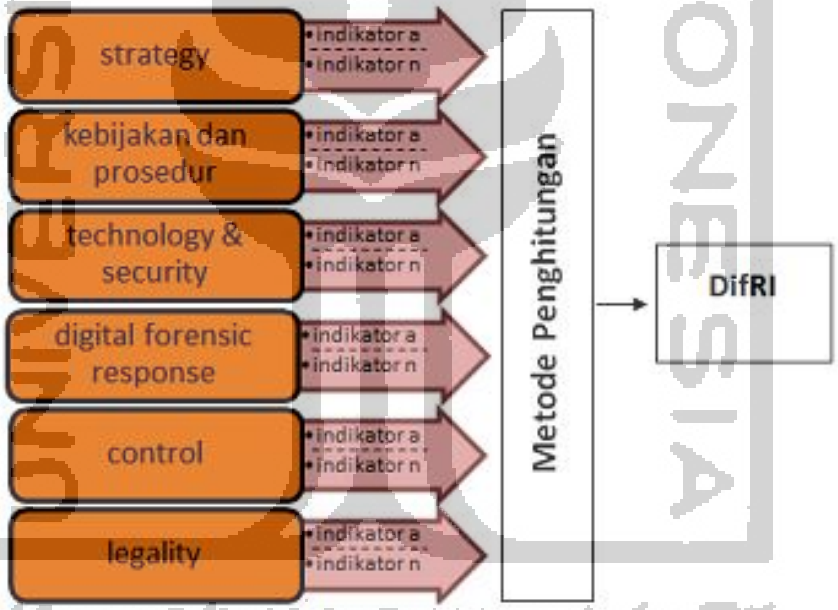
No	Komponen	Aspek
1	*Strategy*	1. Aturan dan regulasi program *Digital forensic readiness* (Barske et al., 2010). 2. Identifikasi teknologi, barang bukti dan SDM (Barske et al, 2010), (Bates, 2011), (Tan, 2001),)(Rowlingson, 2004). 3. Ketersediaan dana (Barske et al., 2010)

2	*Policy & procedure*	1. SOP pemanfaatan TIK dan komponen pendukung (Barske et al., 2010). 2. Kebijakan terkait pengumpulan, perawatan, dan pengamanan barang bukti (Barske et al., 2010), (Tan, 2001), (Sommer, 2012). 3. Pembagian tugas, wewenang dan tanggungjawab (Bates, 2011).
3	*Technology &security*	1. Ketersediaan perangkat penyimpanan/pencatat setiap aktivitas TIK (Barske et al, 2010), (Tan, 2001). 2. Ketersediaan perangkat akuisisi, pengamanan dan analisa barang bukti digital (Barske et al., 2010), (Tan, 2001). 3. Ketersediaan perangkat pengamanan sistem dan TIK (Grobler & Lowrens, 2007).
4	*Digital forensic response*	1. Ketersediaan SOP penanganan insiden, pelaporan, pencegahan dan tindakan *digital forensic* (Barske et al., 2010), (Sommer, 2012), (Tan, 2001) 2. Ketersediaan SDM dan komponen pendukung (tempat dan alat) (Barske et al., 2010)
5	*Control*	Sosialisasi, Pengawasan, evaluasi dan pembahasan program atau tindakan *digital forensic* (Barske et al, 2010), (Rowlingson, 2004)
6	*Legality*	Peninjauan, pemahaman, sosialisasi dan

		pelatihan *Cybercrime*dan *digital forensic* dari sisi hukum (Tan, 2001) (Rowlingson, 2004).

3.3. Model Digital *Forensic readiness* Index (DifRI)

Selanjutnya dari konsep-konsep yang telah dirumuskan, dilakukaneksplorasi lebih lanjut terhadap model tersebut untuk merumuskan model DifRI.Masing-masing komponen di-*breakdown* menjadi sejumlah indikator yangmemberikan informasi/gambaran lebih lengkap dari kriteria/komponen utama.Gambaran model DifRI dapat dilihat pada gambar 7.



Gambar 8 Model DifRI

3.4. Indikator –indikator Komponen Digital *Forensic readiness*

Setelah diketahui komponen-komponen dasar *digital forensic readiness* dan modelnya, selanjutnya disusun indikator-indikator dari komponen-komponen tersebut berdasarkan aspek penilaian setiap komponen.

3.5. Komponen *Strategy*

Komponen yang pertama adalah komponen *strategy*. Dari komponen iniada tiga aspek yang dinilai, antara lain:

a. Aturan dan regulasi program Digital *forensic readiness* (Barske et al.,2010). Indikator aspek ini antara lain:
   1. Program-program Digital *forensic readiness.*
   2. Aturan, regulasi dan kewajiban menyimpan dokumen, file danrekaman (Closed Circuit Televition/CCTV, Log, dokumen).
   3. Ketentuan ketika terjadi peristiwa yang membutuhkan barang buktidigital.

b. Identifikasi teknologi, barang bukti dan SDM (Barske et al., 2010), (Bates,2011), (Tan, 2001),(Rowlingson, 2004). Indikator komponen ini yaitu :
   1. Identifikasi sumber-sumber dan tipe-tipe yang berbeda dari barangbukti digital organisasi.
   2. Identifikasi teknologi dan Sumber Daya manusia untuk menjamindigital *forensic readiness.*

c. Ketersediaan dana (Barske et al., 2010). Indikator aspek ini yaitu:
   Jaminan ketersediaan dana untuk menjalankan dan merawat programdigital *forensic readiness.*

3.6. *Komponen Policy &Procedure*

Komponen kedua adalah kompponen *Policy & Procedure*, dari komponen ini ada tiga aspek yang dinilai, yaitu:

a. SOP pemanfaatan TIK dan komponen pendukung (Barske et al., 2010). Indikator aspek ini yaitu:
   1. Kebijakan dan prosedur sebagai petunjuk aktivitas dan kegiatan anggota organisasi yang mengunakan TIK.
   2. Sangsi bagi pelanggar kebijakan dan prosedur *Digital forensic readiness.*

b. Kebijakan terkait pengumpulan, perawatan, dan pengamanan barang bukti (Barske et al., 2010), (Tan, 2001), (Sommer, 2012). Indikator aspek ini antara lain:
    1. Kebijakan bahwa semua sumber daya informasi dan data merupakan milik organisasi.
    2. Kebijakan dalam keadaan bagaimanakah barang bukti digital dapat diamankan.
    3. Kebijakan barang bukti digital apa saja yang harus diamankan.
    4. Kebijakan yang menyatakan cara dan situasi ketika bukti-bukti yang telah diamankan oleh organisasi dapat dilepaskan kepada pihak di luar organisasi, termasuk ketika harus dirujuk ke penegak hukum.

c. Pembagian tugas, wewenang dan tanggungjawab (Bates, 2011). Indikator aspek ini yaitu:
    1. Kebijakan pembagian wewenang, tugas dan tanggungjawab terkait pengumpulan barang bukti digital, pemeliharaan dan pemeriksaanya

3.7. *Komponen Technology & Security*

Komponen ketiga adalah komponen *technology &Security*. Dari komponen ini ada tiga aspek yang dinilai, yaitu:

a. Ketersediaan perangkat penyimpanan/pencatat setiap aktivitas TIK (Barske et al., 2010), (Tan, 2001). Indikator aspek ini antara lain:
    1. Jaminan manajemen log dari masing-masing sistem, pemeliharaan, dan pengelolaan.
    2. Manajemen media penyimpanan (CD, *hardisk, falshdisk*) dari masingmasing komputer dan *server*.

b. Ketersediaan perangkat akuisisi, pengamanan dan analisa barang bukti digital (Barske et al., 2010), (Tan, 2001). Indikator aspek ini yaitu:
    1. Ketersediaan perangkat akuisisi dan analisis barang bukti digital, baik berupa hardware (*write block protector*, dan lain-lain) maupun software (*analisys tool*).

c. Ketersediaan perangkat pengamanan sistem dan TIK (Grobler & Lowrens, 2007). Indikator aspek ini yaitu:

1. Jaminan keamanan barang bukti, baik secara *online* maupun *offline*, melalui imaging maupun penggandaan fisik.
2. Ketersediaan perangkat pendukung digital forensic seperti cctv, *finger, print*, dan autentikasi sistem.
3. Ketersediaan perangkat pengamanan sistem seperti *firewall*, *anti virus.*
4. Ketersediaan perangkat pendukung keamanan seperti enkripsi dan kriptografi.

3.8. *Komponen Digital Forensic Response*

Komponen keempat adalah *digital forensic response*, dari kemponen ini aspek yang dinilai yaitu:

a. Ketersediaan SOP penanganan insiden, pelaporan, pencegahan dan tindakan *digital forensic* (Barske et al., 2010), (Sommer, 2012), (Tan, 2001). Indikator aspek ini adalah

   Ketersediaan SOP (*standard operating procedure*) penanganan insiden maupun tindakan digital forensik.

b. Ketersediaan SDM dan komponen pendukung (tempat dan alat) (Barske et al., 2010). Indikator untuk aspek ini adalah

1. Ketersediaan SDM yang memiliki sertifikasi/keahlian bidang digital forensik.
2. Tim penanganan *Cybercrime*dan digital *forensicresponse*
3. Pelatihan-pelatihan SDM mengenai penanganan *Cybercrime*dan digital forensi.
4. Petunjuk teknis pengaduan maupun pelaporan insiden.
5. Alat peraga, petunjuk dan arahan mengenai *Cybercrime*berupa poster, banner, dan alat peraga lainya.
6. Ketersediaan sekretariat pengaduan, informasi dan pelaporan *cyber crime.*

3.9. *Komponen Control*

Komponen yang kelima adalah komponen kontrol, dari komponen ini yangdinilai adalah aspek Sosialisasi, Pengawasan, evaluasi dan pembahasan programatau tindakan digital forensic (Barske et al., 2010), (Rowlingson, 2004). Sehinggaindikator komponen control antra lain:

1. Pengawasan program digital *forensic readiness.*
2. Evaluasi secara berkala program digital *forensic readiness.*
3. Sosialisasi program digital forensic kepada anggota organisasi.
4. Pemahaman pada anggota setiap proses digital forensic dan resikokegagalan setiap proses.
5. Pembaharuan perangkat, tool, dan sistem secara berkala.
6. Pembahasan hasil investigasi maupun publikasi hasil investigasikepada kepala-kepala departemen/sub bagian.

3.10. *Komponen Legality*

Komponen kelima yaitu komponen *legality*. Dari komponen ini dinilai aspek yang dinilai yaitu Peninjauan, pemahaman, sosialisasi dan pelatihan *cybercrime*dan *digital forensic* dari sisi hukum (Tan, 2001) (Rowlingson, 2004). Sehingga indikator komponen ini antara lain:

1. Kebijakan peninjauan aspek hukum setiap proses investigasi *digital forensic* dan insiden.
2. Keterlibatan penegak hukum, ahli, auditor profesional dalam evaluasi digital forensic atau *Cybercrime*pada organisasi.
3. Pemahaman setiap anggota institusi akan undang-undang transaksi elektronik dan data digital.
4. Sosialisasi peraturan dan undang-undang transaksi elektronik dan data digital.
5. Pelatihan penanganan *Cybercrime*dan proses hukum.
6. Identifikasi kebijakan-kebijakan untuk menjamin pengumpulan barang bukti sesuai dengan legalitas hukum yang ada.

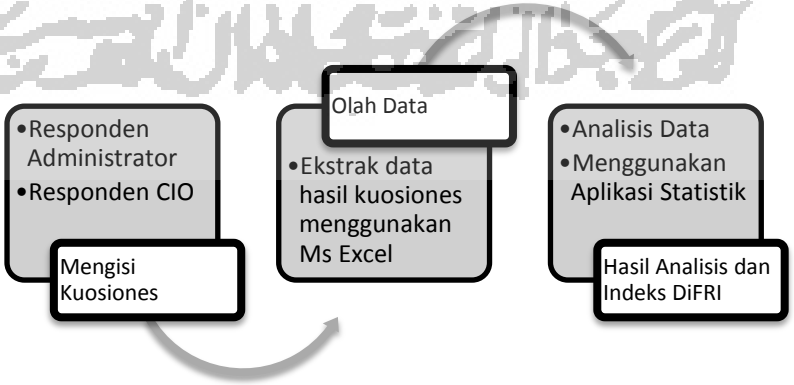
3.11. Metode Pengumpulan Data

Pada penelitian DifRI ini, data akan didapatkan melalui kuesioner.Kuesioner tersebut merupakan model DifRI yang telah dirancang. Setiap direktur/CIO, administrator dan responden akan mengisi kuesioner yang telah disediakan,selanjutnya dilakukan analisis pada data tersebut. Pada penelitian ini populasipenelitian adalah 30 orang, yang meliputi instansi pemerintahan di Kabupaten Banyumas dan teknik pengambilansampel yang digunakan adalah sampling jenuh, yaitu teknik penentuan sampelyang dilakukan bila jumlah populasi relatif kecil, kurang dari 30 orang, ataupenelitian yang ingin membuat generalisasi dengan kesalahan yang sangat kecil(Sugiyono, 2012). Artinya pada penelitian ini sampel adalah seluruh anggotapopulasi, sehingga jumlah sampel adalah 20 orang karyawan di instansi pemerintahan Kabupaten Banyumas.

Menurut Derick Bates (2011), pelaku utama yang berkewajiban danbertanggungjawab dalam pelaksaaan dan kebijakan Digital *forensic readiness*adalah:

1. Direktur eksekutif.
2. Kepala bagian/bidang.
3. Administrator bagian/bidang.
4. Kepala bidang keamanan informasi.
5. Staff bagian/bidang.

Adapun alur proses pengumpulan data seperti terlihat pada gambar 3.4.



Gambar 9 Alur Pengisian Data

3.12. Metode Penghitungan Data

Penelitian ini bersifat evaluatif. Penelitian ini diharapkan menjadi modelevaluasi DifRI dari institusi/organisasi dengan menggunakan analisis statistik yang sesuai.

Pada kuisioner, skala yang digunakan adalah skala Guttman, yaitu skalapengukuran dengan jawaban tegas, antara "ya-tidak". Dipilih skala Guttmankarena digunakan untuk membandingkan antara model DifRI yang dirancangdengan realita yang ada atau terjadi pada suatu organisasi, sehingga organisasidapat melakukan pembenahan dan perbaikan secara tepat sasaran. Selanjutnya,dari enam komponen di atas akan dilakukan scoring untuk menilai aspek DifRIsecara keseluruhan untuk mengetahui digital *forensic readinessIndex* suatuorganisasi.

Contoh kuisioner pengukuran DifRI dapat dilihat pada tabel 2.

Tabel 2 Rancangan Kuosioner

Nama Instansi Pemerintahan : .....

Jabatan : .....

No	**Sub Komponen**	**Jawaban**	
1		Ada	Tidak

Dari kuisioner pada tabel 2, kemudian akan dilakukan penghitungan atas jawaban "Ada" dan "Tidak", selanjutnya dilakukan *scoring* pada masing-masingaspek dengan menggunakan rumus. Hasil *scoring* masing-masing komponentersebut dan DifRI seperti terlihat pada tabel 3.

Tabel 3 Penentuan Skor DifRIInstansi Pemerintahan

No	**Nama Instansi**	**Skor Aspek Pada Komponen 1**	**Skor Aspek Pada Komponen 2**	**Skor Aspek Pada Komponen n**	**Skor Keseluruhan DifRI**
1	Instansi Pemerintahan 1				

DifRI akan dinilai berdasarkan besar nilai dari masing-masing komponen,sehingga didapatkan rumus DifRI yaitu :

DifRI = 1/6 indeks komponen strategy

+ 1/6 indeks komponen *policy & procedure*

+ 1/6 indeks komponen *technology & security*

+ 1/6 indeks komponen digital *forensic response* (1)

+ 1/6 indeks komponen *control*

+ 1/6 indeks komponen *legality*

Selanjutnya besar indeks untuk masing-masing komponen dihitungmenggunakan rumus :

$$I_A = \frac{\sum_{k=1}^{n} A}{n_A} . 10 \quad (2)$$

I_A merupakan indeks dari masing-masing aspek, selanjutnya A merupakanjumlah indikator yang bernilai ”ada”, dan nA adalah total dari indikator padakomponen tersebut. Karena nilai indeks pasti akan selalu bernilai 0≤IA≤1, makadigunakan perkalian 10, yang dimaksudkan untuk mendapatkan skala dari 0sampai dengan 10.

3.13. Skala Tingkat DifRI

Untuk memberikan rekomendasi dan kejelasan status institusi, dibuatlahskala dan status untuk masing-masing nilai DifRI (i), peneliti membuat tigakriteriaberdasarkan skala tertentu, seperti terlihat pada Tabel 4.

Tabel 4 Skala Kesiapan Instansi Pemerintahan berdasarkan DifRI

No	Range/Skala	Status
1	$6 < i \leq 10$	Siap
2	$3 < i \leq 6$	Kurang Siap
3	$0 \leq i \leq 3$	Tidak Siap

Dari skala tersebut mencerminkan keadaan dan status suatu institusi darisegi digital *forensic readiness*. Adapun detail penjabaran masing-masing statusadalah

1. Siap. Status ini merupakan nilai tertinggi bagi istitusi dalam hal digital*forensic readiness*, dari status ini dapat diketahui bahwa sebuah institusimemiliki keenam komponen yang menjadi kriteria digital *forensic readiness* dan mengimplementasikan indikator-indikatornya secaraoptimal. Sehingga institusi siap untuk mengantisipasi, menghadapi, danmenindaklanjuti aktivitas *Cybercrime* pada ranah hukum. Dalam status iniinstitusi direkomendasikan untuk selalu menjaga komponen *control*&*risk*. Dengan menjaga komponen ini, komponen-komponen lainya akantetap terjaga.
2. Kurang Siap. Status ini memberikan gambaran bahwa institusi belummemiliki beberapa komponen/kriteria dari komponen digital *forensic readiness* dan belum mengimplementasikan banyak indikator darikomponen yang ada. Pada kondisi seperti ini, institusi akan sangat mudahmenjadi korban *Cybercrime* dan akan kesulitan mendapatkan barang buktidigital ketika terkena serangan *Cybercrime*. Dalam status ini, institansi direkomendasikan untuk melakukan evaluasi dan pembenahan secaraintens terhadap komponen dan indikator yang belum dimiliki
3. Tidak siap. Pada status ini, institusi hanya memiliki satu atau duakomponen digital *forensic readiness*, itupun hanya dengan beberapaindikator saja. Dalam keadaan seperti ini, institusi akan rentan terkena*Cybercrime*, selain itu institusi juga tidak mampu menghadapi ataupunmenindaklanjuti tindakan *Cybercrime*. Dalam status ini, institusidiharapkan berkoordinasi dengan setiap anggota institusi, untukmerumuskan kembali komponen-komponen digital *forensic readiness* dariawal, agar dapat dibenahi secara bertahap dan berkelanjutan.