

## **BAB 4**

### **HASIL PENELITIAN**

#### **4.1 RINGKASAN HASIL PENELITIAN**

Pada Penelitian ini dilakukan wawancara dan pengisian kuesioner terhadap Pemerintah Kota Yogyakarta terkhususnya Dinas Komunikasi Informasi dan Persandian Kota Yogyakarta. Ada 10 staf yang menjadi narasumber dari Penelitian ini, yang terdiri dari staf :

1. Bidang Sistem Informasi dan Statistika
2. Bidang Infrastruktur Telematika
3. Bidang Persandian dan Telekomunikasi

Terdapat 38 pertanyaan Penelitian sebelum dilakukan uji validitas dan menjadi 26 pertanyaan setelah dilakukan uji validitas yang terdiri dari 6 komponen DiFRI, yaitu:

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

Setelah dilakukan penghitungan hasil kuesioner menggunakan skala Linkert, maka diperoleh nilai DiFRI 74,59027778% yang dapat didefinisikan jika Pemerintah Kota Yogyakarta khususnya Dinas Komunikasi Informasi dan Persandian Kota Yogyakarta sudah dalam status siap dalam menangani kesiapan forensik digital.

#### **4.2 HASIL UJI VALIDITAS**

Uji validitas dilakukan dengan bantuan IBM SPSS Statistics. Uji ini dilakukan untuk setiap komponen yang terdapat dalam penelitian. Proses ini membantu memastikan keandalan dan validitas hasil analisis yang diperoleh dari data yang dikumpulkan (Slamet & Wahyuningsih, 2022).

#### 4.2.1 Komponen Strategy

Hasil dari uji validitas pertanyaan-pertanyaan komponen strategy menunjukkan bahwa dari total 6 pertanyaan yang diuji, 5 pertanyaan menghasilkan nilai  $r_{hitung}$  yang lebih besar daripada nilai kritis  $r_{tabel}$  (0.632 pada tingkat signifikansi 5%), yang menandakan bahwa pertanyaan-pertanyaan tersebut dapat dikategorikan sebagai valid. Namun, satu pertanyaan memiliki nilai  $r_{hitung}$  (0.588) yang lebih kecil dari nilai kritis  $r_{tabel}$ , sehingga pertanyaan ini dianggap tidak valid. Informasi detail mengenai hasil uji validitas ini dapat dilihat pada Tabel 4.1 yang terlampir di bawah ini.

**Tabel 4.1** Komponen Strategy

No	Pertanyaan	$r_{hitung}$	$r_{tabel}$	Keterangan
1	Memiliki program-program kesiapan forensik digital.	0.788	0.632	Valid
2	Terdapat aturan, regulasi, dan kewajiban terkait penyimpanan dokumen, file, dan rekaman (termasuk CCTV, log, dan dokumen lainnya).	0.814	0.632	Valid
3	Terdapat ketentuan yang berlaku saat terjadi peristiwa yang memerlukan barang bukti digital.	0.906	0.632	Valid
4	Melakukan identifikasi dan klasifikasi sumber-sumber dan jenis-jenis barang bukti digital yang berbeda.	0.984	0.632	Valid
5	Melakukan identifikasi dan sertifikasi teknologi serta sumber daya manusia yang diperlukan untuk memastikan kesiapan forensik digital.	0.896	0.632	Valid
6	Terdapat jaminan ketersediaan dana untuk menjalankan dan merawat program kesiapan forensik digital atau evaluasi secara berkala.	0.588	0.632	Tidak Valid

#### 4.2.2 Komponen Policy & Procedure

Hasil dari uji validitas pertanyaan-pertanyaan komponen policy & procedure menunjukkan bahwa dari total 7 pertanyaan yang diuji, 4 pertanyaan

menghasilkan nilai  $r_{hitung}$  yang lebih besar daripada nilai kritis  $r_{tabel}$  (0.632 pada tingkat signifikansi 5%), yang menunjukkan bahwa pertanyaan-pertanyaan tersebut dapat dikategorikan sebagai valid. Namun, terdapat 3 pertanyaan lainnya yang memiliki nilai  $r_{hitung}$  yang lebih rendah dari nilai kritis  $r_{tabel}$ , sehingga pertanyaan-pertanyaan ini dianggap tidak valid. Informasi detail mengenai hasil uji validitas ini dapat dilihat pada Tabel 4.2 yang terlampir di bawah ini..

**Tabel 4.2** Komponen Policy & Procedure

No	Pertanyaan	$r_{hitung}$	$r_{tabel}$	keterangan
1	Terdapat kebijakan dan prosedur yang digunakan sebagai panduan dalam menggunakan Teknologi Informasi dan Komunikasi (TIK).	0.546	0.632	Tidak Valid
2	Terdapat sanksi bagi pelanggar kesiapan forensik digital.	0.624	0.632	Tidak Valid
3	Semua sumber daya informasi dan data di Pemerintah Daerah Yogyakarta dianggap sebagai hak milik.	0.661	0.632	Valid
4	Terdapat kebijakan yang menjelaskan bagaimana barang bukti digital harus diamankan.	0.875	0.632	Valid
5	Terdapat kebijakan yang menetapkan jenis barang bukti digital yang harus diamankan serta klasifikasinya.	0.855	0.632	Valid
6	Terdapat peraturan yang mengatur situasi dan cara ketika bukti yang telah diamankan dapat dilepaskan kepada pihak luar, termasuk ketika harus dirujuk ke penegak hukum.	0.370	0.632	Tidak Valid
7	Terdapat penetapan wewenang, tugas, dan tanggung jawab terkait pengumpulan, pemeliharaan, dan pemeriksaan barang bukti digital.	0.811	0.632	Valid

### 4.2.3 Komponen Technology & Security

Hasil dari uji validitas pertanyaan-pertanyaan komponen technology & security menunjukkan bahwa dari total 7 pertanyaan yang diuji, 3 pertanyaan menghasilkan nilai  $r_{hitung}$  yang lebih besar daripada nilai kritis  $r_{tabel}$  (0.632 pada tingkat signifikansi 5%), yang menandakan bahwa pertanyaan-pertanyaan tersebut dapat dikategorikan sebagai valid. Namun, terdapat 4 pertanyaan lainnya yang memiliki nilai  $r_{hitung}$  yang lebih rendah dari nilai kritis  $r_{tabel}$ , sehingga pertanyaan-pertanyaan ini dianggap tidak valid. Informasi detail mengenai hasil uji validitas ini dapat dilihat pada Tabel 4.3 yang terlampir di bawah ini..

**Tabel 4.3** Komponen Technology & Security

No	Pertanyaan	$r_{hitung}$	$r_{tabel}$	keterangan
1	Dilakukan manajemen log untuk setiap sistem, termasuk pemeliharaan dan administrasinya.	0.736	0.632	Valid
2	Terdapat sistem pengelolaan media penyimpanan (CD, hard disk, flash drive) untuk setiap komputer dan server.	0.447	0.632	Tidak Valid
3	Memiliki perangkat akuisisi dan analisis bukti digital, baik dalam bentuk perangkat keras (write block protector, dll) maupun perangkat lunak (alat analisis).	0.678	0.632	Valid
4	Memiliki proses untuk menjamin keamanan bukti, baik secara online maupun offline, melalui proses imaging dan duplikasi fisik.	0.733	0.632	Valid
5	Memiliki perangkat pendukung forensik digital seperti CCTV, sidik jari, dan otentikasi sistem.	0.254	0.632	Tidak Valid
6	Memiliki perangkat keamanan sistem seperti firewall dan antivirus.	0.532	0.632	Tidak Valid
7	Memiliki perangkat pendukung keamanan seperti enkripsi dan kriptografi.	0.569	0.632	Tidak Valid

### 4.2.4 Komponen Digital Forensic Response

Hasil dari uji validitas pertanyaan-pertanyaan komponen digital forensic response menunjukkan bahwa dari total 7 pertanyaan yang diuji, 5 pertanyaan

menghasilkan nilai  $r_{hitung}$  yang lebih besar daripada nilai kritis  $r_{tabel}$  (0.632 pada tingkat signifikansi 5%), yang menunjukkan bahwa pertanyaan-pertanyaan tersebut dapat dikategorikan sebagai valid. Namun, terdapat 2 pertanyaan lainnya yang memiliki nilai  $r_{hitung}$  yang lebih rendah dari nilai kritis  $r_{tabel}$ , sehingga pertanyaan-pertanyaan ini dianggap tidak valid. Informasi detail mengenai hasil uji validitas ini dapat dilihat pada Tabel 4.4 yang terlampir di bawah ini.

**Tabel 4.4** Digital Forensic Response

No	Pertanyaan	$r_{hitung}$	$r_{tabel}$	keterangan
1	Terdapat SOP (Standard Operating Procedure) untuk menangani insiden dan tindakan forensik digital.	0.925	0.632	Valid
2	Terdapat tenaga kerja yang memiliki sertifikasi atau keahlian dalam bidang forensik digital.	0.629	0.632	Tidak Valid
3	Tim respons terhadap kejahatan siber dan forensik digital telah dibentuk.	0.877	0.632	Valid
4	Pelatihan diberikan kepada tenaga kerja mengenai penanganan kejahatan siber dan forensik digital.	0.431	0.632	Tidak Valid
5	Terdapat panduan teknis untuk melaporkan insiden.	0.696	0.632	Valid
6	Terdapat materi visual seperti poster, spanduk, dan alat peraga lainnya yang memberikan panduan mengenai kejahatan siber.	0.735	0.632	Valid
7	Terdapat sekretariat yang khusus menangani informasi dan pelaporan kejahatan siber.	0.656	0.632	Valid

#### 4.2.5 Komponen Control & Risk

Hasil dari uji validitas pertanyaan-pertanyaan komponen control & risk menunjukkan bahwa dari total 6 pertanyaan yang diuji, semua pertanyaan menghasilkan nilai  $r_{hitung}$  yang lebih besar daripada nilai kritis  $r_{tabel}$  (0.632 pada tingkat signifikansi 5%), yang menandakan bahwa semua pertanyaan dapat

dikategorikan sebagai valid. Informasi detail mengenai hasil uji validitas ini dapat dilihat pada Tabel 4.5 yang terlampir di bawah ini.

**Tabel 4.5** Komponen Control & Risk

No	Pertanyaan	$r_{hitung}$	$r_{tabel}$	keterangan
1	Terdapat pengawasan inisiatif terhadap kesiapan forensik digital	0.902	0.632	Valid
2	Adanya program kesiapan forensik digital di Pemerintah Daerah Yogyakarta yang dievaluasi secara berkala	0.988	0.632	Valid
3	Terdapat program forensik digital di Pemerintah Daerah Yogyakarta yang diperkenalkan kepada seluruh anggota organisasi	0.988	0.632	Valid
4	Terdapat pemahaman tentang setiap proses forensik digital dan risiko kegagalan dalam setiap proses di Pemerintah Daerah Yogyakarta	0.929	0.632	Valid
5	Perangkat, alat, dan sistem forensik digital di Pemerintah Daerah Yogyakarta diperbarui secara rutin	0.801	0.632	Valid
6	Hasil investigasi forensik digital didiskusikan dan dipublikasikan kepada kepala departemen/sub bagian di Pemerintah Daerah Yogyakarta	0.833	0.632	Valid

#### 4.2.6 Komponen Legality

Hasil Hasil dari uji validitas pertanyaan-pertanyaan komponen legality menunjukkan bahwa dari total 5 pertanyaan yang diuji, 3 pertanyaan menghasilkan nilai  $r_{hitung}$  yang lebih besar daripada nilai kritis  $r_{tabel}$  (0.632 pada tingkat signifikansi 5%), yang menandakan bahwa pertanyaan-pertanyaan tersebut dapat dikategorikan sebagai valid. Namun, terdapat 2 pertanyaan lainnya yang memiliki nilai  $r_{hitung}$  yang lebih rendah dari nilai kritis 1, sehingga pertanyaan-pertanyaan ini dianggap tidak valid berdasarkan kriteria yang telah ditetapkan. Informasi detail mengenai hasil uji validitas ini dapat dilihat pada Tabel 4.6 yang terlampir di bawah ini.

**Tabel 4.6** Komponen Legality

No	Pertanyaan	$r_{hitung}$	$r_{tabel}$	keterangan
1	Terdapat kebijakan untuk pemeriksaan aspek hukum dalam setiap proses investigasi forensik digital dan insiden di Pemerintah Daerah Yogyakarta?	0.779	0.632	Valid
2	Penegak hukum, ahli, dan auditor profesional seperti PPNS (Penyidik Pegawai Negeri Sipil) dilibatkan dalam mengevaluasi forensik digital atau kejahatan siber di Pemerintah Daerah Yogyakarta	0.569	0.632	Tidak Valid
3	Setiap anggota institusi di Pemerintah Daerah Yogyakarta memahami undang-undang transaksi elektronik dan data digital	0.803	0.632	Valid
4	Peraturan dan undang-undang terkait transaksi elektronik dan data digital disosialisasikan di Pemerintah Daerah Yogyakarta	0.539	0.632	Tidak Valid
5	Pelatihan dalam penanganan kejahatan siber dan proses hukum dilakukan di Pemerintah Daerah Yogyakarta	0.696	0.632	Valid

### 4.3 NILAI INDEKS SETIAP KOMPONEN

Komponen dalam DiFRI terbagi menjadi 6 bagian yaitu Strategy, Policy & Procedure, Technology & Security, Digital Forensic Response, Control & Risk dan Legality. Setiap komponen dihitung secara terpisah untuk mengetahui nilai indeks disetiap komponennya, berikut adalah penjelasannya.

#### 4.3.1 Komponen Strategy

Nilai indeks komponen strategy seperti terlihat pada Tabel 4.7 dibawah ini menunjukkan nilai 78.5 % yang berarti dalam status siap. Untuk pertanyaan dengan indeks tertinggi yaitu pertanyaan nomor 2 dengan nilai 90 % dan berstatus sangat siap. Sedangkan untuk pertanyaan dengan nilai terendah yaitu pertanyaan nomor 1 dengan nilai 67,5 % dan berstatus siap.

**Tabel 4.7** Komponen Strategy

No	Pertanyaan	Total Nilai				Jumlah Total Nilai	Indeks (%)
		SS	S	TS	STS		
1	Memiliki program-program kesiapan forensik digital.	8	12	6	1	27	67,5
2	Terdapat aturan, regulasi, dan kewajiban terkait penyimpanan dokumen, file, dan rekaman (termasuk CCTV, log, dan dokumen lainnya).	24	12	0	0	36	90
3	Terdapat ketentuan yang berlaku saat terjadi peristiwa yang memerlukan barang bukti digital.	16	15	2	0	33	82,5
4	Melakukan identifikasi dan klasifikasi sumber-sumber dan jenis-jenis barang bukti digital yang berbeda.	20	6	6	0	32	80
5	Melakukan identifikasi dan sertifikasi teknologi serta sumber daya manusia yang diperlukan untuk memastikan kesiapan forensik digital.	8	15	6	0	29	72,5
Indeks Komponen (%)							78,5

#### 4.3.2 Komponen Policy & Procedure

Nilai indeks komponen policy & procedure seperti terlihat pada Tabel 4.8 dibawah ini menunjukkan nilai 79.375 % yang berarti dalam status siap. Untuk pertanyaan dengan indeks tertinggi yaitu pertanyaan nomor 1 dengan nilai 92.5 % dan berstatus sangat siap. Sedangkan untuk pertanyaan dengan nilai terendah yaitu pertanyaan nomor 2 dengan nilai 72.5 % dan berstatus siap.

**Tabel 4.8** Komponen Policy & Procedure

No	Pertanyaan	Total Nilai				Jumlah Total Nilai	Indeks (%)
		SS	S	TS	STS		
1	Semua sumber daya informasi dan data di Pemerintah Daerah Yogyakarta dianggap sebagai hak milik.	28	9	0	0	37	92,5
2	Terdapat kebijakan yang menjelaskan bagaimana barang bukti digital harus diamankan.	12	12	4	1	29	72,5
3	Terdapat kebijakan yang menetapkan jenis barang bukti digital yang harus diamankan serta klasifikasinya.	16	9	4	1	30	75
4	Terdapat penetapan wewenang, tugas, dan tanggung jawab terkait pengumpulan, pemeliharaan, dan pemeriksaan barang bukti digital.	12	15	4	0	31	77,5
Indeks Komponen (%)							79,375

#### 4.3.3 Komponen Technology & Security

Nilai indeks komponen technology & security seperti terlihat pada Tabel 4.9 dibawah ini menunjukkan nilai 77.5 % yang berarti dalam status siap. Untuk pertanyaan dengan indeks tertinggi yaitu pertanyaan nomor 1 dengan nilai 92.5 % dan berstatus sangat siap. Sedangkan untuk pertanyaan dengan nilai terendah yaitu pertanyaan nomor 2 dengan nilai 65 % dan berstatus siap.

**Tabel 4.9** Komponen Technology & Security

No	Pertanyaan	Total Nilai				Jumlah Total Nilai	Indeks (%)
		SS	S	TS	STS		

1	Dilakukan manajemen log untuk setiap sistem, termasuk pemeliharaan dan administrasinya.	28	9	0	0	37	92,5
2	Memiliki perangkat akuisisi dan analisis bukti digital, baik dalam bentuk perangkat keras (write block protector, dll) maupun perangkat lunak (alat analisis).	12	6	6	2	26	65
3	Memiliki proses untuk menjamin keamanan bukti, baik secara online maupun offline, melalui proses imaging dan duplikasi fisik.	16	9	4	1	30	75
Indeks Komponen (%)							77,5

#### 4.3.4 Komponen Digital Forensic Response

Nilai indeks komponen digital forensic response seperti terlihat pada Tabel 4.10 dibawah ini menunjukkan nilai 85.5 % yang berarti dalam status sangat siap. Untuk pertanyaan dengan indeks tertinggi yaitu pertanyaan nomor 3 dengan nilai 92.5 % dan berstatus sangat siap. Sedangkan untuk pertanyaan dengan nilai terendah yaitu pertanyaan nomor 1, 2 dan 4 dengan nilai 82.5 % dan berstatus sangat siap.

**Tabel 4.10** Komponen Digital Forensic Response

No	Pertanyaan	Total Nilai				Jumlah Total Nilai	Indeks (%)
		SS	S	TS	STS		
1	Terdapat SOP (Standard Operating Procedure) untuk menangani insiden dan tindakan forensik digital.	16	15	2	0	33	82,5
2	Tim respons terhadap kejahatan siber dan	16	15	2	0	33	82,5

	forensik digital telah dibentuk.						
3	Terdapat panduan teknis untuk melaporkan insiden.	28	9	0	0	37	92,5
4	Terdapat materi visual seperti poster, spanduk, dan alat peraga lainnya yang memberikan panduan mengenai kejahatan siber.	16	15	2	0	33	82,5
5	Terdapat sekretariat yang khusus menangani informasi dan pelaporan kejahatan siber.	24	9	2	0	35	87,5
Indeks Komponen (%)							85,5

#### 4.3.5 Komponen Control & Risk

Nilai indeks komponen control & risk seperti terlihat pada Tabel 4.11 dibawah ini menunjukkan nilai 55.83333 % yang berarti dalam cukup siap. Untuk pertanyaan dengan indeks tertinggi yaitu pertanyaan nomor 4 dengan nilai 60 % dan berstatus cukup siap. Sedangkan untuk pertanyaan dengan nilai terendah yaitu pertanyaan nomor 1, 2, 3, 5 dan 6 dengan nilai 55 % dan berstatus cukup siap.

**Tabel 4.11** Komponen Control & Risk

No	Pertanyaan	Total Nilai				Jumlah Total Nilai	Indeks (%)
		SS	S	TS	STS		
1	Terdapat pengawasan inisiatif terhadap kesiapan forensik digital	4	6	10	2	22	55
2	Adanya program kesiapan forensik digital di Pemerintah Daerah Yogyakarta yang dievaluasi secara berkala	0	12	8	2	22	55
3	Terdapat program forensik digital di	0	12	8	2	22	55

	Pemerintah Daerah Yogyakarta yang diperkenalkan kepada seluruh anggota organisasi						
4	Terdapat pemahaman tentang setiap proses forensik digital dan risiko kegagalan dalam setiap proses di Pemerintah Daerah Yogyakarta	4	12	6	2	24	60
5	Perangkat, alat, dan sistem forensik digital di Pemerintah Daerah Yogyakarta diperbarui secara rutin	0	12	8	2	22	55
6	Hasil investigasi forensik digital didiskusikan dan dipublikasikan kepada kepala departemen/sub bagian di Pemerintah Daerah Yogyakarta	0	12	8	2	22	55
Indeks Komponen (%)							55,83333

#### 4.3.6 Komponen Legality

Nilai indeks komponen legality seperti terlihat pada Tabel 4.12 dibawah ini menunjukkan nilai 70.83333 % yang berarti dalam status siap. Untuk pertanyaan dengan indeks tertinggi yaitu pertanyaan nomor 2 dan 3 dengan nilai 75 % dan berstatus siap. Sedangkan untuk pertanyaan dengan nilai terendah yaitu pertanyaan nomor 1 dengan nilai 62,5 % dan berstatus siap.

**Tabel 4.12** Komponen Legality

No	Pertanyaan	Total Nilai				Jumlah Total Nilai	Indeks (%)
		SS	S	TS	STS		
1	Terdapat kebijakan untuk pemeriksaan	8	6	10	1	25	62,5

	aspek hukum dalam setiap proses investigasi forensik digital dan insiden di Pemerintah Daerah Yogyakarta?						
2	Setiap anggota institusi di Pemerintah Daerah Yogyakarta memahami undang-undang transaksi elektronik dan data digital	4	24	2	0	30	75
3	Pelatihan dalam penanganan kejahatan siber dan proses hukum dilakukan di Pemerintah Daerah Yogyakarta	12	12	6	0	30	75
Indeks Komponen (%)							70,83333

#### 4.4 NILAI DiFRI

Nilai DiFRI (*Digital Forensic Readiness Index*) dihitung sebagai jumlah dari semua indeks setiap komponen yang diukur dalam penelitian. Setiap komponen memiliki nilai indeks yang diperoleh dari hasil kuesioner, yang mencerminkan tingkat kesiapan forensik digital dalam aspek tertentu. Seperti yang terlihat pada Tabel 4.13, nilai DiFRI keseluruhan adalah 74,59028%. Nilai ini memberikan gambaran keseluruhan tentang kesiapan forensik digital yang ada berdasarkan pengukuran enam komponen utama.

**Tabel 4.13** Nilai DiFRI

No	Komponen	Indeks (%)
1	Strategy	78,5
2	Policy & Procedure	79,375
3	Technology & Security	77,5
4	Digital Forensic Response	85,5
5	Control & Risk	55,83333
6	Legality	70,83333
Nilai DiFRI (%)		74,59028

## 4.5 PEMBAHASAN

### 4.5.1 Tingkat Kesiapan

Hasil evaluasi berdasarkan wawancara dan kuesioner menunjukkan tingkat kesiapan forensik digital yang signifikan. Pemerintah Kota Yogyakarta berhasil mencapai nilai DiFRI sebesar 74,59027778% dengan status "siap", mengindikasikan dedikasi mereka dalam mempersiapkan diri menghadapi ancaman keamanan digital. Secara rinci, komponen-komponen evaluasi menunjukkan nilai indeks DiFRI sebagai berikut:

1. Strategy mencapai 78,5% dengan status "siap"
2. Policy & Procedure mencapai 79,375% dengan status "siap"
3. Technology & Security mencapai 77,5% dengan status "siap"
4. Digital Forensic Response mencapai 85,5% dengan status "sangat siap"
5. Control & Risk mencapai 55,83333333% dengan status "cukup siap"
6. Legality mencapai 70,83333333% dengan status "siap".

Hasil ini menegaskan bahwa Pemerintah Kota Yogyakarta telah mengambil langkah konkret dalam mengimplementasikan strategi keamanan digital, merumuskan kebijakan yang sesuai, mengadopsi teknologi canggih, serta mempersiapkan tim respons forensik digital yang terlatih. Kesiapan ini tidak hanya meningkatkan kemampuan mereka dalam mendeteksi, mengatasi, dan memulihkan dari serangan keamanan digital, tetapi juga memastikan bahwa kebijakan hukum terpenuhi dalam proses penanganan insiden. Dengan demikian, Pemerintah Kota Yogyakarta siap menghadapi tantangan yang kompleks di era digital saat ini, menjaga keamanan infrastruktur dan data publik dengan efektif dan bertanggung jawab.

### 4.5.2 Faktor-faktor yang Mempengaruhi Kesiapan Forensik Digital

Berikut ini adalah faktor-faktor yang mempengaruhi tingkat kesiapan forensik digital di Pemerintah Kota Yogyakarta berdasarkan jawaban kuesioner:

1. Strategi

Pemerintah Kota Yogyakarta memiliki berbagai program kesiapan forensik digital, termasuk aturan regulasi dan kewajiban terkait penyimpanan

dokumen dan rekaman, ketentuan dalam menangani barang bukti digital, serta identifikasi dan sertifikasi teknologi dan sumber daya manusia yang diperlukan untuk forensik digital.

## 2. Kebijakan dan Prosedur

Adanya kebijakan dan prosedur yang menjadi panduan dalam penggunaan Teknologi Informasi dan Komunikasi (TIK), termasuk sanksi bagi pelanggaran, kepemilikan data, serta aturan pengamanan dan pelepasan barang bukti digital.

## 3. Teknologi dan Keamanan

Pemerintah memiliki sistem manajemen log, pengelolaan media penyimpanan, perangkat akuisisi dan analisis bukti digital, serta perangkat keamanan seperti firewall, antivirus, dan teknologi enkripsi.

## 4. Tanggapan Forensik Digital

Terdapat SOP untuk menangani insiden dan tindakan forensik digital, tenaga kerja bersertifikasi, tim respons kejahatan siber, serta pelatihan dan panduan teknis dalam melaporkan insiden.

## 5. Pengendalian dan Risiko

Program kesiapan forensik digital dievaluasi secara berkala, diperkenalkan kepada seluruh anggota organisasi, dan terdapat pemahaman tentang risiko kegagalan dalam proses forensik digital.

## 6. Legalitas

Kebijakan pemeriksaan aspek hukum dalam proses investigasi, keterlibatan penegak hukum dan auditor profesional, pemahaman undang-undang transaksi elektronik, serta sosialisasi dan pelatihan terkait kejahatan siber dan proses hukum.

Faktor-faktor tersebut secara komprehensif mencakup berbagai aspek penting dalam kesiapan forensik digital, mulai dari strategi, kebijakan, teknologi, respons insiden, pengendalian risiko, hingga aspek legalitas.

### 4.5.3 Strategi untuk Meningkatkan Kesiapan Forensik Digital

Berdasarkan hasil analisis, komponen Control & Risk adalah komponen yang paling rendah indeks-nya dalam laporan tersebut, terdapat beberapa kekurangan yang dapat diatasi untuk meningkatkan kesiapan forensik digital di Pemerintah Kota Yogyakarta. Berikut adalah strategi yang diusulkan untuk mengatasi kekurangan tersebut:

1. Membentuk tim pengawasan khusus yang bertanggung jawab untuk memonitor dan mengevaluasi inisiatif kesiapan forensik digital secara berkala. Tim ini harus melibatkan anggota dari berbagai departemen untuk memastikan pengawasan yang menyeluruh dan komprehensif.
2. Mengimplementasikan jadwal evaluasi rutin terhadap program kesiapan forensik digital. Evaluasi ini harus mencakup penilaian terhadap efektivitas program, identifikasi kelemahan, dan perbaikan yang diperlukan. Hasil evaluasi harus didokumentasikan dan disosialisasikan kepada semua pemangku kepentingan.
3. Menyelenggarakan sesi pelatihan dan workshop secara rutin untuk seluruh anggota organisasi tentang program forensik digital yang ada. Materi pelatihan harus mencakup pentingnya kesiapan forensik digital dan prosedur yang harus diikuti.
4. Mengadakan sesi edukasi untuk meningkatkan pemahaman tentang setiap proses forensik digital dan risiko yang terkait. Pemahaman ini harus melibatkan semua anggota organisasi, terutama mereka yang terlibat langsung dalam penanganan barang bukti digital.
5. Menetapkan kebijakan pembaruan perangkat dan sistem forensik digital secara berkala. Kebijakan ini harus mencakup identifikasi teknologi baru yang relevan dan alokasi anggaran untuk pembaruan perangkat serta pelatihan penggunaannya.
6. Membuat sistem untuk mendiskusikan dan mempublikasikan hasil investigasi forensik digital kepada kepala departemen dan sub bagian terkait. Tujuannya adalah untuk memastikan bahwa hasil investigasi digunakan untuk perbaikan proses dan peningkatan keamanan digital.

Dengan mengimplementasikan strategi-strategi ini, diharapkan kesiapan forensik digital di Pemerintah Kota Yogyakarta dapat ditingkatkan secara signifikan, sehingga lebih siap dalam menghadapi dan menangani kejahatan siber.

UNIVERSITAS JENDERAL ACHMAD YANI  
PERPUSTAKAAN  
YOGYAKARTA