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 :

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

I_A 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 :

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

I_{el} 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 :

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

I_{total} 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 ….**

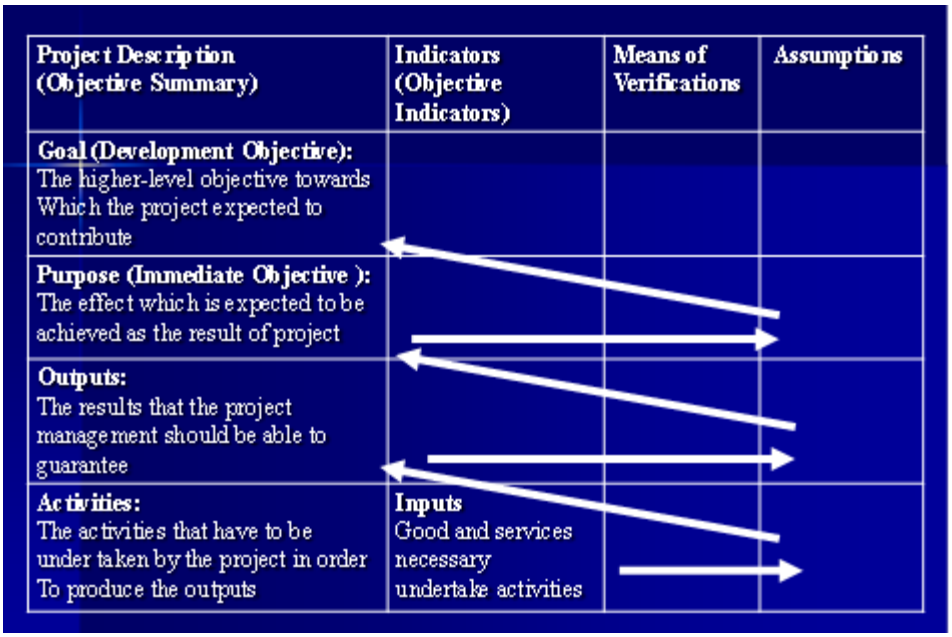
Anda tidak akan dapat mengontrol semua faktor yang berhubungan dengan proyek anda dan oleh karena itu anda harus membuat beberapa asumsi. Langkah berikutnya ialah:

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