Kerangka Kerja *Digital Forensic Readiness* pada Sebuah Organisasi (Studi Kasus : PT Waditra Reka Cipta Bandung)

Asep Sudirman
14917205

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Teknik Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2019

Lembar Pengesahan Pembimbing

Kerangka Kerja Digital Forensic Readiness pada Sebuah Organisasi
(Studi Kasus : PT Waditra Reka Cipta Bandung)

Asep Sudirman
14917205

Yogyakarta, September 2019

Pembimbing

Dr. Bambang Sugiantoro, M.T.

Lembar Pengesahan Penguji

Kerangka Kerja *Digital Forensic Readiness* pada Sebuah Organisasi
(Studi Kasus : PT Waditra Reka Cipta Bandung)

Asep Sudirman
14917205

Yogyakarta, September 2019

Tim Penguji,

{Dr. Bambang Sugiantoro, M.T.}
Ketua Penguji

{Dr. Imam Riadi, M.Kom.}
Penguji I

{Ahmad Rafie Pratama, ST., MIT., Ph.D.}
Penguji II

Mengetahui,
Ketua Program Studi Teknik Informatika Program Magister
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Kerangka Kerja *Digital Forensic Readiness* pada Sebuah Organisasi (Studi Kasus : PT Waditra Reka Cipta Bandung)

Digital Forensic telah berkembang saat ini, tetapi masih memerlukan adanya suatu kerangka kerja sistemik untuk menentukan seberapa siapkah suatu organisasi dalam melakukan Forensik Digital. Penelitian mengenai kesiapan forensik digital sebuah organisasi masih minim, untuk itu perlu dilakukannya suatu penelitian supaya bisa mengidentifikasi faktor-faktor yang berkontribusi terhadap kesiapan forensik digital yang nantinya bisa diukur dan setelah dihitung akan menghasilkan sebuah nilai yang disebut *Digital Forensic Readiness Index*(DiFRI). Suatu organisasi perlu membuat kebijakan keamanan untuk melindungi aset informasi yang secara prinsip berisi berbagai cara yang perlu dilakukan untuk mengontrol, manajemen, mekanisme, prosedur dan tata cara mengamankan sebuah informasi tersebut. indikator yang akan dicoba dibahas masing-masing komponen yakni komponen strategi, kebijakan dan prosedur, teknologi dan keamanan, kendali dan legalitas terhadap suatu insiden *digital forensic* pada suatu organisasi. Pengumpulan dan penghitungan data pada hasil pengolahan kuesioner ini menggunakan skala Linkert yang biasa digunakan untuk mengukur persepsi atau pendapat seseorang mengenai sebuah peristiwa atau fenomena sosial. Berdasarkan hasil dari statistik terkait *handling incident* diketahui bahwa layanan TI merupakan salah satu sasaran yang diincar untuk dijadikan obyek serangan siber, dikarenakan tidak adanya kebijakan terkait dengan DFR di lingkungan perusahaan tersebut. Dengan adanya kebijakan DFR suatu organisasi dapat mengefisiensikan proses penanganan apabila terjadi insiden terhadap layanan TI. Berdasarkan hal tersebut, pada penelitian ini akan dilakukan perancangan kebijakan DFR khusus untuk layanan TI di PT Waditra Reka Cipta Bandung, karena saat sebuah insiden tidak tertangani dengan baik, maka akan memengaruhi dan menghambat proses bisnis dari masing-masing unit kerja yang menggunakan serta menyediakan layanan TI di PT Waditra Reka Cipta Bandung ini. Kebijakan ini diharapkan dapat dijadikan sebagai bentuk prosedural apabila terjadi *cyber crime* di Perusahaan.

Kata kunci

Digital Forensic, kerangka kerja, kesiapan digital forensic, difri, linkert

Abstract

Digital Forensic Readiness Framework for Organizations
(*Case Study*: PT Waditra Reka Cipta Bandung)

Digital Forensic has evolved at this time, but it still needs a systemic framework to determine how prepared an organization is in conducting Digital Forensics. Research on the digital forensic readiness of an organization is still minimal, for this reason it is necessary to conduct a study in order to identify the factors that contribute to digital forensic readiness which can later be measured and after being calculated will produce a value called the Digital Forensic Readiness Index (DiFRI). An organization needs to create a security policy to protect information assets that in principle contains various ways that need to be done to control, management, mechanisms, procedures and procedures for securing such information. the indicators that will be tried are discussed in each component, namely the components of strategy, policy and procedure, technology and security, control and legality of a digital forensic incident in an organization. Data collection and calculation on the results of the processing of this questionnaire uses the Linkert scale which is commonly used to measure a person's perception or opinion regarding an event or social phenomenon. Based on the results of statistics related to incident handling it is known that IT services are one of the targets targeted to be the object of cyber attacks, due to the absence of policies related to DFR in the corporate environment. With the DFR policy an organization can streamline the handling process in the event of an incident on IT services. Based on this, in this research a DFR policy design will be conducted specifically for IT services at PT Waditra Reka Cipta Bandung, because when an incident is not handled properly, it will affect and hinder the business processes of each work unit that uses and provides services IT at PT Waditra Reka Cipta Bandung. This policy is expected to be used as a procedural form in the event of cyber crime in the Company.

Keywords
Digital Forensic, frameworks, digital forensic readiness, diffri, linkert

Pernyataan Keaslian Tulisan

Dengan ini Penulis menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini Penulis juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, September 2019

Asep Sudirman, S.T.

Daftar Publikasi

Tidak ada publikasi yang menjadi bagian dari tesis.

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

Alhamdulilah, Puji dan Syukur Penulis panjatkan kepada Allah Subhanahu Wata'ala, atas segala Rahmat, kesehatan serta kesempatan dalam menyelesaikan tugas akhir tesis ini dengan segala kelebihan dan kekurangannya. Terimakasih Ya Rabb, karena sudah menghadirkan orang-orang berarti disekeliling Penulis, Yang selalu memberi semangat, dukungan juga do'a, sehingga tesis ini dapat terselesaikan.

Sebagai wujud rasa terima kasih atas pengorbanan dan jerih payah kalian sehingga Penulis dapat menggapai cita-cita dan menyelesaikan karya yang sederhana ini, serta lulus menempuh studi S2 (pasca sarjana) di Fakultas Teknik & Industri Universitas Islam Indonesia Jurusan Forensika Digital … maka Penulis persembahkan untuk kalian :

Ayahanda (Saep), **Ibunda** (Saminah) dan tak lupa untuk **Adik** (Neng Sarmilah) tercinta … Apa yang Penulis dapatkan hari ini, belum mampu membayar semua kebaikan, keringat, air mata serta pengorbanan kalian. Terima kasih atas segala dukungan kalian, baik dalam bentuk materi maupun moril. semoga karya ini dapat membahagiakan kalian.

Istriku (Dini Nurhasanah, A.Md.) Tersayang, atas segala motivasi, perhatian dan do'a nya serta kesabaran menunggu di rumah selama beberapa waktu.

Buah hatiku (Lisana Shidqin 'Aliyya dan Syakira Awwaha) kalian berdua adalah penyemangat ayah, semoga kalian menjadi anak yang shalehah dan berakhlak mulia.

Dosen Pembimbing (Bapak Dr. Bambang Sugiantoro, M.T. sebagai dosen pembimbing 1 dan Bapak Yudi Prayudi, S.Si., M.Kom. sebagai dosen pembimbing 2 yang paling memotivasi saya) terima kasih karena sudah menjadi orang tua kedua Penulis di Kampus. Terima kasih atas bantuannya, nasehatnya, dan ilmunya yang selama ini dilimpahkan pada Penulisdengan rasa tulus dan ikhlas.

Dosen Penguji (Bapak Dr. Bambang Sugiantoro, M.T., Bapak Yudi Prayudi, S.Si., M.Kom., Bapak Fietyata Yudha, S.Kom., M.Kom., Bapak Dr. Imam Riadi, M.Kom. dan Bapak Ahmad Rafie Pratama, ST., MIT., Ph.D) yang telah mengevaluasi hasil tesis serta mengevaluasi hasil sidang saya yang masih banyak kekurangannya.

Kaprordi FTI Program Magister (Ibu Izzati Muhimmah, S.T., M.Sc., Ph.D. yang selalu mengingatkan dan memberikan arahan-arahan kepada kami mahasiswanya.

Staff Prodi FTI Program Magister yang tidak bisa saya sebutkan satu persatu

Sahabat dan seluruh **Teman** di kampus tercinta

Tanpa kalian mungkin masa-masa kuliah ini akan menjadi biasa-biasa saja, Penulis memohon maaf atas semua kesalahan saat kita bersama dikelas maupun saat dilingkungan kampus. Terima kasih untuk support yang luar biasa, sampai Penulisbisa menyelesaikan tesis ini.

Kata Pengantar

Alhamdulilah, Puji dan Syukur kupanjatkan kepada Allah Subhanahu Wata'ala, atas segala Rahmat, kesehatan serta kesempatan dalam menyelesaikan tugas akhir tesis ini dengan segala kelebihan dan kekurangannya. Terimakasih Ya Rabb, karena sudah menghadirkan orang-orang berarti disekeliling saya, Yang selalu memberi semangat, dukungan juga do'a, sehingga tesis Penulis ini dapat terselesaikan.

Sebagai wujud rasa terima kasih atas pengorbanan dan jerih payah kalian sehingga Penulis dapat menggapai cita-cita dan menyelesaikan karya yang sederhana ini, serta lulus menempuh studi S2 (pasca sarjana) di Fakultas Teknik & Industri Universitas Islam Indonesia Jurusan Forensika Digital ini … maka Penulis persembahkan untuk kalian :
Dengan memanjatkan puji syukur kehadirat Tuhan Yang Maha Esa atas karunia dan rahmat-Nya, kami dapat menyusun karya tulis ilmiah yang berjudul "Upaya Pencegahan Dampak Global Warming" dengan lancar.

Adapun maksud penyusunan karya tulis ini untuk memenuhi tugas bahasa Indonesia. Rasa terima kasih kami tidak terkirakan kepada yang terhormat Ibu Dra. Lusi Hidayati selaku pembimbing materi dalam pembuatan karya tulis ini, serta semua pihak yang telah mendukung dalam penyusunan karya tulis ini yang tidak bisa kami sebutkan satu persatu.

Harapan kami bahwa karya tulis ini dapat bermanfaat bagi para pembaca untuk menambah wawasan dan pengetahuan tentang pentingnya upaya pencegahan dampak global warming.

Kami menyadari bahwa karya tulis ini masih jauh dari sempurna dengan keterbatasan yang kami miliki. Tegur sapa dari pembaca akan kami terima dengan tangan terbuka demi perbaikan dan penyempurnaan karya tulis ini.

Yogyakarta, September 2019

Penulis

Asep Sudirman

Daftar Isi

Daftar Tabel

Daftar Gambar

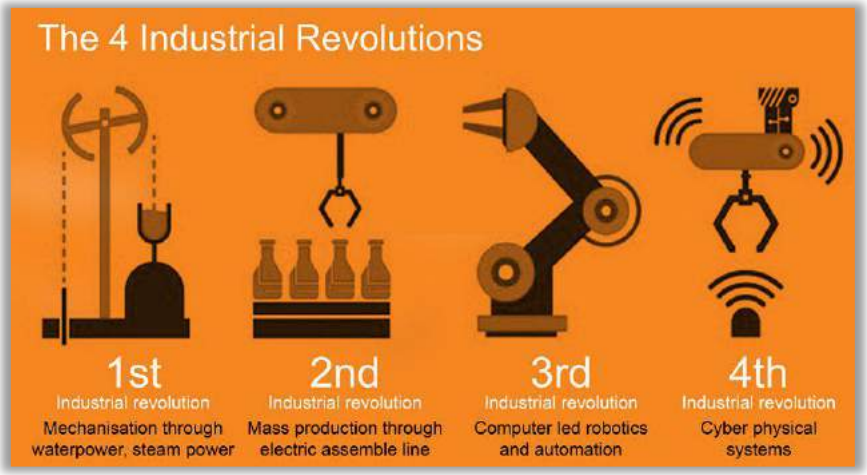
Glosarium

TI	- Teknologi Informasi (istilah umum untuk teknologi apa pun yang membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi)
DFR	- Digital Forensic Readiness (Suatu tingkat kesiapan akan forensic digital)
PT	- Perseroan Terbatas (suatu badan hukum untuk menjalankan usaha yang memiliki modal terdiri dari saham-saham, yang pemiliknya memiliki bagian sebanyak saham yang dimilikinya.
WRC	- Waditra Reka Cipta Bandung (Perusahaan IT Management Services & Software Developer)
IT	- Information Technology (TI dalam bahasa Inggris)

BAB 1
Pendahuluan

1.1 Latar Belakang Masalah

Adanya dorongan pemerintah untuk melaksanakan standar industri 4.0 yang mencakup penggunaan perangkat Internet Of Think (IoT) sebagai salahsatunya, hal tersebut secara tidak sadar sudah menjadi bagian dari kehidupan kita sehari-hari, adanya Peraturan Baru, meningkatnya Serangan Dunia Maya maupun meningkatnya Ketergantungan Aset Digital IT (Rahardjo, 2019) telah menyebabkan Peran adanya Forensik Digital pada Sebuah Organisasi agar lebih diperhitungkan. Oleh karena itu, Sebuah Organisasi harus siap secara Forensik Digital untuk memaksimalkan potensi mereka dalam merespon peristiwa Cyber Crime dan dapat dengan tepat menunjukkan identifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital serta bagaimana faktor-faktor ini bekerja bersama untuk mencapai kesiapan Forensik Digital dalam suatu organisasi.

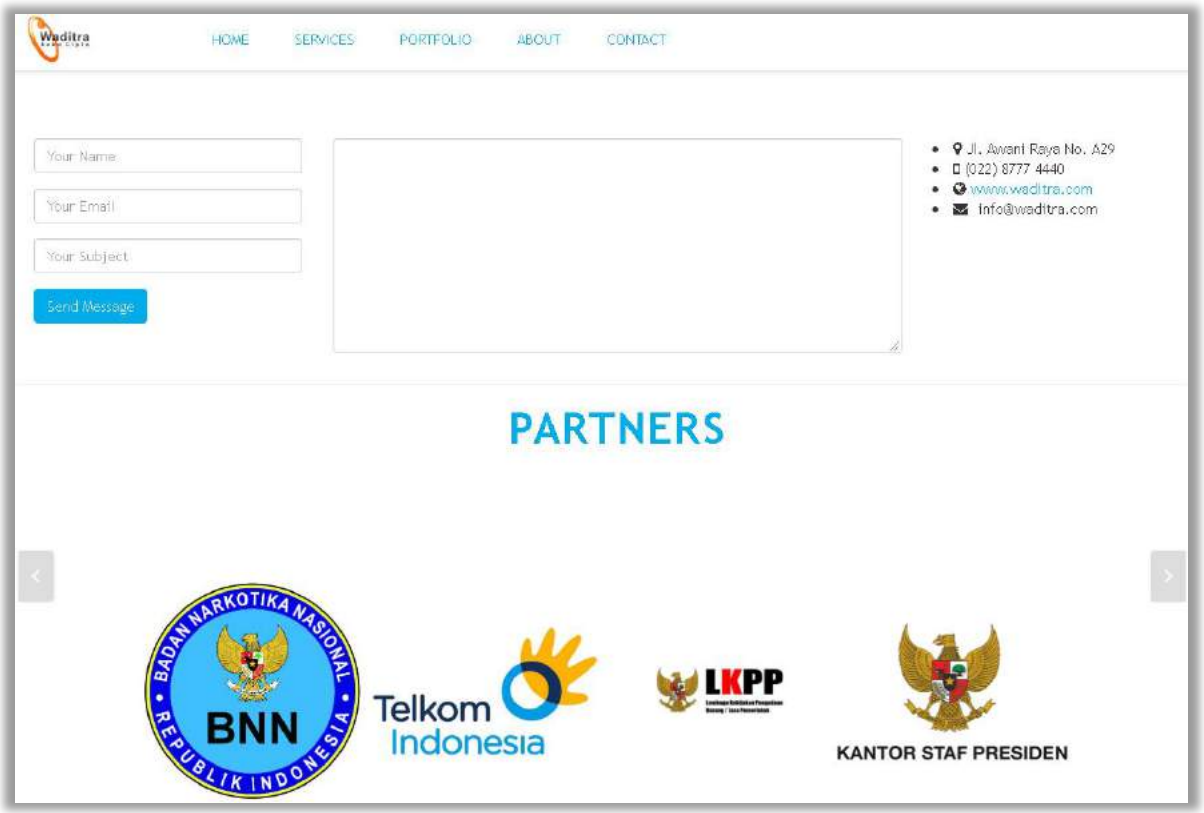


Gambar 1.1 Ilustrasi Perkembangan Industri

Meskipun Digital Forensik telah berkembang saat ini dalam menyelesaikan kasus-kasus Cyber Crime seperti carding, hacking, cracking, defacing, phising, spamming serta kejahatan lainnya yang berbasis digital, tetapi masih memerlukan adanya suatu standar yang sistemik untuk menentukan seberapa siapkah suatu organisasi dalam melakukan Forensik Digital.

Namun, untuk penelitian mengenai kesiapan forensik digital sebuah organisasi masih minim. Untuk itu perlu dilakukannya suatu penelitian supaya bisa mengidentifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital yang nantinya bisa diukur dan setelah dihitung akan mengahasilkan sebuah nilai yang disebut *Digital Forensic Readiness Index*(DiFRI).

PT Waditra Reka Cipta Bandung adalah Salahsatu Konsultan IT yang berkedudukan di Kabupaten Bandung Barat yang menyediakan layanan solusi IT (mengkhususkan pada pengembangan perangkat lunak beserta implementasi dan Tata Kelola sistem informasi/ teknologi informasi) bagi beragam kebutuhan pelanggan di berbagai industri dan jasa. Perusahaan ini mempunyai komitmen untuk menjadi mitra terpercaya bagi pelanggan dan membantu mereka dalam upaya mencapai target bisnisnya melalui penyediaan solusi IT. Serta mempunyai tujuan untuk memberikan kualitas layanan yang tinggi pada setiap proyek pekerjaan yang ditangani.

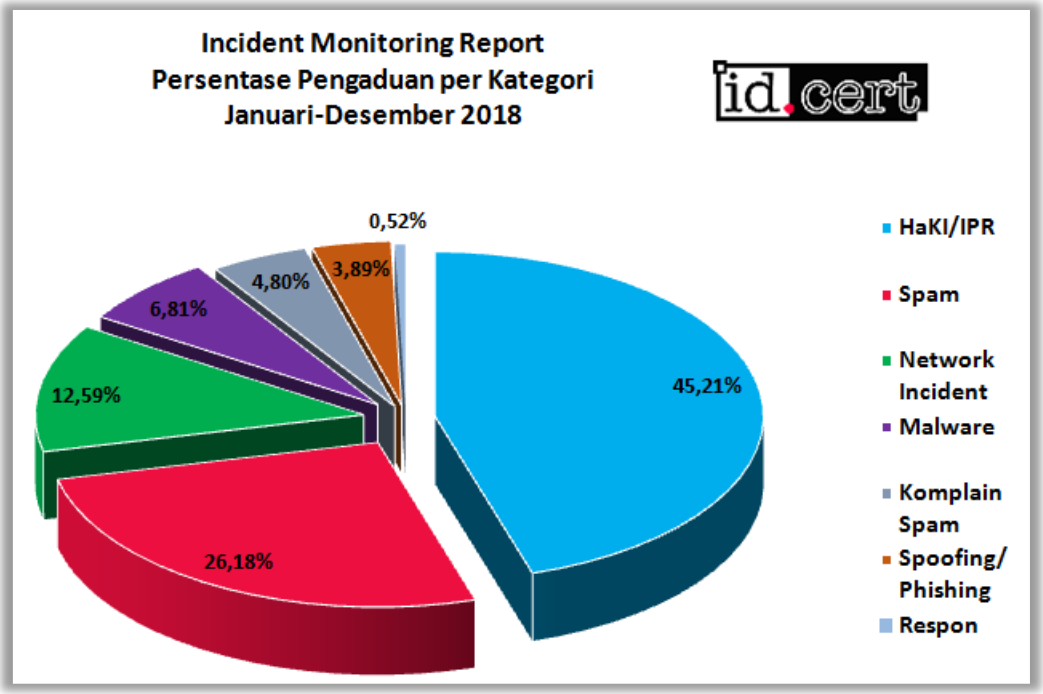


Gambar 1.2 Website PT Waditra Reka Cipta bandung

Berdasarkan hasil dari statistik terkait *handling incident* diketahui bahwa layanan TI merupakan salah satu sasaran yang diincar untuk dijadikan obyek serangan siber (ID-CERT,

2018). Dengan adanya kebijakan DFR, PT WRC Bandung dapat mengefisiensikan proses penanganan apabila terjadi insiden terhadap layanan TI. Namun, sampai sekarang belum terdapat kebijakan terkait dengan DFR di lingkungan perusahaan.

Berdasarkan hal tersebut, pada penelitian ini akan dilakukan perancangan kebijakan DFR khusus untuk layanan TI di PT WRC bandung. Hal ini dikarenakan, saat sebuah insiden tidak tertangani dengan baik, maka akan memengaruhi dan menghambat proses bisnis dari masing-masing unit kerja yang menggunakan serta menyediakan layanan TI di PT WRC Bandung ini. Selain itu kebijakan ini dapat dijadikan sebagai bentuk prosedural apabila terjadi *cyber crime* di Perusahaan.



Gambar 1.3 Incident Monitoring ID-CERT Tahun 2018

Perancangan kebijakan DFR pada PT WRC Bandung ini menggunakan pengembangan dari model DiFRI (Digital Forensic Readiness Index) yang dikemukakan oleh (Widodo, 2016)

1.2 Rumusan Masalah

Berdasar latar belakang dapat ditarik suatu rumusan masalah pada penelitian ini yakni "Bagaimana menerapkan kebijakan *Digital Forensic Readiness* (DFR) untuk layanan TI pada PT Waditra Reka Cipta Bandung?".

1.3 Tujuan Penelitian

Berdasarkan rumusan yang dibuat maka dapat diambil suatu tujuan terhadap penelitian ini yakni memberikan pemahaman, menambah pengetahuan dan dapat di adaptasi dalam melaksanakan perancangan kebijakan pada suatu organisasi.

1.4 Batasan Masalah

Berdasarkan rumusan yang dibuat maka dibuat Batasan permsalahan agar penelitian lebih fokus dan tepat sasaran, Batasan tersebut antara lain :

1. Penelitian dilakukan pada salah satu Perusahaan Penyedia Jasa TI yakni PT Waditra Reka Cipta Bandung
2. Penelitian berfokus pada seberapa siapkah perusahaan dalam menghadapi masalah yang berkaitan dengan *Digital Forensik.*

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari dibuatnya penelitian ini adalah memberikan suatu rancangan kebijakan Digital Forensic Readiness (DFR) untuk mengoptimalisasikan serta tanggap insiden TI pada PT Waditra Reka Cipta Bandung

1.6 Review Penelitian

Perkembangan Teknologi informasi dan Komunikasi semakin berkembang sehingga dapat menyebabkan peningkatan tindak kejahatan dalam dunia maya atau sering disebut “cyber crime”. Maka dibutuhkan suatu kesiapan dari sebuah organisasi dalam menghadapi hal tersebut. Kesiapan itu sendiri dapat disebut dengan istilah *Readiness* yang berdasarkan pada proses bisnis serta fungsi dari teknologi tersebut. Dalam penelitian ini topik pembahasannya mengenai *Digital Forensic Readiness* pada suatu organisasi.

Kemudian dari berbagai studi dan telaah terkait *Digital Forensic Readiness,* ditemukan beberapa penelitian dan jurnal terkait serta membahas tentang *Digital Forensic Readiness,* diantaranya sebagai berikut :

A. Penelitian dilakukan oleh (Mohamed, B., Atif, & Andrew, 2014) yang membagi kesiapan forensic menjadi dua bagian fokus utama yakni Kesiapan Infrastruktur dan Kesiapan Operasional. Kesiapakan infrastruktur berfokus pada menjamin ketersediaan data pada suatu organisasi disajikan dengan tepat, sedangkan pada

kesiapan operasional berfokus pada penyediaan peralatan serta pelatihan individu yang akan terlibat pada digital forensic itu sendiri.

B. Penelitian dilakukan oleh (Elyas, Ahmad, Maynard, & Lonie, 2015) beberapa ahli merumuskan model atau *framework* logis dari *Digital Forensic Readiness* yang dapat digunakan secara umum. Dalam model atau *framework* logis yang disusun ini terdapat beberapa faktor atau aspek yang saling mempengaruhi dan berhubungan, antara lain *forensic readiness capability* yang berhubungan dengan *forensic radiness objective*. Dalam *forensic readiness capability* terdapat 2 faktor yang mempengaruhi, yaitu *Organizatinal Factors* dan *Forensic Strategy*. Sementara dalam *forensic readiness objectives* ada 4 faktor yang mempengaruhi, yaitu *regulatory compliance, legal evidence management, forensic respone, business objectives*.

C. Penelitian dilakukan oleh (Robert Rownlingston, 2004) memaparkan dalam penelitiannya bahwa ada sepuluh tahapan dalam proses *Digital Forensic Readiness,* mulai dari skenario bisnis yang memerlukan bukti digital, identifikasi bukti-bukti digital, hingga tindakan-tindakan legal di dalam menangani insiden yang terjadi.

D. Penelitian dilakukan oleh (Grobler & Louwrens, 2007) memaparkan dalam penelitiannya tentang *Digital Forensic Readiness* sebagai sebuah komponen dalam keamanan sistem informasi. Pada penelitian ini dibahas berbagai isu keamanan dari sistem informasi dan *Digital Forensic Readiness*, belum adanya keseimbangan antara keamanan sistem dan *Digital Forensic Readiness*, serta tujuan dari *Digital Forensic Readiness* sebagai bentuk keamanan sistem informasi.

E. Penelitian dilakukan oleh (Barske, Stander, & Jordaan, 2010) memaparkan dalam penelitiannya tentang *framework* atau model *Digital Forensic Readiness* untuk Usaha Kecil dan Menengah (UKM) di Afrika Selatan. Pada penelitian ini mereka membuat model *Digital Forensic Readiness* dan faktor-faktor yang harus diperhitungkan, mulai dari strategi, kebijakan dan prosedur, teknologi yang digunakan, *digital forensic respone*, hingga pada pengawasan. Model yang dibuat oleh Barske, Stander dan Jordaan ini masih memiliki kekurangan, yaitu tidak adanya metode perhitungan dari kompone-komponen penyusun model *Digital Forensic Readiness,* sehingga masih sulit diaplikasikan.

F. Penelitian dilakukan oleh (Mouhtaropoulos, Li, & Grobler, 2014) memaparkan pada

penelitian ini seharusnya sebelum insiden atau tindak kejahatan terjadi mayoritas institusi / organisasi sudah menyiapkan cara mengatasi masalah yang akan ditimbulkan dari tindakan tersebut. Maka dibutuhkan *Digital Forensic Readiness* untuk menjadi penghubung antara kelangsungan usaha/bisnis dengan investigasi forensik yang berjalan baik. *Digital Forensic Readiness* dijelaskan sebagai rencana pra-insiden yang berhubungan dengan identifikasi bukti digital, pelestarian, penyimpanan, analisis dan penggunaan serta meminimalkan biaya penyilidikan forensik. Dengan kata lain *Digital Forensic Readiness* ini bertujuan untuk mengelola bukti digital, membantu proses penyelidikan forensik agar tepat waktu dan menghemat biaya penyelidikan.

G. Penelitian dilakukan oleh (Widodo, 2016) memaparkan dalam penelitiannya tentang Model *Digital Forensic Readiness Index* (DiFRI) untuk mengukur tingkat kesiapan Institusi dalam menanggulangi aktivitas *Cyber Crime*. Pada penelitian ini dijelaskan komponen-komponen yang membentuk *Digital Forensic Readiness Index* (DiFRI), seperti komponen strategi, kebijakan dan prosedur, teknologi dan keamanan, *digital forensic respone*, kontrol, *legality*. Komponen-komponen tersebut juga dilengkapi dengan indikator-indikator yang nantinya berguna untuk menghitung kesiapan dari institusi-institusi tersebut.
H. Jurnal Penelitian (Sachowski & Sachowski, 2019). Dijelaskan mengenai pentingnya kesiapan suatu organisasi dalam Forensik Digital, terutama saat pengumpulan dan penanganan barang bukti digital untuk dikelola oleh auditor suatu organisasi sebelum disajikan ke ranah hukum.
I. Penelitian dilakukan oleh (Reddy & Venter, 2008) mengusulkan serangkaian kebijakan untuk meningkatkan potensi forensik suatu organisasi dalam membantu menerapkan kemampuan kesiapan forensic untuk suatu insiden informasi, Secara khusus, kerangka kerja memberikan panduan untuk menentukan kebijakan tingkat tinggi, proses bisnis dan fungsi organisasi, dan untuk menentukan prosedur forensik tingkat perangkat, standar dan proses yang diperlukan untuk menangani insiden privasi informasi.
J. Penelitian dilakukan oleh (Moussa, Ithnin, & Miaikil, 2014) menyarankan kesiapan forensic bagi para penyedia layanan cloud (internet) agar dapat bertanggungjawab dalam mengumpulkan bukti digital ketika terjadinya insiden. Karena kurangnya

respon insiden secara efisien dan konsumen tidak mempunyai pilihan lain, selain menerima bukti digital dari penyedia.

K. Penelitian dilakukan oleh (Kazadi & Jazri, 2015) membahas tentang bagaimana pentingnya seorang administrator system pada suatu organisasi dalam mengamankan dan melindungi system informasi. Selain pada system juga bertanggungjawab dalam penyiapan alat keamanan untuk mengamankan system computer serta menyiapkan bukti digital bila diperlukan.

Rangkuman terhadap penelitian-penelitian yang telah dilakukan sebelumnya, dapat dilihat pada tabel perbandingan penelitian-penelitian yang disebutkan sebelumnya dan dapat dilihat pada tabel 1.1 seperti tabel di bawah ini.

Tabel 1.1 Perbandingan Penelitian Terdahulu

No	**Penulis Paper**	**Komponen yang diteliti**	**Persamaan atau perbedaan penelitian**
1	(Mohamed et al., 2014)	Kesiapan Infrastruktur dan Kesiapan Operasional	beberapa komponen yang diteliti yakni kesiapan infrastruktur organisasi serta operasional organisasi
2	(Elyas, *et al.*, 2015)	Terdapat 7 komponen, yaitu *Strategy, Policy & Procedure, Technology, Security, Digital Forensic Response, Control, Legality.*	Terdapat komponen-komponen yang diteliti dalam penelitian ini
3	(Robert Rownlingston, 2004)	Terdapat 3 komponen, yaitu *Policy&Procedure, Security, Legality.*	Memiliki komponen yang diteliti yakni *policy,procedure,security dan legality*
4	(Grobler & Louwrens, 2007)	Terdapat 1 komponen, yaitu *Security*.	Salah satu aspek yang diteliti dalam penelitian ini

5	(Barske, Stander, et al., 2010)	Terdapat 5 komponen, yaitu *Strategy, Policy & Procedure, Technology, Digital Forensic Response, Control.*	Beberapa komponen yang diteliti seperti *strategy,policy,procedure,digital forensic respone*
6	(Mouhtaropoulos et al., 2014)	Terdapat 6 komponen, yaitu *Technology, Security, Digital Forensic Response, Control, Cost, Legality.*	Ada beberapa komponen yang di uji kecuali "cost"
7	(Widodo, 2016)	Terdapat 6 komponen, yaitu *Strategy, Policy & Procedure, Technology & Security, Digital Forensic Response, Control, Legality.*	dikembangkan dari 6 komponen menjadi 5 komponen dalam menilai forensic readiness suatu organisasi/perusahaan.
8	(Sachowski & Sachowski, 2019).	Pengumpulan dan penanganan barang bukti digital oleh auditor organisasi	Merupakan aspek yang akan diteliti
9	(Reddy & Venter, 2008)	Serangkaian kebijakan dalam penerapan *forensic readiness* di organisasi	Merupakan aspek yang akan diteliti
10	(Moussa, et al., 2014)	kesiapan forensic bagi para penyedia layanan jasa	Memiliki kesamaan dengan tempat studi kasus yang diteliti
11	(Kazadi & Jazri, 2015)	Pentingnya administrator system pada suatu organisasi dalam *forensic readiness*	Sebagai bahan penelitian ditempat studi kasus
12	Usulan Penelitian	Membangun sebuah kerangka kerja DFR dari hasil penghitungan *Digital Forensic Readiness Index* (DiFRI) terhadap suatu perusahaan, agar lebih tanggap insiden *Digital Forensik*	

1.7 Metodologi Penelitian

Metode dalam penelitian ini menggunakan beberapa tahapan metodologi penelitian yang dapat dilihat pada Gambar 1.4.

Gambar 1.4 Bagan Proses Metodologi Penelitian

1.8 Sistematika Penulisan

Adapun sistematika penulisan yang dimaksud adalah sebagai berikut :

BAB 1 PENDAHULUAN

Pada bagian ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, *review* penelitian, metodologi penelitian dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bagian ini berisi tentang teori-teori yang terkait dengan kebijakan keamanan, *digital forensic*, *digital forensic readiness*, tahapan *digital forensic readiness* dan DiFRI.

BAB 3 METODOLOGI PENELITIAN

Pada bagian ini berisi tentang langkah-langkah penelitian dan gambaran umum langkah penyelesaian.

BAB 4 HASIL DAN PEMBAHASAN

Pada ini berisi tentang pembuatan model *Digital Forensic Readiness* berdasarkan

penelitian-penelitian yang telah ada, serta hasil uji coba dan evaluasi dari model yang telah dibangun tersebut.

BAB 5 KESIMPULAN DAN SARAN

Pada bagian ini berisi tentang kesimpulan dari hasil penelitian yang telah dilakukan serta saran dan rekomendasi untuk penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 Kebijakan Keamanan

Kebijakan adalah prinsip-prinsip, pedoman dan tujuan yang digunakan untuk memandu kegiatan baik di organisasi, sektoral, tingkat nasional atau internasional (Subarsono, 2005). Sejalan dengan pengertian yang dikemukakan oleh (Subarsono, 2005), (Suharto, 2005) juga mendefinisikan kebijakan sebagai suatu ketetapan yang memuat prinsip-prinsip untuk mengarahkan cara bertindak yang dibuat secara terencana dan konsisten dalam mencapai tujuan tertentu. Oleh karena itu, fungsi dari kebijakan yaitu menjadi rujukan utama para anggota organisasi atau anggota masyarakat dalam berperilaku (Dunn, 2000). Kebijakan dianggap penting pada organisasi menurut (Winarno, 2002) karena:

a. Kebijakan digunakan untuk mengidentifikasi aset yang ada pada organisasi;
b. Kebijakan memberikan wewenang kepada tim keamanan dan kegiatan yang dilakukan;
c. Kebijakan memberikan panduan untuk pemeriksaan ketika terjadi masalah atau konflik;
d. Kebijakan menjelaskan tanggung jawab tiap pihak yang ada dalam organisasi

Dokumen kebijakan keamanan adalah infrastruktur keamanan yang harus dimiliki oleh organisasi untuk melindungi aset informasi yang secara prinsip berisi berbagai cara yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara untuk mengamankan informasi (Indrajit, 2014). Menurut Indrajit, terdapat dua peranan penting kebijakan keamanan, yaitu :

a. Mendefinisikan dan memetakan secara detail aset informasi yang harus dilindungi dan dikelola dengan baik.
b. Mengurangi risiko yang dapat ditimbulkan karena adanya penyalahgunaan sumber daya yang terkait dengan manajemen pengelolaan data dan informasi, insiden, atau pelanggaran hak akses data.

Tujuan dari adanya kebijakan keamanan menurut (Indrajit, 2014) diantaranya:

a. Melindungi sumber daya sistem dan teknologi informasi organisasi dari penyalahgunaan hak akses,

b. Menangkis serangan atau dakwaan hukum dari pihak lain terkait dengan insiden keamanan, dan
c. Memastikan keutuhan data bebas dari perubahan dan modifikasi oleh pihak yang tidak berwenang.

2.2 Digital Forensic

Menurut (Prayudi & Ashari, 2015) digital forensic adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital dalam rangka kepentingan rekontruksi kejadian serta memastikan keabsahan pada proses peradilan. (Kebande, Karie, & Venter, 2016) menambahkan bahwa digital forensic mencakup pengujian terhadap bukti digital dengan analisis forensik yang dilakukan oleh Law Enforcement Agencies (LEA). Tujuan utama dari digital forensic adalah menemukan bukti-bukti digital yang akan digunakan oleh pengacara, LEA, dan kantor kejaksaan untuk dipresentasikan di pengadilan.

Dalam digital forensic terdapat tiga entitas yang memiliki peran yang sangat penting, yaitu human sebagai aktor yang melakukan aktivitas, digital evidence sebagai objek dan aset vital, dan process sebagai pedoman yang harus diikuti sepanjang proses investigasi digital forensic berlangsung (Mabuto & Venter, 2011). Pedoman dalam pelaksanaan investigasi tersebut menggunakan metode ilmiah, artinya dalam setiap tahapan atau langkah yang dilakukan oleh tim investigasi ataupun lembaga hukum harus menjunjung tinggi kaidah metode ilmiah (Mabuto & Venter, 2011). Dengan berpedoman pada karakteristik metode ilmiah, maka process dalam bidang digital forensic harus mengacu pada langkah-langkah secara prosedural dan terstruktur (Mabuto & Venter, 2011). Proses dalam digital forensic dikenal dengan digital forensic investigation

Digital forensic investigation diterapkan setiap dibutuhkan penyelidikan terhadap barang bukti digital sebagai hasil dari suatu insiden, untuk menentukan insiden itu termasuk sebagai kegiatan kriminal atau tidak.

Dalam digital forensic investigation terdapat tahap perencanaan (pre incident) yang bisa diterapkan sebelum dilakukan investigasi yang disebut dengan DFR (Kigwana & Venter, 2018). DFR mensyaratkan organisasi memiliki data terkait penanganan insiden sebelumnya guna mengefisiensikan, meningkatkan serta mengefektifkan proses investigasi apabila terjadi insiden. Untuk itu diperlukan pendekatan yang efektif yang dapat membantu

organisasi dan investigator dalam melaksanakan DFR. Salah satu pendekatan yang dapat dilakukan adalah menyusun kebijakan DFR dalam sebuah organisasi.

2.3 Digital Forensic Readiness (DFR)

Digital Forensic Readiness digambarkan sebagai rencana pra-insiden dalam siklus proses investigasi digital forensik yang berhubungan dengan identifikasi bukti digital, pelestarian, penyimpanan, analisis dan meminimalisir biaya penyelidikan. Dengan kata lain, DFR bertujuan untuk mengelola bukti digital agar dapat membantu proses penyelidikan dan menghemat biaya penyilidikan (Mouhtaropoulos et al., 2014).

Digital Forensic Readiness adalah kemampuan sebuah organisasi/institusi untuk memaksimalkan potensi mereka dalam menggunakan barang bukti digital dan meminimalisir biaya investigasi yang dikeluarkan organisasi (Robert Rowlingson, 2004).

Digital Forensic Readiness memiliki tujuan, yaitu untuk memaksimalkan penggunaan data sebagai barang bukti ketika terjadi insiden dan meminimalisir biaya investigasi ketika merespon insiden (Tan, 2001).

Dari penjelasan para ahli di atas dapat diambil kesimpulan bahwa, *Digital Forensic Readiness* adalah sebuah tindakan pra-insiden dengan memanfaatkan barang bukti digital dalam proses investigasi dan menghemat biaya proses penyelidikan.

2.4 Tahapan-tahapn dalam Digital Forensic Readiness (DFR)

Dalam proses Digital Forensic Readiness dibutuhkan tahapan-tahapan untuk mencapai tujuan dari Digital Forensic Readiness itu sendiri. Tahapan-tahapan dari Digital Forensic Readiness (Robert Rowlingson, 2004) adalah, sebagai berikut :

- Menentukan skenario bisnis yang membutuhkan barang bukti digital.
- Mengidentifikasi sumber-sumber yang tersedia dari barang bukti yang potensial.
- Menentukan barang bukti yang perlu dikumpulkan.
- Menetapkan kemampuan dalam organisasi untuk mengumpulkan barang bukti secara aman agar dapat dijadikan barang bukti yang memenuhi persyaratan atau sah secara hukum.
- Menetapkan kebijakan-kebijakan untuk mengamankan media penyimpanan dan menangani barang bukti yang potensial.

- Memastikan sumber-sumber sistem informasi terawasi untuk mendeteksi dan mencegah insiden besar.
- Mengidentifikasi keadaan ketika investigasi normal dilakukan pada saat kejadian.
- Melatih anggota organisasi/institusi dalam kesadaran terhadap insiden sehingga semua pihak yang terlibat memahami peran dan tanggungjawab mereka dalam proses barang bukti digital dan kepekaan terhadap hukum atas barang bukti tersebut.
- Mendokumentasikan kasus-kasus yang berbasis barang bukti yang menjelaskan insiden dan dampaknya terhadap organisasi/institusi.
- Memastikan telah dilakukannya review hukum untuk memfasilitasi berbagai tindakan dalam merespon insiden yang terjadi.

2.1.1 DiFRI (Digital Forensic Readiness Index) (Widodo, 2016)

Merupakan suatu cara untuk mengukur kesiapan suatu institusi/organisasi dalam mencegah dan menangani kejahatan dunia maya yang nantinya dapat diukur dengan melihat berbagai faktor dan indikator yang setelahnya dihitung akan menghasilkan suatu nilai yang disebut DiFRI.

2.1.2 Komponen dan Indikator Penilaian

Adapun detail Adapun detail indikator masing-masing komponen tersebut adalah :

a. Komponen Strategy

Indikator Komponen Strategy yaitu :

- 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

b. Komponen Policy & Procedure

- Indikator komponen Policy & Procedure antara lain :
- Kebijakan dan prosedur sebagai petunjuk aktifitas dan kegiatan anggota organisasi yang mengunakan TIK
- Sangsi bagi pelanggar kebijakan dan prosedur Digital Forensic Readiness
- Kebijakan bahwa semua sumber daya informasi dan data merupakan milik organisasi
- Kebijakan dalam keadaan bagaimanakah barang bukti digital dapat diamankan
- Kebijakan barang bukti digital apa saja yang harus diamankan
- 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
- Kebijakan pembagian wewenang, tugas dan tanggungjawab terkait pengumpulan barang bukti digital, pemeliharaan dan pemeriksaanya

c. Komponen Technology & Security

Indikator komponen Technoloy & Security antara lain :

- 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

d. Komponen Digital Forensic Response

- Indikator komponen Digital Forensic Response yaitu :

- 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

e. Komponen Control & Risk

- Indikator komponen Control& Risk antara lain :
- Pengawasan program Digital Forensic Readiness
- Evaluasi secara berkala program Digital Forensic Readiness
- Sosialisasi program digital forensic kepada anggota organisasi
- Pemahaman pada anggota setiap proses digital forensic dan resiko kegagalan setiap proses
- Pembaharuan perangkat, tool, dan sistem secara berkala
- Pembahasan hasil investigasi maupun publikasi hasil investigasi kepada kepala-kepala departemen/sub bagian

f. Legality

Indikator komponen Legality yaitu :

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

2.1.3 Metode Pengumpulan Data

Beberapa metode pengumpulan data yang dilakukan dengan setiap responden, Admin, CEO maupun direktur mengisi kuisioner yang telah disediakan, selanjutnya dilakukan analisis pada data tersebut.

2.1.4 Metode Pengitungan

Pada kuesioner, skala yang digunakan adalah skala Guttman, yaitu skala pengukuran dengan jawaban tegas, antara “ada-tidak”. Selanjutnya, dari enam komponen diatas akan dilakukan scoring untuk menilai aspek DiFRI secara keseluruhan untuk mengetahui Digital Forensic Readiness Index suatu organisasi Dari kuesioner kemudian akan dilakukan penghitungan atas jawaban “Ada” dan “Tidak”, selanjutnya dilakukan scoring pada masing-masing aspek dengan menggunakan rumus :

$$I_{\mathrm{A}} = \frac{\sum_{k=1}^{n} A}{n_A} . 10$$

IA merupakan indeks dari masing-masing aspek, selanjutnya A merupakan jumlah indikator yang bernilai ”ada”, dan nA adalah total dari indikator pada aspek tersebut, sedangkan perkalian 10, dimaksudkan untuk mendapatkan skala dari 0 sampai dengan 10. Adapun untuk secoring keseluruhan dari DiFRI yaitu dengan menggunakan rumus :

$$I_{\mathrm{el}} = \frac{\sum_{k=1}^{n} Ael}{n_{el}} . 10$$

Iel merupakan indeks dari semua komponen, selanjutnya A*el* merupakan jumlah indikator yang bernilai ”ada”, dan nel adalah total dari seluruh indikator, sedangkan perkalian 10, dimaksudkan untuk mendapatkan skala dari 0 sampai dengan 10. Atau bisa juga digunakan

rumus :

$$I_{\mathrm{total}} = \frac{\sum_{k=1}^{n} I_A}{n_{I_A}}$$

Itotal merupakan indeks DiFRI keseluruhan komponen, *I*A merupakan indeks masing-masing komponen, dan adalah banyaknya komponen.

2.1.5 Skala Tingkat DiFRI

Untuk memberikan rekomendasi dan kejelasan status institusi/organisasi, dibuatlah skala dan status untuk masing-masing nilai DiFRI (i), peneliti membuat lima kriteria berdasarkan skala tertentu, seperti pada table dibawah ini :

Tabel 2.1 Skala Kesiapan Institusi berdasarkan DiFRI

No	Range/Skala	Status
1	$8 < i \leq 10$	Sangat Siap
2	$6 < i \leq 8$	Siap
3	$4 < i \leq 6$	Cukup Siap
4	$2 < i \leq 4$	Kurang Siap
5	$0 \leq i \leq 2$	Tidak Siap

2.5 Pedoman Penyusunan Kerangka Kerja Logis (LFA) Secara Bertahap

Dalam menyusun Kerangka Kerja Logis (Logical Framework Analysis – LFA) secara bertahap, bekerjalah dengan mengikuti alur tahapan dasar di dalam penyusunan suatu rancangan proyek yang menggunakan LogFrame. Keseluruhan proses pengembangan LogFrame senantiasa mengikuti prinsip-prinsip pokok yaitu bekerja mulai dengan sesuatu yang umum hingga kepada yang spesifik.

Pada tahap pertama pengembangan LogFrame anda hendaknya menyiapkan suatu uraian umum, atau “Ringkasan Narasi”, bagi proyek tersebut. Ini berarti anda perlu:

A. menetapkan **Sasaran (Goal)** yang ingin dicapai lewat kontribusi proyek anda;
B. menetapkan **Tujuan (Purpose)** yang akan dicapai oleh proyek itu;
C. menetapkan **Keluaran (Outputs)** guna mencapai sasaran di atas;
D. menetapkan **Kegiatan-kegiatan (Activities)** guna mencapai tiap Keluaran (Outputs).

   Mengingat bahwa pernyataan-pernyataan tersebut di atas saling terkait secara logis, maka anda perlu menegaskan bahwa logika yang ada telah benar. Agar dapat menjamin bahwa hal itu memang demikian adanya, maka sekarang anda harus :

E. Melakukan verifikasi logis secara vertikal dengan cara **“Jika… /Maka ….**

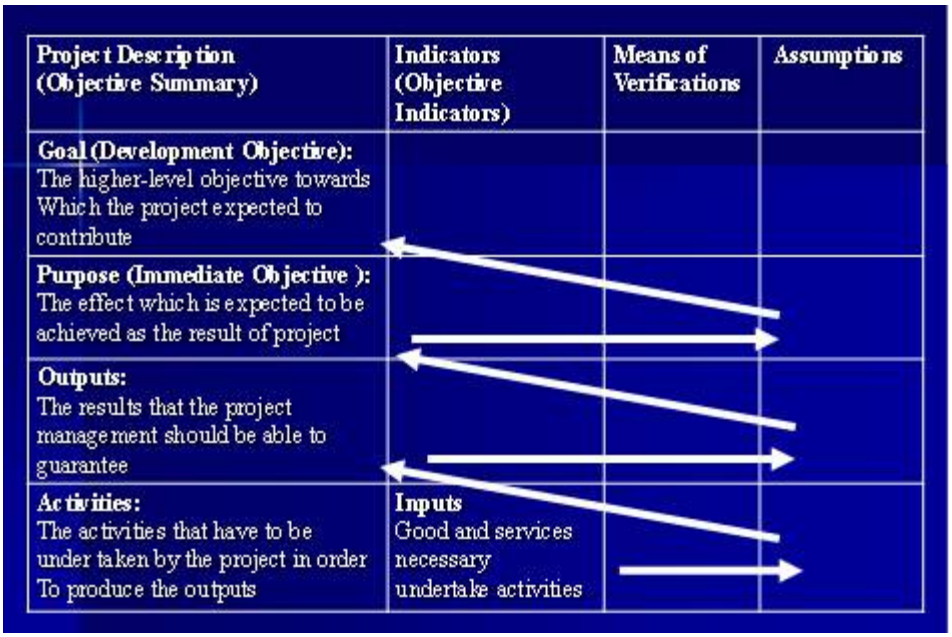
Anda tidak akan dapat mengontrol semua faktor yang berhubungan dengan proyek anda dan oleh karena itu anda harus membuat beberapa asumsi. Langkah berikutnya ialah:

F. Menetapkan **asumsi-asumsi** yang berkaitan dengan masing-masing tingkatan.
   Anda perlu mengembangkan suatu dasar untuk mengukur efektifitas proyek. Agar supaya bisa melakukannya, sekarang anda harus:
G. menetapkan **Indikator-indikator Penentu Obyektif** yang dapat diukur pada tingkat **Sasaran (Goal)** kemudian **Tujuan (Purpose)** , kemudian **Keluaran (Output)**, kemudian **Kegiatan-Kegiatan (Activities)**.
H. menetapkan Alat-alat / Perangkat Verifikasi.
   Anda kini sudah memproduksi sebuah uraian mengenai proyek itu dan anda bisa melanjutkan ke langkah selanjutnya yaitu :
I. mengalokasikan biaya-biaya pada setiap kegiatan : mempersiapkan Anggaran Pelaksanaan.
   Akhirnya, lakukan dua langkah lebih jauh lagi guna membantu memastikan bahwa LogFrame sudah selesai disusun dan dirancang dengan baik:
J. periksa LogFrame dengan menggunakan Daftar Periksa Rancangan Proyek;
K. mengkaji ulang rancangan LogFrame tersebut dengan menggunakan pengalaman anda tentang kegiatan-kegiatan yang sama.

Dari langkah-langkah tersebut di atas, maka Anda akan menampilkan LogFrame anda sebagai sebuah tabel dengan model sebagai berikut:

Tabel 2.2 Model LogFrame

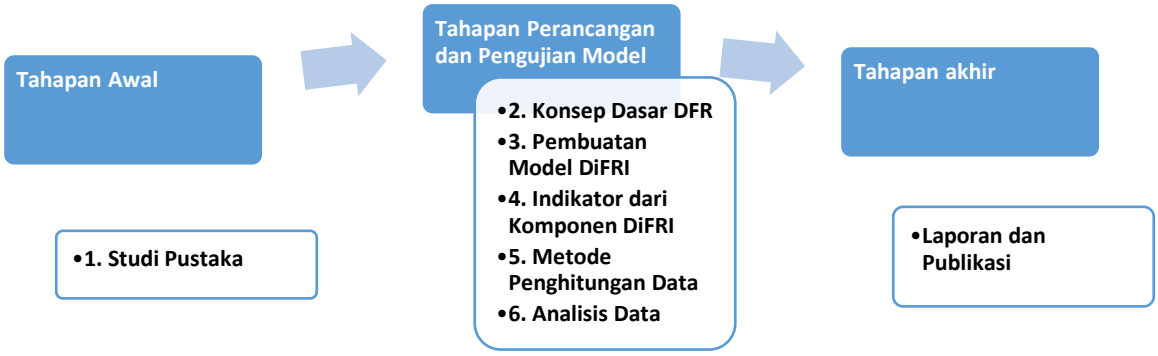
	Summary	Indicators	Verification	Assumptions
GOAL				
PURPOSES				
OUTPUTS				
ACTIVITIES				



.Gambar 2.1 Model LogFrame

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)

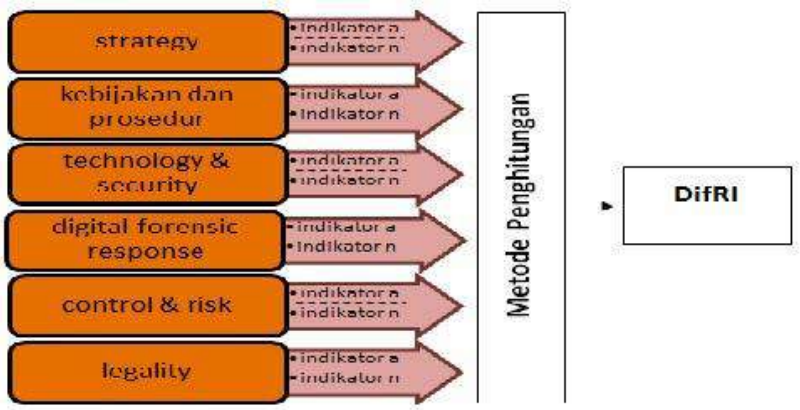
c. *Technology & Security*. Hal ini adalah bagian paling penting ketika akan menerapkan *digital forensic*. Setiap pengguna internet seharusnya memiliki perangkat keras maupun perangkat lunak untuk mencari, mengambil dan melindungi barang bukti digital. Hal ini dipaparkan oleh (Grobler & Louwrens, 2007),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

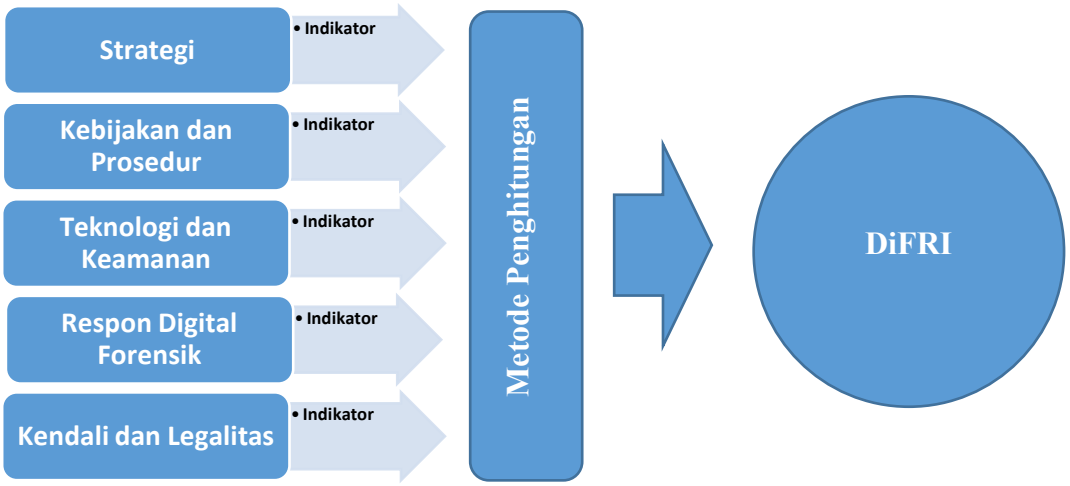
3.3 Pembuatan Model DiFRI terhadap Perusahaan PT Waditra Reka Cipta Bandung

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

BAB 4
Hasil dan Pembahasan

4.1 Hasil Penelitian

Berdasarkan pada komponen utama *digital forensic readiness* dan studi pustaka berbagai model *readiness* dan model DiFRI yang telah ada, maka dibuatlah pengembangan dari model DiFRI tersebut. Hasil pengembangan model DiFRI memiliki 5 komponen utama, sebagai berikut :

1. *Strategy*
2. *Policy & Procedure*
3. *Technology & Security*
4. *Digital Forensic Response*
5. *Control & Legality*

Selanjutnya berdasarkan komponen-komponen utama dari model DiFRI di atas diuraikan indikator-indikator dari setiap komponennya, seperti pada Gambar 3.3. Indikator-indikator ini menjadi penjelasan dari setiap komponen dan kemudian menjadi alat ukur dari model DiFRI ini.

4.2 Penerapan DiFRI

Model DiFRI ini diterapkan pada PT Reka Cipta Bandung. Pada penerapan model DiFRI ini, peneliti mengambil data dari 22 responden yang merupakan keseluruhan dari pegawai beserta jajaran pimpinan.

4.3 Hasil Pengujian

Indeks DiFRI dapat dihitung berdasarkan komponen-komponen utama dan juga dapat dihitung secara keseluruhan. Berikut adalah hasil penghitungan dari setiap komponen-komponen utama dari model DiFRI ini :

4.3.1 Komponen Strategy

Tabel 4.1 Hasil Perhitungan Indeks (%) Komponen *Strategy*

No	Indikator	Total Skor					Jumlah Total Skor	Indeks (%)
		SS	S	RG	TS	STS		
1	Memiliki program-program *digital forensics.*	0	0	30	12	6	48	43.64
2	Memiliki Aturan, regulasi dan kewajiban menyimpan dokumen, file dan rekaman (log, dokumen).	60	40	0	0	0	100	91
3	Memiliki ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital.	0	0	18	24	4	46	42
4	Identifikasi sumber-sumber yang berbeda dari barang bukti digital instansi.	0	0	21	20	5	46	42
5	Identifikasi teknologi dan sumber daya manusia untuk menjamin *digital forensic readiness*.	0	12	36	2	6	56	51
Indeks (%) Komponen								**54**

Berdasarkan hasil penghitungan pada komponen ini dengan nilai indeks 54% dapat dilihat pada Tabel 4.1, PT WRC BANDUNG telah dinyatakan **Kurang Siap** dalam hal *strategy* dalam mengahadapi *digital forensic*. Namun ada 1 indikator yang memiliki nilai indeks sudah **siap** dan kemudian dapat dicermati, yaitu Memiliki Aturan, regulasi dan kewajiban menyimpan dokumen, file dan rekaman (log, dokumen).

4.3.2 Komponen Policy & Procedure

Tabel 4.2 Hasil Perhitungan Indeks (%) Komponen *Policy & Procedure*

No	Indikator	Total Skor					Jumlah Total Skor	Indeks (%)
		SS	S	RG	TS	STS		
1	Memiliki petunjuk atau prosedur aktifitas pegawai instansi dalam menggunakan TIK.	110	0	0	0	0	110	100
2	Mengetahui sangsi jika melanggar aturan dan prosedur dari *digital forensic readiness.*	110	0	0	0	0	110	100
Indeks (%) Komponen								**100**

Berdasarkan hasil penghitungan pada komponen ini dengan nilai indeks 100% dapat dilihat pada Tabel 4.2, PT WRC BANDUNG telah dinyatakan sudah **siap** dalam hal *policy & procedure* dalam mengahadapi *digital forensic*.

4.3.3 Komponen Technology & Security

Tabel 4.3 Hasil Perhitungan Indeks (%) Komponen *Technology & Security*

No	Indikator	Total Skor					Jumlah Total Skor	Indeks (%)
		SS	S	RG	TS	STS		
1	Ketersediaan jaminan manajemen log.	0	20	15	24	0	59	54
2	Ketersediaan manajemen media penyimpanan (CD, hardisk, flashdisk) dari perangkat komputer dan *server*.	110	0	0	0	0	110	100
3	Ketersediaan perangkat akuisisi analisis barang bukti digital, baik berupa *hardware* (*write block protector*) maupun *software* (*analisys tool*).	0	20	30	10	2	62	62

4	Ketersesiaan jaminan keamanan barang bukti, baik secara *online* maupun *offline*, melalui *imaging* maupun penggandaan fisik.	0	20	30	10	2	62	62
5	Ketersediaan perangkat pendukung *digital forensic* seperti CCTV, *finger print* dan autentifikasi system.	0	0	0	44	0	44	40

No	**Indikator**	**Total Skor**					**Jumlah Total Skor**	**Indeks (%)**
		SS	**S**	**RG**	**TS**	**STS**		
6	Ketersediaan perangkat pengamanan sistem, seperti *firewall, anti-virus*.	110	0	0	0	0	110	100
7	Ketersediaan perangkat pendukung keamanan seperti enkripsi dan kriptografi.	0	20	45	4	0	69	63
Indeks (%) Komponen								**45**

Berdasarkan hasil penghitungan pada komponen ini dengan nilai indeks 45% dapat dilihat pada Tabel 4.3, PT WRC BANDUNG dinyatakan **kurang siap** dalam hal *technology & security* dalam mengahadapi *digital forensic*. Namun ada 5 indikator yang memiliki nilai indeks siap dan kemudian dapat dicermati, yaitu Ketersediaan manajemen media penyimpanan, Ketersediaan perangkat akuisisi analisis barang bukti digital, Ketersediaan perangkat pengamanan system (firewall) dan ketersediaan perangkat pendukung keamanan seperti enkripsi dan kriptografi.

4.3.4 Komponen Digital Forensic Response

Tabel 4.4 Hasil Perhitungan Indeks (%) Komponen *Digital Forensic Response*

No	Indikator	Total Skor					Jumlah Total Skor	Indeks (%)
		SS	S	RG	TS	STS		
1	Ketersediaan SOP (*standart operating procedure*) dalam penanganan insiden atau tindakan *digital forensic.*	25	0	30	10	2	67	61
2	Ketersediaan SDM / Pengguna internet yang memiliki	0	8	0	40	0	48	43.7
No	**Indikator**	**Total Skor**					**Jumlah Total Skor**	**Indeks (%)**
		SS	**S**	**RG**	**TS**	**STS**		
	sertifikasi / keahlian di bidang *digital forensic*.							
3	Ketersediaan pelatihan-pelatihan bagi SDM/pengguna internet mengenai penanganan serangan *penanganan insident forensic digital* dan *digital forensic*.	50	40	6	0	0	96	87.3
4	Ketersediaan tim penanganan *penanganan insident forensic digital* dan *digital forensic.*	0	0	6	40	0	46	41.8
5	Ketersediaan petunjuk teknis pengaduan maupun pelaporan insiden.	0	0	6	40	0	46	41.8
6	SDM memiliki pengetahuan tentang bahaya *penanganan insident forensic digital.*	50	40	9	2	0	99	90

7	Ketersediaan alat peraga, petunjuk dan arahan mengenai *penanganan insident forensic digital* berupa poster, banner dan alat peraga lainnya	0	0	0	44	0	44	40
Indeks (%) Komponen								**43**

Berdasarkan hasil penghitungan pada komponen ini dengan nilai indeks 43% dapat dilihat pada Tabel 4.4, PT WRC BANDUNG dinyatakan **kurang siap** dalam hal *digital forensic response* dalam mengahadapi *digital forensic*. Namun ada 3 indikator yang memiliki nilai indeks **siap** dan kemudian dapat dicermati, yaitu :

1. Ketersediaan SOP (standart operating procedure) dalam penanganan insiden atau tindakan digital forensic.
2. Ketersediaan pelatihan-pelatihan bagi SDM/pengguna internet mengenai penanganan serangan penanganan insident forensic digital dan digital forensic.

4.3.5 Komponen Control & Legality

Tabel 4.5 Hasil Perhitungan Indeks (%) Komponen *Control & Legality*

No	Indikator	Total Skor					Jumlah Total Skor	Indeks (%)
		SS	S	RG	TS	STS		
1	Adanya sosialisasi tentang *digital forensic* kepada pegawai instansi.	5	8	18	14	7	52	47.2
2	Adanya Sosialisasi tentang bahaya *penanganan insident forensic digital* kepada pegawai instansi.	15	40	18	6	0	79	71.8
3	Adanya pengawasan program *digital forensic readiness.*	5	0	21	28	0	54	49
4	Adanya pemahaman dari setiap pegawai mengenai setiap proses *digital forensic* dan resiko kegagalan setiap prosesnya.	10	8	24	20	0	62	56.36

5	Adanya pembaharuan perangkat, *tool* dan sistem secara berkala.	10	8	0	36	0	54	49
6	Memahami kebijakan aspek hukum setiap proses investigasi *digital forensic.*	5	4	18	20	4	51	46.36
7	Adanya pemahaman dari setiap pegawai instansi akan undang-undang ITE.	20	20	24	10	0	74	67.2
8	Adanya sosialisasi peraturan dan undang-undang ITE.	10	8	30	16	0	64	58.2

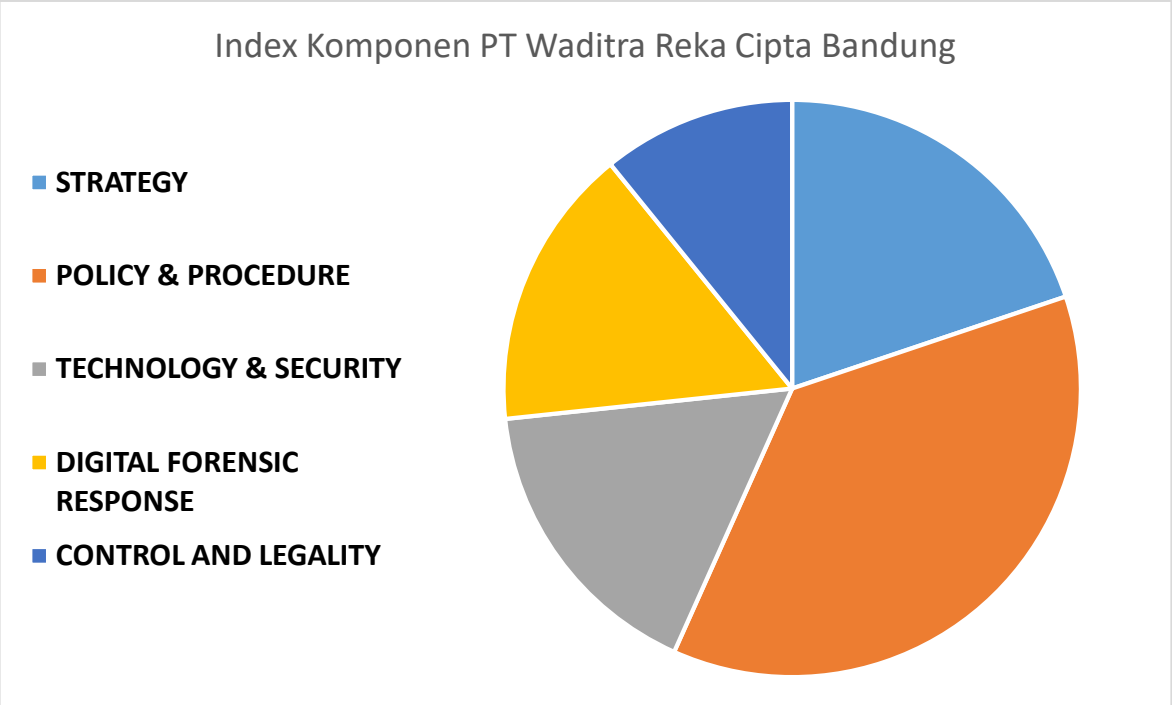
No	**Indikator**	**Total Skor**					**Jumlah Total Skor**	**Indeks (%)**
		SS	**S**	**RG**	**TS**	**STS**		
9	Adanya pelatihan penanganan terhadap serangan *penanganan insident forensic digital* dan proses hukumnya.	0	0	12	36	0	48	43.63
Indeks (%) Komponen								**29.4**

Berdasarkan hasil penghitungan pada komponen ini dengan nilai indeks 29.4% dapat dilihat pada Tabel 4.5, PT WRC BANDUNG telah dinyatakan **tidak siap** dalam hal *control & legality* dalam mengahadapi *digital forensic*. Namun ada 1 indikator yang memiliki nilai indeks **siap** dan kemudian dapat dicermati, yaitu Adanya pemahaman dari setiap pegawai instansi akan undang-undang ITE.

4.3.6 Hasil DiFRI Komponen

Tabel 4.6 Hasil Scoring Digital Forensic Readiness Index PT Waditra Reka Cipta Bandung

Komponen	**Index Komponen (%)**
Strategy	53.81818182
Policy & Procedure	100
Technology & Security	45.06493506
Digital Forensic Response	42.98701299
Control and Legality	29.39393939
Nilai DiFRI (%)	54.25281385



Gambar 4.1 Grafik *Scoring* DiFRI

Setelah mengetahui indeks setiap komponen-komponen utama dari model DiFRI ini, maka dihitung nilai indeks keseluruhan dari model DiFRI ini seperti pada Tabel 4.6. Berdasarkan penghitungan tersebut, nilai indeks DiFRI yang diperoleh dari keseluruhan komponen-komponen utama pada model ini adalah **54.25%**. Maka, dengan indeks tersebut PT WADITRA REKA CIPTA BANDUNG **kurang siap** dalam menghadapi *digital forensic*.

4.3.7 Pembahasan Penerapan DiFRI

Perbandingan pada setiap komponen-komponen utama menunjukkan bahwa indeks tertinggi terletak pada komponen *policy & procedure*, yaitu 100%. Indeks terendah terletak pada komponen *Control and Legality*, yaitu 29.4%. Hal ini menunjukkan bahwa secara **kebijakan dan prosedur** PT WADITRA REKA CIPTA BANDUNG telah siap menghadapi *digital forensic*, namun tidak diimbangi dengan kendali dan legalitas (*Control and Legality*) yang memiliki nilai indeks terendah serta index komponen yang lainnya, maka PT WADITRA REKA CIPTA BANDUNG akan **tidak tanggap/tidak siap** apabila terjadi kejahatan dunia maya kejadian digital forensic beserta kejahatan dunia maya.

Selain itu ada indikator-indikator dengan nilai indeks yang rendah dibandingkan dengan indikator lainnya, yaitu :

1. Memiliki petunjuk atau prosedur aktifitas pegawai instansi dalam menggunakan TIK (Komponen *Policy & Procedure*).
2. SDM memiliki pengetahuan tentang bahaya cara penanganan insident forensic digital (Komponen *Digital Forensic Response*).
3. Ketersediaan alat peraga, petunjuk dan arahan mengenai *penanganan insident forensic digital* berupa poster, banner dan alat peraga lainnya (Komponen *Digital Forensic Response*).
4. Adanya pemahaman dari setiap pegawai instansi akan Undang-undang ITE (Komponen *Control & Legality*).

Hal ini menunjukkan bahwa belum meratanya sosialisasi dan pemahaman dari setiap pegawai PT WADITRA REKA CIPTA BANDUNG tentang *Digital Forensic* secara umum. Sehingga PT WADITRA REKA CIPTA BANDUNG harus segera melakukan atau meningkatkan sosialisasi tentang *Digital Forensic*, program kegiatan maupun kebijakan kepada setiap pegawai, agar memiliki pemahaman yang lebih baik lagi, guna tercapainya target dari institusi dengan baik.

4.3.8 Analisa Model DiFRI

Berdasarkan kompilasi beberapa penelitian, penerapan dan pembahasan tentang model DiFRI serta pengembangan dari model DiFRI yang dikemukakan (Widodo, 2016), diperoleh beberapa hal yang dapat dicermati dan dianalisa dari pengembangan model DiFRI ini :

- Suatu organisasi memerlukan suatu kebijakan mengenai *handling incident* terkait kejadian digital forensic, agar aktifitas kerja serta layanan yang berjalan tidak menghambat maupun menyebabkan kerugian yang terlalu besar khususnya bagi perusahaan dan umumnya bagi para konsumen (pengguna).
- Suatu organisasi memerlukan suatu alat (teknologi) beserta sumber daya manusia (SDM) yang mumpuni terkait pencegahan maupun penanganan kejadian forensic digital agar file-file maupun data yang akan dijadikan sebagai barang digital dapat secara aman dan dapat secara legal dijadikan bukti yang sah di depan hukum.

4.3.9 Kerangka Kerja Logis (LFA) Digital Forensik Readiness

A. Tabel 4.7 **Kerangka Kerja Logis Strategi**

	SSummary	**I**Indicators	**V**Verifications	**A**Assumptions
GGoal Sasaran	Mempunyai Strategi yang dapat menangani Digital Forensic	Mempunyai berbagai langkah penanganan kejadian	Dokumen SOP strategi penanganan *digital forensic*	Berupa aturan baku yang tertulis dan harus dipatuhi pegawai.
PPurpose Tujuan	Memperkecil maupun mencegah kerugian perusahaan baik itu berupa aset data maupun aset harta	Biaya perawatan aset software serta biaya perawatan hardware	Laporan keuangan periodik, neraca kas laba-rugi	Berupa grafik pada dashboard aplikasi supaya lebih interaktif
OOutput Keluaran	1. Mempunyai Program *Digital Forensic* 2. Memiliki Aturan, regulasi dan kewajiban menyimpan dokumen, file dan rekaman (log, dokumen). 3. Memiliki ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital. 4. Identifikasi sumber- sumber yang berbeda dari barang	1. Encase, Autopsy, Kali Linux OS. 2. File log, File History. 3. Gudang penyimpanan aset 4. Penggunaan tool digital forensik 5. Mengenali berbagai Teknologi digital forensik dan SDM yang faham digital forensik	1. Lisensi Software, Sertifikat pelatihan penggunaan alat. 2. Folder berisi file-file log. 3. Cd, dvd, hardisk, flashdrive 4. Memahami penggunaan tool 5. Dapat menyebutkan nama teknologi dan mengetahui fungsinya	1. Membeli lisensi aplikasi opensource agar lebih murah, dan ikuti pelatihan online 2. File-file tersebut digandakan ke eksternal storage agar lebih aman 3. File backup agar mudah digunakan saat keadaan darurat

	bukti digital instansi. 5. Identifikasi teknologi dan sumber daya manusia untuk menjamin *digital forensic readiness*.			4. Menggunakan tool bias lebih efektif 5. Pemakaian akan bias tepat sasaran
AActivities Kegiatan	1. Mendownload atau membeli secara resmi lisensi 2. Membuat secara resmi regulasi di instansi yang disepakati oleh setiap pegawai 3. Mempunyai aturan dalam penanganan barang bukti digital 4. Menggunakan tool forensic dalam pengidentifikasian sumber-sumber data 5. Menjalani pelatihan pengenalan dan pemakaian perangkat maupun software digital forensik	1. Mencoba menggunakan tool yang mudah dalam penggunaanhya 2. Rutin backup log apabila sering terjadi human error 3. Menyiapkan tempat untuk barang-barang digital 4. Mencoba menangani contoh kasus digital forensic agar faham sumber file 5. Mengkikuti kegiatan seminar maupun workshop digital forensik	1. Mengecek/ memvalidasi lisensi 2. Mengecek file-file log yang sudah dibackup ke eksternal storage 3. Mengecek kondisi eksternal storage apakah masih layak digunakan 4. Melakukan kegiatan diskusi maupun brainstorming dengan yang faham digital forensic 5. Mengecek pengethuan pegawai mengenai digital forensik	

B. Tabel 4.8 **Kerangka Kerja Logis Kebijakan dan Prosedur**

	SSummary	**I**Indicators	**V**Verifications	**A**Assumptios
GGoal Sasaran	Mempunyai kebijakan dan prosedur dalam instansi	SOP yang mengatur kerja	Dokumen SOP yang disahkan oleh instansi	
PPurpose Tujuan	mempermudah instansi dalam tanggap digital forensic	Proses penanganan lebih baik dan cepat	Dari laporan penanganan digital forensic berkala	Berupa grafik pada dashboard aplikasi supaya lebih interaktif
OOutput Keluaran	1. Memiliki petunjuk atau prosedur aktifitas pegawai instansi dalam menggunakan TIK. 2. Mengetahui sangsi jika melanggar aturan dan prosedur dari *digital forensic readiness.*	1. SOP karyawan, SOP troubleshooting, dan SOP Maintenance 2. Sanksi bagi yang melanggar.	1. Karyawan melakukan kerja dengan terarah, baik dan aman 2. Karyawan yang melanggar dikenakan sanksi tertulis maupun lisan	
AActivities Kegiatan	1. Perancangan SOP oleh tim 2. Sosialisasi Sanksi yang akan diterima bagi pelanggar			

C. Tabel 4.9 **Kerangka Kerja Logis Komponen Teknologi & Keamanan**

	SSummary	**I**Indicators	**V**Verifications	**A**Assumptios
GGoal Sasaran	Mempunyai teknologi dan keamanan yang lebih baik	CCTV, Fingerprint, Log data	Md5, chipper, ssh-key	
PPurpose Tujuan	Menurunnya angka serangan hacking, Virus dan serangan malware	Log serangan hacking, History Vault Virus dan History Detect malware	File log serangan	Berupa grafik pada dashboard aplikasi supaya lebih interaktif
OOutput Keluaran	1. Ketersediaan jaminan manajemen log. 2. Ketersediaan manajemen media penyimpanan (CD, hardisk, flashdisk) dari perangkat computer dan *server*. 3. Ketersediaan perangkat akuisisi analisis barang bukti digital, baik berupa *hardware* (*write block protector*) maupun *software* (*analisys tool*).	1. Folder log, backup log 2. Cd/dvd drive, hardisk eksternal, flashdisk 3. Write blocker protector, wireshark, autopsy, kali linux OS 4. Brankas, plastik faraday, storage cloud 5. SSH, ID, Password, CCTV, fingerprint 6. Firewall, antivirus, antimalware	1. File log 2. Cd/dvd disk, hardisk, flashdisk 3. Write blocker protector, wireshark, autopsy, kali linux OS 4. Brankas, plastik faraday, storage cloud 5. SSH, ID, Password, CCTV, fingerprint 6. Firewall, antivirus, antimalware 7. Enkripsi, kriptografi	

	4. Ketersediaan jaminan keamanan barang bukti, baik secara *online* maupun *offline*, melalui *imaging* maupun penggandaan fisik. 5. Ketersediaan perangkat pendukung *digital forensic* seperti CCTV, *finger print* dan autentifikasi system. 6. Ketersediaan perangkat pengamanan sistem, seperti *firewall, anti-virus*. 7. Ketersediaan perangkat pendukung keamanan, seperti enkripsi dan kriptografi.	7. Enkripsi, kriptografi		
AActivities Kegiatan	1. Membuat SOP kerja karyawan perihal manajemen log 2. Penyediaan storage untuk backup oleh instansi 3. Menambah aset tool akuisisi (write blocker, hdd docking, os kali linux)	1. Mengecek file log setelah dan sebelum melakukan aktivitas kerja 2. Melakukan backup ke storage yang telah disediakan secara periodik		

	4. Backup periodik storage online maupun backup storage offline 5. Penambahan aset CCTV, finger print, ID System Authentificatio n 6. Mengatur dan melakukan filter dengan firewall dan scan PC maupun update antivirus berkala 7. Melakukan enkripsi dan kriptograsi terhadap data-data yang penting atau bersifat rahasia	3. Melakukan akuisisi terhadap barang bukti yang sudah di imaging		

D. Tabel 4.10 **Kerangka Kerja Logis Tanggapan**

	SSummary	**I**Indicators	**V**Verificatio ns	**A**Assumptio s
GGoal Sasaran	Meningkatkan tanggapan terhadap serangan maupun penanganan digital forensic	Laporan serangan, laporan penanganan		
PPurpose Tujuan	Memperkecil kerugian aset digital (data)	Biaya perawatan aset software serta biaya perawatan hardware	Laporan keuangan periodik, neraca kas laba-rugi	Berupa grafik pada dashboard aplikasi supaya lebih interaktif
OOutput Keluaran	1. Ketersediaan SOP (*standart operating procedure*) dalam penanganan insiden atau tindakan *digital.* 2. Ketersediaan SDM/Pengguna internet yang memiliki sertifikasi / keahlian di bidang *digital forensic.* 3. Ketersediaan pelatihan-pelatihan bagi SDM/pengguna internet mengenai penanganan serangan *penanganan insident forensic digital* dan *digital forensic.* 4. Ketersediaan tim	1. Dokumen SOP penanganan insiden digital 2. File sertifikat keahlian bidang digital forensic 3. Pelatihan maupun seminar penanganan serangan/ insiden digital forensic 4. Tim penanganga n insident digital forensic 5. Pedoman pengaduan		

	penanganan *penanganan insident forensic digital* dan *digital forensic*. 5. Ketersediaan petunjuk teknis pengaduan maupun pelaporan insiden. 6. SDM memiliki pengetahuan tentang bahaya *penanganan insident forensic digital.* 7. Ketersediaan alat peraga, petunjuk dan arahan mengenai *penanganan insident forensic digital* berupa poster, banner dan alat peraga lainnya	maupun pelaporan insiden 6. Buku maupun infografik bahaya penanganan insiden digital forensic 7. Alat peraga (infografik, banner, video, dsb) petunjuk penanganan insiden digital forensic		
AActivities Kegiatan	1. Membuat SOP kerja karyawan perihal penanganan insiden digital forensic 2. Tes Sertifikasi karyawan instansi dalam penanganan insiden digital forensic 3. Pengikutsertaan karyawan instansi dalam seminar penanganan insiden digital forensic 4. Pembentukan tim penanganan insiden digital forensic 5. Pembuatan petunjuk teknis pengaduan maupun			

	pelaporan insiden digital forensic 6. Sosialisasi dan penambahan aset buku dan media lain mengenai penanganan insiden digital forensic 7. Menambah aset alat peraga dan sosialisasi cara penanganan insiden digital forensic			

E. Tabel 4.11 **Kerangka Kerja Kontrol dan Legalitas**

	SSummary	**I**Indicators	**V**Verifications	**A**Assumptios
GGoal Sasaran	Menguatkan posisi control dan legalitas penanganan digital forensic	Dokumen legalitas	Disahkan oleh pejabat yang berwenang dan di akui oleh hokum	
PPurpose Tujuan	Mempercepat proses pengumpulan barangbukti, akuisisi dan proses analisis barang bukti digital secara legal atau sah secara hukum	Waktu yang lebih cepat, pemeriksaan dan pemprosesan barang bukti secara legal dan sah menurut hukum	Md5	Berupa grafik pada dashboard aplikasi supaya lebih interaktif
OOutput Keluaran	1. Adanya sosialisasi tentang *digital forensic* kepada pegawai instansi. 2. Adanya Sosialisasi tentang bahaya *penanganan insident forensic digital* kepada pegawai instansi. 3. Adanya pengawasan program *digital forensic*	1. Seminar, pelatihan, sertifikasi 2. Sosialisasi penanganan *insident forensic digital* 3. Pengawas program *penanganan insident forensic digital* 4. Diskusi mengenai *penanganan insident forensic digital* 5. Update perangkat		

	readiness. 4. Adanya pemahaman dari setiap pegawai mengenai setiap proses *digital forensic* dan resiko kegagalan setiap prosesnya. 5. Adanya pembaharuan perangkat, *tool* dan sistem secara berkala. 6. Memahami kebijakan aspek hukum setiap proses investigasi *digital forensic.* 7. Adanya pemahaman dari setiap pegawai instansi akan undang-undang ITE. 8. Adanya sosialisasi peraturan dan undang-undang ITE. 9. Adanya pelatihan penanganan terhadap serangan penanganan *insident forensic digital* dan proses hukumnya.	dan update system 6. Pedoman kebijakan aspek hokum proses investigasi digital forensic 7. Peraturan Undang-undang ITE 8. Peraturan Undang-undang ITE 9. Seminar, workshop dan sertifikasi *penanganan insident forensic digital*		

AActivities Kegiatan	1. Sosialisasi tentang *digital Forensic* 2. Sosialisasi tentang bahaya penanganan *insident forensic digital* 3. Melakukan pengawasan program *forensic digital readiness* 4. Melakukan sosialisasi mengenai setiap proses *digital forensic* dan resiko kegagalan setiap prosesnya. 5. Melakukan pembaharuan perangkat, *tool* dan sistem secara berkala 6. Sosialisasi kebijakan aspek hukum setiap proses investigasi *digital forensic* 7. Sosialisasi Peraturan dan undang-undang ITE 8. Sosialisasi Peraturan dan undang-undang ITE 9. Pelatihan Penanganan terhadap			

	srangan insiden digital forensic			

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil studi pustaka dari model-model *digital forensic readiness* yang telah ada, pengembangan dari model DiFRI sebelumnya, dan berdasarkan hasil penghitungan dari penerapan model DiFRI, maka dapat ditarik beberapa kesimpulan, sebagai berikut :

1. Terdapat perubahan komponen-komponen utama dari model DiFRI sebelumnya, dari 6 komponen utama menjadi 5 komponen utama. Dimana terjadi penggabungan komponen *control* dan komponen *legality*.
2. Hasil penghitungan dari penerapan model DiFRI pada PT Waditra Reka Cipta Bandung Perusahaan dinyatakan kurang siap dalam menghadapi kejahatan *digital forensic*, terutama dari sisi infrastruktur dan keamanan (*technology & security*).
3. Ada beberapa indikator dari komponen-komponen utama yang memiliki nilai indeks yang mendekati nilai kurang siap, sehingga ini harus menjadi hal yang harus dicermati dengan sangat baik.

5.2 Saran

Adapun saran-saran yang perlu diberikan atas hasil dari penelitian ini adalah sebagai berikut :

1. Perlu diadakan nya sosialisasi serta pelatihan maupun sertifikasi mengenai Digital Forensik Readiness diperusahaan tersebut.
2. Pada penelitian selanjutnya kita bias menggunakan metode maupun framework yang lebih efektif maupun efisien.

Daftar Pustaka

Barske, D., Stander, A., & Jordaan, J. (2010). A digital forensic readiness framework for South African SME's. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*, (March). https://doi.org/10.1109/ISSA.2010.5588281

D, R. R. P. (2004). International Journal of Digital Evidence Winter 2004 , Volume 2 , Issue 3 A Ten Step Process for Forensic Readiness International Journal of Digital Evidence. *International Journal of Digital Evidence*, *2*(3), 1–28. Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

Dunn, W. N. (2000). *Pengantar analisis kebijakan publik*. Gadjah Mada University Press.

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers and Security*, *52*(April), 70–89. https://doi.org/10.1016/j.cose.2015.04.003

Grobler, C. P., & Louwrens, C. P. (2007). Digital forensic readiness as a component of information security best practice. *IFIP International Federation for Information Processing*. https://doi.org/10.1007/978-0-387-72367-9_2

ID-CERT. (2018). *Incident Monitoring Report Tahun 2017*. 1–85. Retrieved from https://www.cert.or.id/media/files/UMUM_-_Laporan_Tahunan_2017.pdf

Indrajit, E. R. (2014). Manajemen Organisasi dan Tata Kelola Teknologi Informasi. *Yogyakarta: Graha Ilmu*.

Kazadi, J. M., & Jazri, H. (2015). Using digital forensic readiness model to increase the forensic readiness of a computer system. *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015*, (April), 131–137. https://doi.org/10.1109/ETNCC.2015.7184822

Kebande, V. R., Karie, N. M., & Venter, H. S. (2016). A generic Digital Forensic Readiness model for BYOD using honeypot technology. *2016 IST-Africa Week Conference*, 1–12. IEEE.

Kigwana, I., & Venter, H. S. (2018). A Digital Forensic Readiness Architecture for Online Examinations. *South African Computer Journal*, *30*(1), 1–39. https://doi.org/10.18489/sacj.v30i1.466

Mabuto, E. K., & Venter, H. S. (2011). State of the Art of Digital Forensic Techniques. *ISSA*.

Mohamed, E., B., M. S., Atif, A., & Andrew, L. (2014). Towards A Systemic Framework for Digital Forensic Readiness. *Journal of Computer Information Systems*, *54*(3), 97–105. https://doi.org/10.1080/08874417.2014.11645708

Mouhtaropoulos, A., Li, C. T., & Grobler, M. (2014). Digital forensic readiness: Are we there yet? *Journal of International Commercial Law and Technology*.

Moussa, A. N., Ithnin, N. B., & Miaikil, O. A. M. (2014). Conceptual forensic readiness framework for infrastructure as a service consumers. *Proceedings - 2014 IEEE Conference on System, Process and Control, ICSPC 2014*, (April), 162–167. https://doi.org/10.1109/SPC.2014.7086250

Prayudi, Y., & Ashari, A. (2015). A Study on Secure Communication for Digital Forensics Environment. *Int. J. Sci. Eng. Res*, *6*(1), 1036–1043.

Rahardjo, B. (2019). *Security Outlook 2019*.

Reddy, K., & Venter, H. (2008). Chapter 11 A FORENSIC FRAMEWORK FOR HANDLING INFORMATION. In *Advances in Digital Forensics IV* (pp. 143–155). https://doi.org/10.1007/978-3-642-04155-6_11

Sachowski, J., & Sachowski, J. (2019). Digital Forensic Readiness. *Digital Forensics and Investigations*, (October), 203–217. https://doi.org/10.4324/9781315194820-13

Subarsono, A. G. (2005). *Analisis kebijakan publik: konsep, teori dan aplikasi*. Pustaka Pelajar.

Suharto, E. (2005). *Analisis kebijakan publik: panduan praktis mengkaji masalah dan kebijakan sosial*. Alfabeta.

Tan, J. (2001). Forensic Readiness Assessment. *Cambridge, MA:@ Stake*, 1–23. Retrieved from http://project.honeynet.org

Widodo, T. (2016). Pengembangan Model Digital Forensic Readiness Index (DiFRI) Untuk Mencegah Kejahatan Dunia Maya. *Jurnal Informatika Sunan Kalijaga*, *1*(1), 41–46.

Winarno, B. (2002). *Teori dan proses kebijakan publik*. Media Pressindo.

Yosepyn, Tino. (2011, September 9). Pedoman Penyusunan Kerangka Kerja Logis (LFA) Secara Bertahap [Blog post]. Restrieved from http://lingkarlsm.com/pedoman-penyusunan-kerangka-kerja-logis-lfa-secara-bertahap/