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

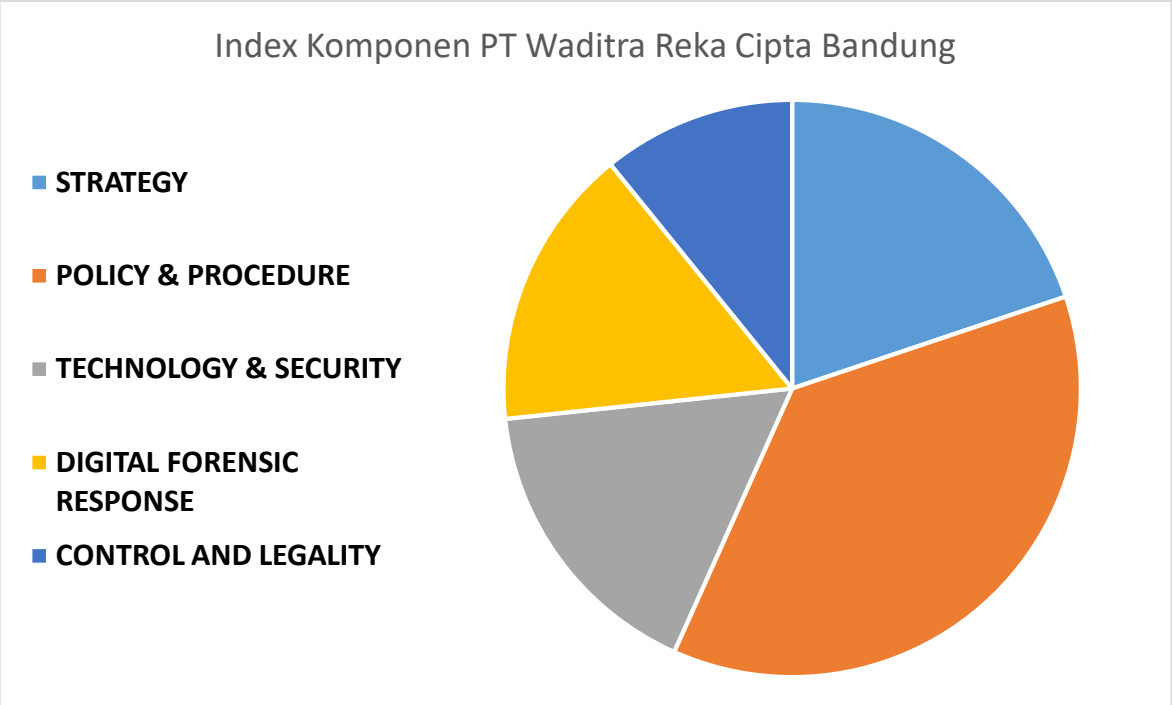
No	**Indikator**	**Total Skor**					**Jumlah Total Skor**	**Indeks (%)**
		SS	**S**	**RG**	**TS**	**STS**		
9	Adanya pelatihan penanganan terhadap serangan *penanganan insident forensic digital* dan proses hukumnya.	0	0	12	36	0	48	43.63
Indeks (%) Komponen								**29.4**

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			