CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 2, November 2019, hlm. 82-88

KERANGKA KERJA *DIGITAL FORENSIC READINESS* PADA SEBUAH ORGANISASI (STUDI KASUS : PT WADITRA REKA CIPTA BANDUNG)

Asep Sudirman, S.T.[1], Dr. Bambang Sugiantoro, M.T.[2], Yudi Prayudi, S.Si, M.Kom.[2]

[1]Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
[2]Teknik Informatika UIN Sunan Kaliijaga Yogyakarta
Email: [1]asep.sudirman@unsil.ac.id, [2]bambang.sugiantoro@uin-suka.ac.id, [3]prayudi@uii.ac.id

Abstrak

Digital Forensik 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 juga 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). 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, respon *forensic digital* serta kendali dan legalitas. Metode penghitungan pada pada hasil pengolahan kuesioner ini menggunakan skala Linkert yang biasa digunakan untuk mengukur persepsi atau pendapat seseorang mengenai sebuah peristiwa atau fenomena sosial.

Kata kunci: *Digital forensik, kerangka kerja, kesiapan digital forensic, difri, linkert*

A DIGITAL FORENSIC READINESS FRAMEWORK FOR AN ORGANIZATION (CASE STUDY: PT WADITRA REKA CIPTA BANDUNG)

Abstract

Digital forensics 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 Digital forensic Readiness of an organization is also 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 result in 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, Digital forensic Response and control and Legality. The calculation method 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.

Keywords: *Digital forensics, framework, Digital forensic Readiness, difri, linkert*

1. PENDAHULUAN

Meningkatnya serangan Dunia Maya maupun meningkatnya Ketergantungan Aset Digital IT (Rahardjo, 2019) menyebabkan adanya Forensik Digital pada Sebuah Organisasi agar lebih diperhitungkan. Oleh karena itu, Sebuah rrganisasi 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.

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.

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 diatas, 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.

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.

2.5 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.

2.5 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.

2.6 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.

2.7 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 :

$$I_A = \frac{\sum_{k=1}^{n} A}{n_a} .10$$

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 :

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

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 :

$$I\text{total} = \frac{\sum_{k=1}^{n} I_A}{n_{I_A}}$$

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

2.8 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

2.9 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

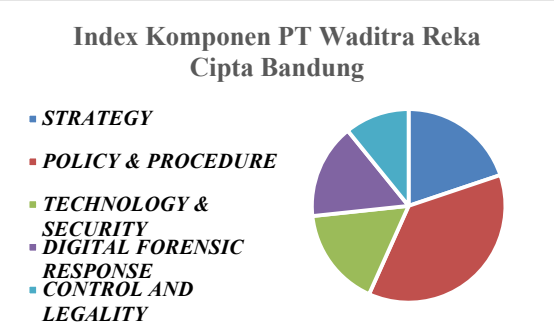
	Summary	Indicators	Verification	Assumptions
GOAL				
PURPOSES				
OUTPUTS				

ACTIVITIES				

4. Hasil DiFRI Komponen

Tabel 0.1 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 0.1 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*.

4.1. 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.

4.2. 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 khususnya bagi perusahaan dan umumnya bagi para konsumen.
- 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.

5. 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.

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 forensic*s 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.