

UJIAN AKHIR SEMESTER
MATA KULIAH KEAMANAN WEB



Disusun oleh :

NAMA ANGGOTA		NIM
M. Khoulifuji Wantoro Aji	:	21.01.4657
Muhammad Arpiansyah	:	21.01.4602
Idola Aji Bayu P	:	21.01.4607

FAKULTAS ILMU KOMPUTER
PRODI D3 TEKNIK INFORMATIKA
UNIVERSITAS AMIKOM
YOGYAKARTA

DAFTAR ISI

BAB I	3
Latar Belakang.....	3
Penjelasan tentang objek.....	3
BAB II	4
I Kategori SE	4
II Tata Kelola.....	5
III Resiko	6
IV Kerangka Kerja	7
V Pengelolaan Aset	8
VI Teknologi.....	10
VII Suplemen	12
BAB III	15
3.1 Meningkatkan kematangan	15
3.2 Kelayakan / Efektifitas.....	17

BAB I

Latar Belakang

Pekapuran Raya adalah sebuah instansi pemerintahan yang berada di tingkat paling bawah dalam struktur administrasi di Indonesia. Terletak di kecamatan tertentu, kelurahan merupakan unit terkecil dalam pembagian administratif suatu daerah, bertanggung jawab atas pelayanan masyarakat di wilayahnya.

Indeks Keamanan Informasi (Indeks KAMI)

Identitas Instansi atau Perusahaan	<i>Kantor Kecamatan</i>
Alamat	<i>Desa Muser Kec.Muara Samu Kab.Paser, Kaltim</i>
Nomor Telpon	<i>085251519561</i>
Email	<i>sahrulsekdes@gmail.com</i>
Pengisi Lembar Evaluasi	<i>Sahrul</i>
Jabatan	<i>Staf di kantor Kecamatan</i>
Tanggal Pengisian	<div>Kekurangan pegawai yg ASN</div>
Deskripsi Ruang Lingkup	<i>Isi dengan deskripsi ruang lingkup struktur organisasi (Departemen, Bagian atau Satuan Kerja) dan infrastruktur TIK</i>

Penjelasan tentang objek

Kantor Kecamatan adalah kantor kecamatan yang berada di suatu Desa Muser, Kecamatan Muara Samu, Kabupaten Paser, Kalimantan timur. Kelurahan ini merupakan salah unit administratif di Indonesia, yang bertanggung jawab atas pelayanan masyarakat di wilayahnya.

Memiliki sejarah pendirian dan perkembangannya sendiri. Informasi sejarah ini mungkin mencakup tahun berdirinya kelurahan, asal usul nama, dan peristiwa penting yang terjadi di wilayah tersebut. Sejarah dapat memberikan gambaran tentang perkembangan sosial, ekonomi, dan budaya kelurahan seiring waktu.

Kantor Kecamatan ini memiliki populasi penduduk yang tinggal di dalam wilayahnya. Informasi demografis seperti jumlah penduduk, usia, jenis kelamin, dan latar belakang sosial budaya dapat memberikan gambaran tentang keragaman masyarakat yang tinggal di kelurahan tersebut.

BAB II

I Kategori SE

Bisa dilihat pada gambar bawah ini :

[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		Status	Skor	NOMOR DOKUMEN	NAMA DOKUMEN
#	Karakteristik Instansi/Perusahaan				
1.1	Nilai investasi sistem elektronik yang terpasang (A) Lebih dari Rp.30 Miliar (B) Lebih dari Rp.3 Miliar s/d Rp.30 Miliar (C) Kurang dari Rp.3 Miliar	C	1	1.1	
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik (A) Lebih dari Rp.10 Miliar (B) Lebih dari Rp.1 Miliar s/d Rp.10 Miliar (C) Kurang dari Rp.1 Miliar	C	1	1.2	
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu (A) Peraturan atau Standar nasional dan internasional (B) Peraturan atau Standar nasional (C) Tidak ada Peraturan khusus	C	1	1.3	
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik (A) Teknik kriptografi khusus yang disertifikasi oleh Negara (B) Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri (C) Tidak ada penggunaan teknik kriptografi	C	1	1.4	
1.5	Jumlah pengguna Sistem Elektronik (A) Lebih dari 5.000 pengguna (B) 1.000 sampai dengan 5.000 pengguna (C) Kurang dari 1.000 pengguna	C	1	1.5	
1.6	Data pribadi yang dikelola Sistem Elektronik (A) Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya (B) Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha (C) Tidak ada data pribadi	A	5	1.6	
1.7	Tingkat klasifikasi/kekritisian Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi (A) Sangat Rahasia (B) Rahasia dan/atau Terbatas (C) Biasa	A	5	1.7	
1.8	Tingkat kekritisian proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi (A) Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik (B) Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung (C) Proses yang hanya berdampak pada bisnis perusahaan	A	5	1.8	
1.9	Dampak dari kegagalan Sistem Elektronik (A) Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara (B) Tidak tersedianya layanan publik dalam 1 propinsi atau lebih (C) Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	A	5	1.9	
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) (A) Menimbulkan korban jiwa (B) Terbatas pada kerugian finansial (C) Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	C	1	1.10	
Skor penetapan Kategori Sistem Elektronik		26			

- Point 1.1 status nya C dengan skor 1
- Point 1.2 status nya C dengan skor 1
- Point 1.3 status nya C dengan skor 1
- Point 1.4 status nya C dengan skor 1
- Point 1.5 status nya C dengan skor 1
- Point 1.6 status nya A dengan skor 5
- Point 1.7 status nya A dengan skor 5
- Point 1.8 status nya A dengan skor 5
- Point 1.9 status nya A dengan skor 5
- Point 1.10 status nya C dengan skor 1

Maka hasil dari **I Kategori SE** ini adalah **26** dengan tingkat ketergantungan **Tinggi**

II Tata Kelola

Bisa dilihat pada gambar bawah ini :

[illegible]

- Point 2.1 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 2.2 status nya Diterapkan Secara Menyeluruh dengan skor 3
- Point 2.3 status nya Diterapkan Secara Menyeluruh dengan skor 3
- Point 2.4 status nya Dalam Perencanaan dengan skor 1
- Point 2.5 status nya Diterapkan Secara Menyeluruh dengan skor 3
- Point 2.6 status nya Dalam Perencanaan dengan skor 1
- Point 2.7 status nya Dalam Perencanaan dengan skor 1
- Point 2.8 status nya Dalam Perencanaan dengan skor 1
- Point 2.9 status nya Diterapkan Secara Menyeluruh dengan skor 6
- Point 2.10 status nya Diterapkan Secara Menyeluruh dengan skor 6
- Point 2.11 status nya Diterapkan Secara Menyeluruh dengan skor 6
- Point 2.12 status nya Diterapkan secara menyeluruh dengan skor 6
- Point 2.13 status nya Diterapkan secara menyeluruh dengan skor 6
- Point 2.14 status nya Dalam Perencanaan dengan skor 2
- Point 2.15 status nya Diterapkan secara menyeluruh dengan skor 6
- Point 2.16 status nya Dalam Penerapan / Diterapkan Sebagian dengan skor 4
- Point 2.17 status nya Diterapkan secara menyeluruh dengan skor 9
- Point 2.18 status nya Diterapkan secara menyeluruh dengan skor 9
- Point 2.19 status nya Diterapkan secara menyeluruh dengan skor 9
- Point 2.20 status nya Diterapkan secara menyeluruh dengan skor 9
- Point 2.21 status nya Dalam Perencanaan dengan skor 3

- Point 2.22 status nya Dalam Perencanaan dengan skor 3

Maka nilai evaluasi hasil dari **II Tata Kelola** ini adalah **99**

III Resiko

Bisa dilihat pada gambar bawah ini :

Bagian III: Pengelolaan Risiko Keamanan Informasi										
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.										
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh							Status	Skor	NOMOR DOKUMEN	NAMA DOKUMEN
#	Kajian Risiko Keamanan Informasi									
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?				Dalam Perencanaan	1	3.1	
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?				Dalam Perencanaan	1	3.2	
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?				Dalam Penerapan / Diterapkan Sebagian	2	3.3	
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?				Dalam Perencanaan	1	3.4	
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?				Dalam Perencanaan	1	3.5	
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?				Diterapkan Secara Menyeluruh	3	3.6	Prinsip dan kebijakan yang mengatur kepemilikan dan pengelolaan aset informasi dalam perusahaan kecamatan. Dokumen ini mencakup definisi kepemilikan, tanggung jawab pihak pengelola (custodian), proses penunjukan pemilik aset, serta kriteria dan persyaratan pengelolaan aset informasi.
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?				Dalam Perencanaan	1	3.7	
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?				Dalam Perencanaan	1	3.8	
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisis/ajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?				Dalam Perencanaan	1	3.9	
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?				Dalam Perencanaan	1	3.10	
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?				Dalam Perencanaan	2	3.11	
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?				Dalam Penerapan / Diterapkan Sebagian	4	3.12	
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang objektif/terukur untuk memastikan konsistensi dan efektivitasnya?				Dalam Penerapan / Diterapkan Sebagian	4	3.13	
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?				Dalam Perencanaan	2	3.14	
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektivitasnya?				Dalam Perencanaan	0	3.15	
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian objektif kinerja efektivitas pengamanan?				Dalam Perencanaan	0	3.16	
Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi							25			

- Point 3.1 status nya Dalam perencanaan dengan skor 1
- Point 3.2 status nya Dalam perencanaan dengan skor 1
- Point 3.3 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 3.4 status nya Dalam perencanaan dengan skor 1
- Point 3.5 status nya Dalam perencanaan dengan skor 1
- Point 3.6 status nya Diterapkan secara menyeluruh dengan skor 3
- Point 3.7 status nya Dalam perencanaan dengan skor 1
- Point 3.8 status nya Dalam perencanaan dengan skor 1
- Point 3.9 status nya Dalam perencanaan dengan skor 1
- Point 3.10 status nya Dalam perencanaan dengan skor 1
- Point 3.11 status nya Dalam perencanaan dengan skor 2
- Point 3.12 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
- Point 3.13 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
- Point 3.14 status nya Dalam perencanaan dengan skor 2
- Point 3.15 status nya Dalam perencanaan dengan skor 0
- Point 3.16 status nya Dalam perencanaan dengan skor 0

Maka nilai evaluasi hasil dari **III Risiko** pengelolaan risiko keamanan informasi adalah **25**

IV Kerangka Kerja

Bisa dilihat pada gambar bawah ini :

Bagian IV: Kerangka Kerja Pengelolaan Kemauan Informasi									
Bagian ini menguraikan kebijakan dan prosedur kerangka kerja (Bingkai Kerja) pengelolaan kemauan informasi dan strategi pengumpulan data.									
Mencakup		Tidak Dilakukan		Dilakukan		Dilakukan		Dilakukan	
Mencakup		Tidak Dilakukan		Dilakukan		Dilakukan		Dilakukan	
4.1	1	1	1	1	1	1	1	1	1
4.2	1	1	1	1	1	1	1	1	1
4.3	1	1	1	1	1	1	1	1	1
4.4	1	1	1	1	1	1	1	1	1
4.5	1	1	1	1	1	1	1	1	1
4.6	1	1	1	1	1	1	1	1	1
4.7	1	1	1	1	1	1	1	1	1
4.8	1	1	1	1	1	1	1	1	1
4.9	1	1	1	1	1	1	1	1	1
4.10	1	1	1	1	1	1	1	1	1
4.11	1	1	1	1	1	1	1	1	1
4.12	1	1	1	1	1	1	1	1	1
4.13	1	1	1	1	1	1	1	1	1
4.14	1	1	1	1	1	1	1	1	1
4.15	1	1	1	1	1	1	1	1	1
4.16	1	1	1	1	1	1	1	1	1
4.17	1	1	1	1	1	1	1	1	1
4.18	1	1	1	1	1	1	1	1	1
4.19	1	1	1	1	1	1	1	1	1
4.20	1	1	1	1	1	1	1	1	1
4.21	1	1	1	1	1	1	1	1	1
4.22	1	1	1	1	1	1	1	1	1
4.23	1	1	1	1	1	1	1	1	1
4.24	1	1	1	1	1	1	1	1	1
4.25	1	1	1	1	1	1	1	1	1
4.26	1	1	1	1	1	1	1	1	1
4.27	1	1	1	1	1	1	1	1	1
4.28	1	1	1	1	1	1	1	1	1
4.29	1	1	1	1	1	1	1	1	1
4.30	1	1	1	1	1	1	1	1	1
4.31	1	1	1	1	1	1	1	1	1
4.32	1	1	1	1	1	1	1	1	1
4.33	1	1	1	1	1	1	1	1	1
4.34	1	1	1	1	1	1	1	1	1
4.35	1	1	1	1	1	1	1	1	1
4.36	1	1	1	1	1	1	1	1	1
4.37	1	1	1	1	1	1	1	1	1
4.38	1	1	1	1	1	1	1	1	1
4.39	1	1	1	1	1	1	1	1	1
4.40	1	1	1	1	1	1	1	1	1
4.41	1	1	1	1	1	1	1	1	1
4.42	1	1	1	1	1	1	1	1	1
4.43	1	1	1	1	1	1	1	1	1
4.44	1	1	1	1	1	1	1	1	1
4.45	1	1	1	1	1	1	1	1	1
4.46	1	1	1	1	1	1	1	1	1
4.47	1	1	1	1	1	1	1	1	1
4.48	1	1	1	1	1	1	1	1	1
4.49	1	1	1	1	1	1	1	1	1
4.50	1	1	1	1	1	1	1	1	1
4.51	1	1	1	1	1	1	1	1	1
4.52	1	1	1	1	1	1	1	1	1
4.53	1	1	1	1	1	1	1	1	1
4.54	1	1	1	1	1	1	1	1	1
4.55	1	1	1	1	1	1	1	1	1
4.56	1	1	1	1	1	1	1	1	1
4.57	1	1	1	1	1	1	1	1	1
4.58	1	1	1	1	1	1	1	1	1
4.59	1	1	1	1	1	1	1	1	1
4.60	1	1	1	1	1	1	1	1	1
4.61	1	1	1	1	1	1	1	1	1
4.62	1	1	1	1	1	1	1	1	1
4.63	1	1	1	1	1	1	1	1	1
4.64	1	1	1	1	1	1	1	1	1
4.65	1	1	1	1	1	1	1	1	1
4.66	1	1	1	1	1	1	1	1	1
4.67	1	1	1	1	1	1	1	1	1
4.68	1	1	1	1	1	1	1	1	1
4.69	1	1	1	1	1	1	1	1	1
4.70	1	1	1	1	1	1	1	1	1
4.71	1	1	1	1	1	1	1	1	1
4.72	1	1	1	1	1	1	1	1	1
4.73	1	1	1	1	1	1	1	1	1
4.74	1	1	1	1	1	1	1	1	1
4.75	1	1	1	1	1	1	1	1	1
4.76	1	1	1	1	1	1	1	1	1
4.77	1	1	1	1	1	1	1	1	1
4.78	1	1	1	1	1	1	1	1	1
4.79	1	1	1	1	1	1	1	1	1
4.80	1	1	1	1	1	1	1	1	1
4.81	1	1	1	1	1	1	1	1	1
4.82	1	1	1	1	1	1	1	1	1
4.83	1	1	1	1	1	1	1	1	1
4.84	1	1	1	1	1	1	1	1	1
4.85	1	1	1	1	1	1	1	1	1
4.86	1	1	1	1	1	1	1	1	1
4.87	1	1	1	1	1	1	1	1	1
4.88	1	1	1	1	1	1	1	1	1
4.89	1	1	1	1	1	1	1	1	1
4.90	1	1	1	1	1	1	1	1	1
4.91	1	1	1	1	1	1	1	1	1
4.92	1	1	1	1	1	1	1	1	1
4.93	1	1	1	1	1	1	1	1	1
4.94	1	1	1	1	1	1	1	1	1
4.95	1	1	1	1	1	1	1	1	1
4.96	1	1	1	1	1	1	1	1	1
4.97	1	1	1	1	1	1	1	1	1
4.98	1	1	1	1	1	1	1	1	1
4.99	1	1	1	1	1	1	1	1	1
4.100	1	1	1	1	1	1	1	1	1
42									

Penyusunan dan pengelolaan kebijakan & prosedur keamanan informasi

- Point 4.1 status nya Dalam perencanaan dengan skor 1
- Point 4.2 status nya Diterapkan secara menyeluruh dengan skor 3
- Point 4.3 status nya Diterapkan secara menyeluruh dengan skor 3
- Point 4.4 status nya Tidak dilakukan dengan skor 0
- Point 4.5 status nya Tidak dilakukan dengan skor 0
- Point 4.6 status nya Tidak dilakukan dengan skor 0
- Point 4.7 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 4.8 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
- Point 4.9 status nya Dalam perencanaan dengan skor 2
- Point 4.10 status nya Tidak dilakukan dengan skor 0
- Point 4.11 status nya Dalam perencanaan dengan skor 2
- Point 4.12 status nya Dalam perencanaan dengan skor 2
- Point 4.13 status nya Dalam perencanaan dengan skor 2
- Point 4.14 status nya Dalam perencanaan dengan skor 2

- Point 5.1 status nya Dalam perencanaan dengan skor 1

- Point 5.2 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 5.3 status nya Dalam perencanaan dengan skor 1
- Point 5.4 status nya Dalam perencanaan dengan skor 1
- Point 5.5 status nya Tidak dilakukan dengan skor 0
- Point 5.6 status nya Tidak dilakukan dengan skor 0
- Point 5.7 status nya Dalam perencanaan dengan skor 1
- Point 5.8 status nya Tidak dilakukan dengan skor 0
- Point 5.9 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 5.10 status nya Tidak dilakukan dengan skor 0
- Point 5.11 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 5.12 status nya Dalam perencanaan dengan skor 1
- Point 5.13 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 5.14 status nya Dalam perencanaan dengan skor 1
- Point 5.15 status nya Dalam perencanaan dengan skor 1
- Point 5.16 status nya Dalam perencanaan dengan skor 1
- Point 5.17 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 5.18 status nya Dalam perencanaan dengan skor 1
- Point 5.19 status nya Tidak dilakukan dengan skor 0
- Point 5.20 status nya Tidak dilakukan dengan skor 0
- Point 5.21 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
- Point 5.22 status nya Tidak dilakukan dengan skor 0
- Point 5.23 status nya Dalam perencanaan dengan skor 2
- Point 5.24 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
- Point 5.25 status nya Dalam penerapan / Diterapkan sebagian dengan skor 0
- Point 5.26 status nya Dalam penerapan / Diterapkan sebagian dengan skor 0
- Point 5.27 status nya Tidak dilakukan dengan skor 0

Pengamanan fisik

- Point 5.27 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 5.28 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 5.30 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 5.31 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 5.32 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 5.33 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 5.34 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 5.35 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 5.36 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 5.37 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 5.38 status nya Dalam perencanaan dengan skor 0
- Maka nilai evaluasi hasil dari **V Pengelolaan Aset** adalah **57**

VI Teknologi

Bisa dilihat pada gambar bawah ini :

Bagian VI: Teknologi dan Keamanan Informasi								
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.								
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh					Status	Skor	NOMOR DOKUMEN	NAMA DOKUMEN
#	Pengamanan Teknologi							
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Dalam Perencanaan	1	6.1		
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Dalam Perencanaan	1	6.2		
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dalam Penerapan / Diterapkan Sebagian	2	6.3		
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kebutuhan penerapan konfigurasi standar yang ada?	Dalam Perencanaan	1	6.4		
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/kebutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2	6.5		
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundansi) sesuai kebutuhan/peryaratan yang ada?	Dalam Perencanaan	1	6.6		
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Dalam Perencanaan	1	6.7		
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Perencanaan	1	6.8		
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Perencanaan	1	6.9		
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan	1	6.10		
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Penerapan / Diterapkan Sebagian	2	6.11		
6.12	II	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh	6	6.12	Enkripsi ini mengatur penggunaan enkripsi dalam perlindungan data dan komunikasi di dalam perusahaan/kecamatan. Dalam hal ini mencakup persyaratan penggunaan enkripsi pada perangkat, komunikasi melalui jaringan, penyimpanan data, serta kebijakan pengelolaan kunci enkripsi.	
6.13	II	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Penerapan / Diterapkan Sebagian	4	6.13		
6.14	II	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/penggunaannya dan penggunaan kembali password lama?	Dalam Perencanaan	2	6.14		
6.15	II	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Tidak Dilakukan	0	6.15		
6.16	II	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeout, lockout setelah kegagalan login, dan penarikan akses?	Dalam Perencanaan	2	6.16		
6.17	II	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Perencanaan	2	6.17		
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	2	6.18		
6.19	II	1	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Diterapkan Secara Menyeluruh	3	6.19		
6.20	II	1	Apakah setiap desktop dan server dilindungi dari penyerangan virus/malware?	Dalam Penerapan / Diterapkan Sebagian	2	6.20		
6.21	II	2	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Dalam Penerapan / Diterapkan Sebagian	4	6.21		
6.22	II	2	Apakah adanya laporan penyerangan virus/malware yang gagal/berhasil ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagian	4	6.22		
6.23	II	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Perencanaan	2	6.23		
6.24	II	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Dalam Perencanaan	2	6.24		
6.25	II	3	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	Dalam Perencanaan	3	6.25		
6.26	II	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji keadaan keamanan informasi secara rutin?	Dalam Perencanaan	0	6.26		
Total Nilai Evaluasi Teknologi dan Keamanan Informasi					52			

Pengamanan Teknologi

- Point 6.1 status nya Dalam perencanaan dengan skor 1
- Point 6.2 status nya Dalam perencanaan dengan skor 1
- Point 6.3 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 6.4 status nya Dalam perencanaan dengan skor 1
- Point 6.5 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 6.6 status nya Dalam perencanaan dengan skor 1
- Point 6.7 status nya Dalam perencanaan dengan skor 1

- Point 6.8 status nya Dalam perencanaan dengan skor 1
 - Point 6.9 status nya Dalam perencanaan dengan skor 1
 - Point 6.10 status nya Dalam perencanaan dengan skor 1
 - Point 6.11 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 6.12 status nya Diterapkan secara menyeluruh dengan skor 6
 - Point 6.13 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 6.14 status nya Dalam perencanaan dengan skor 2
 - Point 6.15 status nya Tidak dilakukan dengan skor 0
 - Point 6.16 status nya Dalam perencanaan dengan skor 2
 - Point 6.17 status nya Dalam perencanaan dengan skor 2
 - Point 6.18 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 6.19 status nya Diterapkan secara menyeluruh dengan skor 3
 - Point 6.20 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 6.21 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 6.22 status nya Dalam penerapan / Diterapkan sebagian dengan skor 4
 - Point 6.23 status nya Dalam perencanaan dengan skor 2
 - Point 6.24 status nya Dalam perencanaan dengan skor 2
 - Point 6.25 status nya Dalam perencanaan dengan skor 3
 - Point 6.26 status nya Dalam perencanaan dengan skor 0
- Maka nilai evaluasi hasil dari **VI Teknologi** pengelolaan aset adalah **52**

7.2	Pengamanan Laganan Infrastruktur Binaan Kelas Standar		1.38		
7.2.1	1) Apakah insulasi perancah sudah melakukan kajian risiko terkait pengaman laganan berisiko aloof dan menggunakan kebijakan manajemen informasi terkait laganan aloof?	Dalam Perencanaan	1	7.2.1	
7.2.2	2) Apakah insulasi perancah sudah menerapkan dalam upaya yang akan diimpas/dilakukan/dipertahankan melalui laganan berisiko aloof?	alam Penerapan / Diterapkan Sekali	2	7.2.2	
7.2.3	3) Apakah insulasi perancah sudah menerapkan langkah pengaman dalam pribadi yang diimpas/dilakukan/dipertahankan melalui laganan aloof?	Dalam Perencanaan	1	7.2.3	
7.2.4	4) Apakah insulasi perancah sudah memiliki, menerapkan kriteria dan memelihara aspek hukum (perizinan, hak dan kewajiban) terkait pengaman laganan berisiko aloof?	Tidak Dilakukan	0	7.2.4	
7.2.5	5) Apakah insulasi perancah sudah menggunakan prosedur laganan aloof terkait regulasi pengaman aloof?	Dalam Perencanaan	1	7.2.5	
7.2.6	6) Apakah insulasi perancah sudah menerapkan standar keamanan teknis pengaman laganan aloof, termasuk aspek pengaman aloof yang ada di internal insulasi perancah?	Tidak Dilakukan	0	7.2.6	
7.2.7	7) Apakah insulasi perancah sudah menggunakan kebijakan keamanan laganan aloof termasuk aspek keselamatan dan keamanan informasi laganan berisiko ISO 27002?	alam Penerapan / Diterapkan Sekali	2	7.2.7	
7.2.8	8) Apakah insulasi perancah sudah memiliki kebijakan, alir alir dan prosedur untuk menguji laganan aloof dan menggunakan fasilitas pengujian apabila terjadi kegagalan keamanan pada laganan berisiko?	alam Penerapan / Diterapkan Sekali	2	7.2.8	
7.2.9	9) Apakah insulasi perancah sudah memiliki prosedur pengujian terkait laganan aloof?	alam Penerapan / Diterapkan Sekali	2	7.2.9	
7.2.10	10) Apakah insulasi perancah sudah memiliki prosedur untuk menguji laganan aloof, termasuk prosedur pengaman dalam yang ada (termasuk dan menggunakan aloof)?	alam Penerapan / Diterapkan Sekali	2	7.2.10	
7.3	7.3.1		1.44		
7.3.1	1) Apakah insulasi perancah sudah melakukan kajian risiko terkait laganan berisiko aloof/berisiko dalam pribadi yang diimpas, dilak dan dipertahankan dengan pihak eksternal?	alam Penerapan / Diterapkan Sekali	2	7.3.1	
7.3.2	2) Apakah insulasi perancah sudah melakukan alir pengaman dalam di internal dan pelaksanaan dalam dengan pihak eksternal, termasuk kapan dan dimana dalam pribadi terkait dipertah?	alam Penerapan / Diterapkan Sekali	2	7.3.2	
7.3.3	3) Apakah prosedur terkait pengaman, pelaksanaan dan pelaksanaan dalam pribadi di insulasi perancah sudah dilakukan aloof?	Dalam Perencanaan	1	7.3.3	
7.3.4	4) Apakah insulasi perancah sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Dalam Perencanaan	1	7.3.4	
7.3.5	5) Apakah insulasi perancah sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	alam Penerapan / Diterapkan Sekali	2	7.3.5	
7.3.6	6) Apakah insulasi perancah sudah menggunakan dampak terkait laganan aloof dalam pribadi yang diimpas, dilak dan dipertahankan secara legal dan karena insiden lain?	alam Penerapan / Diterapkan Sekali	2	7.3.6	
7.3.7	7) Apakah laganan berisiko keamanan pada insulasi perancah sudah memelihara aspek Perlindungan Data Pribadi?	Dalam Perencanaan	1	7.3.7	
7.3.8	8) Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan pribadi risiko dan prosedur pengamanan yang berlaku?	Dalam Perencanaan	1	7.3.8	
7.3.9	9) Apakah insulasi perancah sudah menerapkan prosedur perlindungan pribadi dalam Perlindungan Data Pribadi, termasuk kebijakan terkait Perlindungan Data Pribadi?	Dalam Perencanaan	1	7.3.9	
7.3.10	10) Apakah insulasi perancah sudah menerapkan prosedur dari pribadi dalam pribadi asal menguji dalam pribadi, termasuk pengujian hak pribadi dalam, apa saja yang akan dilakukan pada dalam pribadi terkait dan menggunakan alir pengujian pribadi?	Dalam Perencanaan	1	7.3.10	
7.3.11	11) Apakah insulasi perancah sudah memiliki prosedur untuk melaporkan insiden terkait laganan aloof dalam pribadi?	alam Penerapan / Diterapkan Sekali	2	7.3.11	
7.3.12	12) Apakah insulasi perancah sudah menerapkan prosedur yang menjamin hak pribadi dalam pribadi untuk menguji dalam pribadi?	alam Penerapan / Diterapkan Sekali	2	7.3.12	
7.3.13	13) Apakah insulasi perancah sudah menerapkan prosedur yang terkait dengan memelihara dalam pribadi terkait aloof dan laganan berisiko?	alam Penerapan / Diterapkan Sekali	2	7.3.13	
7.3.14	14) Apakah insulasi perancah sudah menerapkan prosedur terkait periode pengujian dalam pribadi dan pengujian perancah yang sesuai dengan prosedur alir pengujian dengan pribadi dalam?	Dalam Perencanaan	1	7.3.14	
7.3.15	15) Apakah insulasi perancah sudah menerapkan prosedur terkait pengujian perancah dalam pribadi dan laganan berisiko yang akan dilakukan menggunakan teknik legal dan alir pengamanan pribadi dalam dan menggunakan alir pengamanan pribadi?	Dalam Perencanaan	1	7.3.15	
7.3.16	16) Apakah insulasi perancah sudah menerapkan prosedur terkait pengujian dalam pribadi dan pengamanan pribadi yang akan dilakukan?	Dalam Perencanaan	1	7.3.16	

Pengamanan keterlibatan pihak ketiga penyedia layanan

- Point 7.1.1.1 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.1.2 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.1.3 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.1.4 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.1.5 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.1.6 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.1.7 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.2.1 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.2.2 statusnya Diterapkan secara menyeluruh dengan skor 3
- Point 7.1.2.3 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.3.1 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.3.2 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.3.3 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.3.4 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.3.5 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.3.6 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.3.7 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.3.8 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.4.1 statusnya Diterapkan secara menyeluruh dengan skor 3
- Point 7.1.4.2 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.5.1 statusnya Diterapkan secara menyeluruh dengan skor 3
- Point 7.1.5.2 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.6.1 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.1.6.2 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.7.1 statusnya Dalam perencanaan dengan skor 1
- Point 7.1.7.2 statusnya Tidak dilakukan dengan skor 0
- Point 7.1.7.3 statusnya Dalam perencanaan dengan skor 1

Pengamanan layanan infrastruktur awan (cloud service)

- Point 7.2.1 statusnya Dalam perencanaan dengan skor 1
- Point 7.2.2 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.2.3 statusnya Dalam perencanaan dengan skor 1
- Point 7.2.4 statusnya Tidak dilakukan dengan skor 0
- Point 7.2.5 statusnya Dalam perencanaan dengan skor 1
- Point 7.2.6 statusnya Tidak dilakukan dengan skor 0
- Point 7.2.7 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.2.8 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.2.9 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2
- Point 7.2.10 statusnya Dalam penerapan / Diterapkan sebagian dengan skor 2

Perlindungan Data Pribadi

- Point 7.3.1 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.2 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.3 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.4 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.5 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.6 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.7 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.8 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.9 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.10 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.11 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.12 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.13 status nya Dalam penerapan / Diterapkan sebagian dengan skor 2
 - Point 7.3.14 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.15 status nya Dalam perencanaan dengan skor 1
 - Point 7.3.16 status nya Dalam perencanaan dengan skor 1
- Maka nilai evaluasi hasil dari **VI Suplemen** pengelolaan aset adalah **78**

BAB III

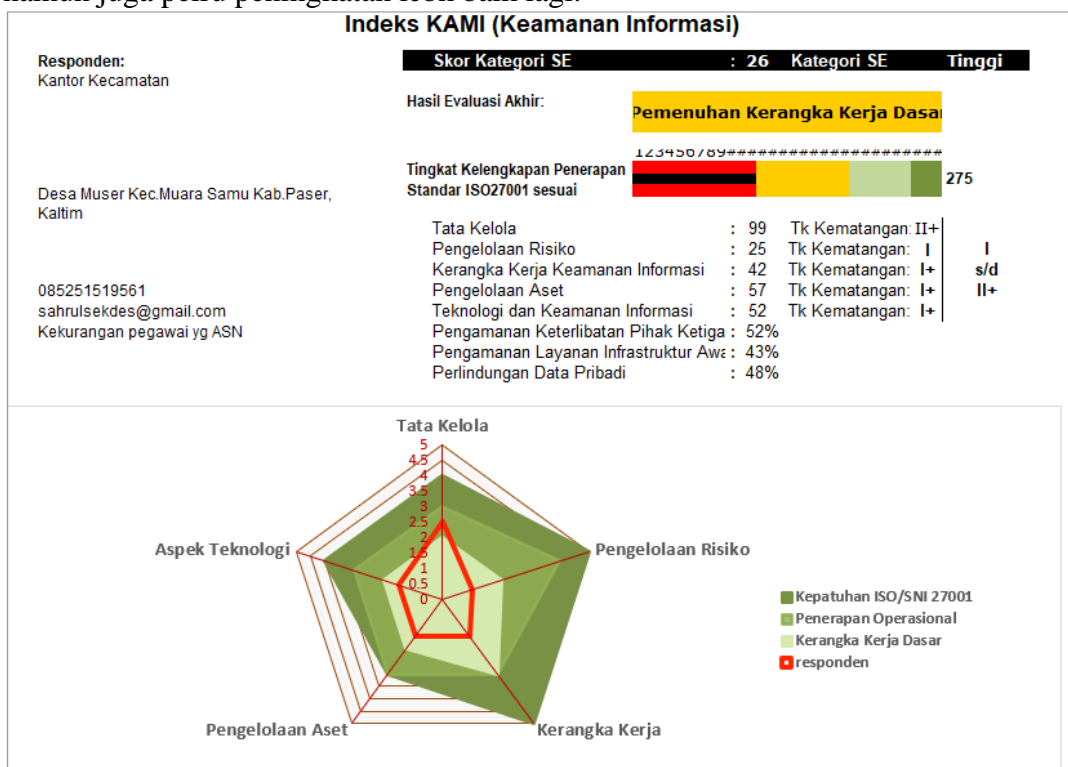
3.1 Meningkatkan kematangan

Dapat dilihat dari Hasil Indeks KAMI (Keamanan Informasi)

Skor Kategori SE : 26 Kategori SE - Tinggi

Disini dapat kita lihat bahwa hasil evaluasi yaitu Pemenuhan Kerangka Kerja Dasar, pada bagian tata kelola, pengelolaan risiko perlu peningkatan lebih lagi, untuk kerangka kerja keamanan informasi, pengelolaan aset, teknologi dan keamanan informasi sudah cukup baik namun tetap perlu peningkatan.

Untuk bagian berikut nya pengamanan ketertiban pihak ketiga, pengamanan layanan infrastruktur awan, dan perlindungan data pribadi sudah cukup baik juga namun juga perlu peningkatan lebih baik lagi.



Untuk detail dari hasil evaluasi bisa dilihat dari table dibawah ini atau gambar dibawah ini

	Tata Kelola	Manajemen Risiko	Kerangka Kerja	Manajemen Aspek	Aspek Teknologi	Total Skor		
Kategori Kontrol								
1	8	10	12	24	14	204	68	136
2	8	4	10	10	10	252	42	168
3	6	2	7	4	2	189	21	126
Total Pertanyaan	22	16	29	38	26	645	131	
Agregat Skor	1	1	1	1	1			
1	24	30	36	72	42			
2	72	54	96	132	102			
3	126	72	159	168	120			
Responden	99	25	42	57	52	275		
Tk Ketergatalungan TIK	Batas Bawah	Batas Atas	Klasifikasi	10	15	0	174	Tidak Layak
A	10	15	Rendah			175	312	Pemenuhan Kerangka Kerja Dasar
B	16	34	Tinggi			313	535	Cukup Baik
C	35	50	Strategis			536	645	Baik
				16	34	0	272	Tidak Layak
						273	455	Pemenuhan Kerangka Kerja Dasar
						456	583	Cukup Baik
						584	645	Baik
				35	50	0	333	Tidak Layak
						334	535	Pemenuhan Kerangka Kerja Dasar
						536	609	Cukup Baik
Ambang Batas Valid	16	20	24	24	14	610	645	Baik
			Valid					
	Hasil Evaluasi	Tinggi	an Kerangka Kerja Dasar					
	Merah	272						
	Kuning	455						
	Hijau Muda	583						

	Tata Kelola	Manajemen Risiko	Kerangka Kerja	Manajemen Aspek	Aspek Teknologi		
Tingkat II							
Status	II	No	I+	I+	I+		
Tingkat III							
Validitas	Yes	No	No	No	No		
Status	II+	No	No	No	No		
Tingkat IV							
Validitas	No	No	No	No	No		
Status	No	No	No	No	No		
Tingkat V							
Validitas	No	No	No	No	No		
Status	No	No	No	No	No		
Status Akhir	II+	I	I+	I+	I+		
	4	1	2	2	2	I	II+
						1	4
	Tata Kelola	Manajemen Risiko	Kerangka Kerja	Manajemen Aspek	Aspek Teknologi		
1	2	2	3	2	2		
2	3	4	3	3	3		
3	4	5	5	3	4		
responden	2.5	1	1.5	1.5	1.5		
						I	1
						I+	1.5
						II	2
						II+	2.5
						III	3
						III+	3.5
						IV	4
						IV+	4.5
						V	5

3.2 Kelayakan / Efektifitas

Bagian kelayakan untuk suatu instansi pemerintahan ini sangat Pemenuhan Kerangka Kerja Dasar karena banyak bagian yang perlu ditingkatkan dan segera diperbaiki.

Pada bagian efektivitas keamanan, karena dilebih banyak keterlibatan pihak ketiga mungkin lebih efektif namun perlu prosedural yang lebih baik lagi dan kejelasan hukum.