BAB 2
TINJAUAN PUSTAKA

Pada bab 2 ini menjelaskan tentang berbagai teori yang menjadi dasar dari pelaksanaan penelitian ini dan juga akan menjelaskan mengenai penelitian serupa yang telah dilakukan sebelumnya.

2.1 Keamanan Informasi

Suatu upaya yang dilakukan guna mengamankan aset informasi dari ancaman atau risiko yang akan datang adalah Keamanan informasi. Keamanan informasi dapat membantu kelancaran bisnis, mengurangi risiko, dan mengoptimalisasi pengembalian investasi. Banyaknya informasi yang disimpan oleh instansi, maka kemungkinan terjadinya kerusakan, kehilangan atau data yang terekspos akan semakin tinggi. (R. Sarno dan I. Iffano, 2019)

Terdapat 3 karakteristik penting dalam keamanan informasi yang disebut dengan singkatan CIA yang dapat dijelaskan seperti berikut :

- *Confidentiality* : pada karakteristik ini menjadi alasan bagi seluruh kebijakan dari instansi tentang keamanan informasi. Karakteristik ini adalah aturan yang ditetapkan dan menentukan bagi pengguna untuk melakukan akses pada data yang dinilai sensitif pada sistem informasi instansi terkait.
- *Integrity* : pada karakteristik ini menjadi alasan bagi kepercayaan terhadap sebuah informasi yang tersedia. Keutuhan sebuah informasi dapat dilakukan bila informasi tidak menerima perubahan secara disengaja maupun tidak sengaja.
- *Availability* : pada karakteristik ini menjadi alasan bagi ketersediaan dari suatu informasi sewaktu dibutuhkan. Hal tersebut dapat dibengaruhi oleh teknik, alam dan manusia. Pada umumnya manusia adalah faktor yang yang sering menjadi permasalahan awam.

Kesimpulan yang didapatkan pada penjelasan diatas, yaitu karakteristik CIA merupakan karakteristik penting yang saling membutuhkan dan digunakan guna

menjaga keamanan informasi.pada instansi terkait. Keterkaitan karakteristik CIA dengan keamanan informasi dapat digambarkan sebagai berikut :

Gambar 2.1 Diagram CIA

Pada Gambar 2.1 dapat dilihat aspek dari tata kelola instansi, kinerja TI akan terganggu apabila permasalahan keamanan informasinya terdapat pada diagram CIA organisasi. Dikarenakan Diagram CIA merupakan salah satu dari bentuk dari keamanan informasi yang dapat mengurangi atau menghindari risiko keamanan informasi. (Basyarahil, 2017)

2.2 Sistem Mananjemen Keamanan Informasi (SMKI)

Instansi sebaiknya mengaplikasikan sistem manajemen keamanan informasi guna mengamankan aset dari sistem informasi yang digunakan pada instansi. Sistem manajemen keamanan informasi merupakan sekumpulan kebijakan serta prosedur guna mengatur data yang dirasa penting dan privasi oleh instansi dengan tujuan sebisa mungkin meminimalisir risiko serta menjamin keberlangsungan bisnis dari pelanggaran keamanan yang mungkin terjadi. Hal itulah juga melatarbelakangi pembentukan seri ISO/IEC 27000 yang menjadi standar dari Sistem Manajemen Keamanan Informasi (SMKI).

Dalam pengaplikasiannya keamanan informasi dipastikan tidak hanya terbatas dalam penggunaan perangkat keamanan lunak pembantu namun diharapkam lebih mengarah kepada keamanan sistem secara keseluruhan. Dikarenakan SMKI dalam ISO/IEC 27001 merupakan sebuah pendekatan yang dilakukan secara sistematis guna berjalannya implementasi, penetapan, operasional, pemantauan, pemeliharan dan peningkatan keamanan informasi pada instansi dengan berlandaskan tujuan bisnis.

International Organization for Standardization atau disingkat (ISO) merupakan sebuah organisasi internasional non-pemerintahan dikhususkan untuk standarisasi keamanan informasi. *International Electrotechnical Commision* atau disingkat (IEC) merupakan suatu organisasi standarisasi internasional dengan tujuan menyiapkan dan mempublikasikan standar internasional untuk seluruh teknologi yang terkait. Standarisasi digunakan untuk melandasi inovasi dan memberikan solusi untuk tantangan global yang akan dihadapi bagi organisasi. (Chazar, 2015)

2.3 ISO/IEC 27001

ISO 27001 adalah salahsatu standar yang publikasi oleh *International Organization for Standardization*. standar yang digunakan untuk mempermudah instansi dalam upaya melindungi keamanan informasi pada instansi dan guna melindungi sistem manajemen keamanan informasi (SMKI). ISO 27001 dirancang secara khusus agar dapat disesuaikan dengan kondisi segala skala organisasi dan dapat diaplikasikan pada organisasi kecil, menengah hingga besar tanpa melihat sektor yang dijalani oleh organisasi dengan tujuan untuk keamanan informasi instansi terkait.

ISO 27001 merupakan salah satu contoh standar yang dikembangkan menggunakan pendekatan yang mencakup model yang tepat bagi penetapan, penerapan, pengoprasian, pemantauan, review, pemeliharaan dan peningkatan SMKI. Model yang diterapkan dalam keseluruhan struktur SMKI adalah model *Plan, Do, Check, Act* (PDCA). Berikut penjabaran dari Model PDCA :

- *Plan* : pada tahap ini dilakukan penetapan SMKI yang beriki kebijakan seperti, sasaran, proses dan prosedur yang sesuai dalam mengelola risiko dan meningkatkan keamanan informasi pada instansi terkait.
- *Do* : pada tahap ini dilakukan penerapan dan pengoperasian dari kebijakan SMKI, kontrol, proses dan prosedur yang telah disepakati oleh organisasi.
- *Check* : pada tahap ini dilakukan pemantauan dari kinerja serta prosedur dan kebijakan yang sedang dijalankan oleh organisasi.
- *Act* : pada tahap ini dilakukan perbaikan dan pencegahan dengan berdasarkan hasil dari evaluasi, audit internal dan tinjauan manajemen tentang SMKI pada Instansi terkait.

Dengan adanya penerapan ISO/IEC 27001 maka organisasi memiliki acuan penilaian keamanan informasi yang dimana hasil penelitian tersebut dapat dijadikan data untuk meyakintakan pihak trakeholder terhadap pentingnya keamanan informasi pada organisasi. (Chazar, 2015)

2.4 Indeks Keamanan Informasi (KAMI) Versi 4.0

Indeks KAMI merupakan sebuah metode atau *tools* evaluasi untuk atau menganalisa tingkat dari kesiapan sebuah keamanan informasi pada suatu instansi. Indeks KAMI tidak digunakan untuk melakukan analisa kelayakan maupun efektifitas sebuah keamanan informasi sesuai dengan standar ISO/IEC 27001:2013 memberikan gambaran kerangka keja dan keamanan informasi dengan menampilkan kesiapan keamanan informasinya dengan tampilan diagram dan dapat diserahkan kepada pemimpin instansi atau penanggungjwab sub-bagian bersangkutan. Dapat digunakan sebagai sarana pengganti bagi penyampaian data kesiapan keamanan sebuah sistem kepada *client* atau *stakeholders* dan Indeks KAMI dapat digunakan secara berkala guna menghasilkan gambaran dokumentasi jelas dari perkembangan kondisi keamanan sistem informasi pada instansi terkait. (BSSN, 2018)

2.4.1 Area Penilaian Indeks KAMI Versi 4.0

Penilaian dari Indeks KAMI dilakukan setelah dilakukannya wawancara dengan penanggungjawab atau anggota sub-bagian terkait pada organisasi

diseluruh cakupan Indeks KAMI. Terdapat 5 area yang akan nilai dalam penggunaan Indeks KAMI, yaitu :

- **Area tata kelola**

  Pada area ini dilakukan penilaian dari bentuk tata kelola pada keamanan informasi yang diterapkan pada instansi dan juga tugas-tugas serta tanggungjawab dari pengelola sistem terkait.

- **Area pengelolaan risiko**

  Pada area ini dilakukan penilaian dari penerapan kesiapan terjadinya risiko keamanan informasi sebagaimana instansi melakukan pengelolaan risiko yang akan dihadapi.

- **Area kerangka kerja**

  Pada area ini dilakukan penilaian kesiapan serta kelengkapan dari struktur kerangka kerja dalam pengelolaan keamanan informasi pada instansi.

- **Area pengelolaan aset informasi**

  Pada bagian ini dilakukan evaluasi kelengkapan dari pengamanan yang diterapkan pada aset informasi pada instansi serta siklus dari penggunaan aset.

- **Area teknologi dan keamanan informasi**

  Pada area ini dilakukan penilaian pengamanan informasi yang dapat dilihat dari beberapa nilai seperti, kelengkapan, konsisten, dan efektivitas penggunaan teknologi yang terdapat pada instansi terkait

2.4.2 Skor Penilaian Indeks KAMI Versi 4.0

Dalam proses klasifikasi dilakukan wawancara dengan tujuan mengetahui penilaian Sistem Elektronik yang akan digunakan dalam penilaian kuantitatif. Tahap ini dilakukan guna untuk mengelompokkan sistem informasi yang ada pada organisasi kedalam ukuran tertentu yang akan ditampilkan pada gambar berikut :

Rendah	
10	15
Tinggi	
16	34
Strategis	
35	50

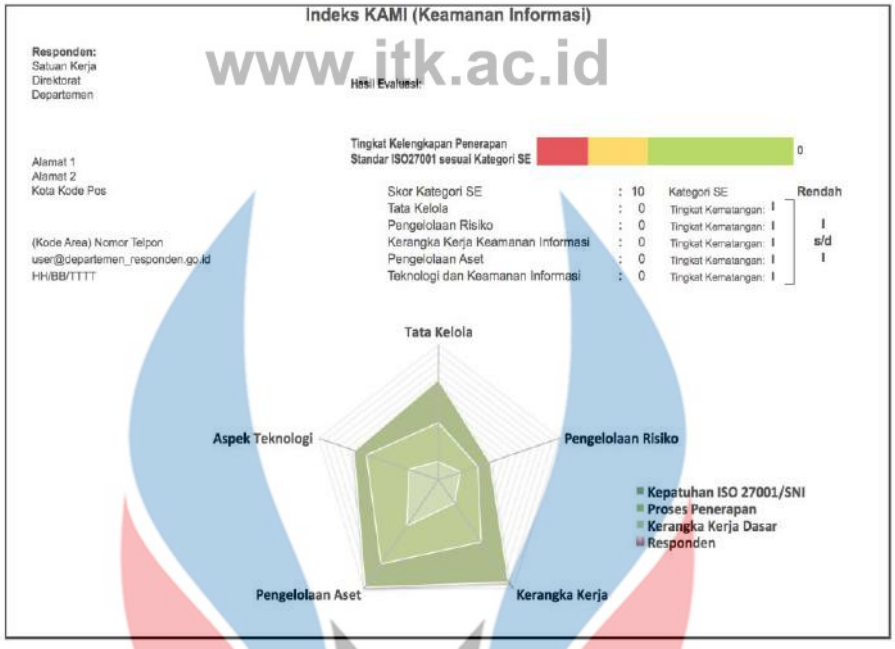
Gambar 2.2 Nilai Kategori SE

Dapat dilihat pada Gambar 2.2 diatas pengelompokan dari hasil nilai yang didapatkan akan dijumlahkan namun sebelum itu kategori dibagi menjadi 3 kriteria terdahulu, yaitu Rendah, Tinggi, dan Strategis. Terkait kategori SE yang akan diberikan kepada responden dengan metode wawancara. Untuk mengetahui besaran peran Sistem Elektronik pada instansi maka dapat diberikan sejumlah pertanyaan yang dapat menjawab besaran tersebut. Setiap pertanyaan memiliki tiga kriteria dari penilaian. Kriteria penilaian akan digunakan pada setiap pertanyaan yang akan diberikan pada responden dapat lihat pada Tabel 2.1 sebagai berikut :

Tabel 2.1 Kriteria Pertanyaan

Kriteria	Nilai
A	5
B	2
C	1

Setelah dilakukan klasifikasi peran dari SE penilaian dari lima area Indeks KAMI dapat dilakukan. Hasil dari penilaian yang didapatkan akan digambarkan melalui *spider chart* . Pada diagram tersebut digambarkan nilai kepatuhan instansi pada standar ISO/IEC 27001 dengan penilaian dari Indeks KAMI dapat digambarkan sebagai berikut :



Gambar 2.3 Penilaian Indeks KAMI

Dapat dilihat pada Gambar 2.3 diatas setelah dijadikan 3 bagian kategori pengamanan maka, selanjutnya adalah pengelompokan pertanyaan terkait kerangka kerja dikategorikan sebagai nomor 1 untuk efektivitas dan konsistensi penerapannya akan dikategorikan sebagai nomor 2 dan pada kemampuan untuk selalu mengembangkan kinerja keamanan informasinya akan dikategorikan sebagai nomor 3 (Basyarahil, 2017)

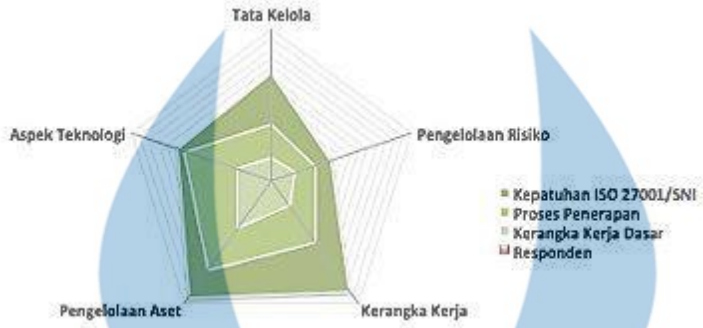
Indeks KAMI hanya memiliki 4 jawaban dan setiap dari pertanyaan yang ada menanyakan tentang status dari keamanan informasi pada organisasi terkait, dan setiap pertanyaan akan diberi skor yang nilainya sudah disesuaikan oleh Indeks KAMI, berikut matrik dari skor pengamanan :

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 2.4 Matriks Skor Pengamanan

Dapat dilihat Gambar 2.4 diatas menjelaskan bahwa nilai yang didapatkan akan disesuaikan dengan kategori pengamanan dan status dari pengamanan yang ada pada instansi. Hasil dari penjumlahan skor area akan disajikan dalam bentuk

tabel nilai pada area yang dinilai serta dalam bentuk *Radar Chart* lima sumbu berdasarkan area yang telah dilakukan penilaian seperti ditunjukkan pada gambar berikut :



Gambar 2.5 Diagram Radar Chart

Dapat dilihat pada Gambar 2.5 diatas *Radar chart* menunjukkan diagram tersebut memiliki 3 sisi pada masing masing area yang dinilai Indeks KAMI dan gradasi warna yang digambarkan oleh diagram menunjukkan batasan dari setiap kategori pengamanan 1 hingga 3 yang telah dinilai dan area merah dikhususkan sebagai pembanding kondisi dengan acuan yang dipilih. (BSSN, 2018)

Semakin pentingnya sistem informasi pada organisasi semakin banyaknya bentuk pengamanan yang diperlukan dan diterapkan hingga tahap tertinggi. Skor akhir yang dapat dicapai dalam Indeks KAMI dapat dilihat pada gambar berikut :

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Gambar 2.6 Petunjuk Kategori SE dan Status Kesiapan

2.5 Penelitian Terdahulu

Penelitian serupa telah dilakukan sebelumnya, Penelitian itu diantaranya dapat dilihat pada Tabel 2.2 sebagai berikut :

Tabel 2.2 Penelitian Terdahulu

No	Nama dan tahun Publikasi	Hasil
1	Firzah Abdullah, 2017	Metode : Indeks KAMI Versi 3.1, ISO/IEC 27001:2013 Hasil : klasifikasi yang didapat mencapai dengan tingkat ketergantungan pada penggunaan kerangka kerja elektronik dari 26 dari 50 skor dan dapat terus berkembang
2	Pramudhita Ferdiansyah, subekthiningsih, & Rini Indrayani, 2019	Metode : Indeks KAMI Versi 4.0, ISO/IEC 27001:2013 Hasil : Dari penilaian tersebut diketahui bahwa konsekuensi keamanan data yang rendah dengan skor elektronik 20 dari kulminasi data yang lolos jauh, tepatnya 245. Dari sini cenderung disimpulkan bahwa ada kebutuhan yang luar biasa untuk pengembangan dan peningkatan partisipasi dengan perancang keamanan sumber daya data dan pihak luar yang terlibat dengan organisasi.
3	Nabilla Diva, Widhy, & Nugraha Putra, 2020	Metode : Indeks KAMI Versi 4.0, ISO/IEC 27001:2013. Hasil : Penilaian yang telah diselesaikan diperoleh 17 poin untuk wilayah administrasi keamanan data, 16 poin untuk wilayah hazard eksekutif, 27 gagasan untuk wilayah sistem, 31 poin untuk wilayah dewan sumber daya, 6 poin untuk wilayah inovasi dan keamanan data, dan 9 poin untuk daerah suplemen. Selanjutnya

No	Nama dan tahun Publikasi	Hasil
		ditampilkan dengan mendapatkan skor lengkap 193 poin.
4	Mustaqim Siga, 2014	Metode : Indeks KAMI Versi 2.3, ISO/IEC 27001:2005 Hasil : Hasil dari pengujian ini adalah penilaian yang ditujukan untuk mengetahui nilai keamanan TI para eksekutif, tingkat pengembangan, dan pemberian proposal tergantung pada konsekuensi dari keamanan data yang diperoleh dewan penyelidikan.
5	Tri Yani Akhirina, Sutan Muhammad Arif, dan Rahmatika, 2016	Metode : Indeks KAMI, ISO 27001:2009 Hasil : Evaluasi ini digunakan untuk memberikan gambaran tentang tingkat perkembangan keamanan data di PT. Indotama Accomplice Coordination, dengan harapan hasil penilaian dapat dimanfaatkan untuk lebih mengembangkan keamanan data oleh organisasi.
6	Darmawan Setiya Budi, dan Avinanta Taringan, 2018	Metode : Indeks KAMI 3.1, ISO 27001:2013, HAIS-Q Hasil : Evaluasi ini merupakan studi penulisan yang diharapkan dapat membentuk sistem dari penilaian keamanan data para eksekutif dan karyawan yang memperhatikan keamanan data yang dimiliki dan oleh klien.
7	I Gede Putu Krisna Juliharta, Komang Tri werthi, dan Ni Luh Putu Ning S.P Astawa	Metode : KAMI 4.0, ISO 27001 : 2013 Hasil : Pemanfaatan Indeks KAMI 4.0 merupakan alasan bahwa pelaksanaan keamanan data framework board di framework kota Denpasar berada pada level I-I+ yang bersifat reseptif, dan perlu pergantian peristiwa lebih lanjut (tidak

No	Nama dan tahun Publikasi	Hasil
		layak) untuk mendapatkan sertifikasi ISO 27001:2013.
8	Muhammad Imron Rosadi dan Lukman Hakim	Metode : Indeks KAMI 3.1, ISO 27001 : 2009 Hasil : Diketahui bahwa tingkat pengembangan keamanan inovasi berada di level I hingga II, skor lengkap untuk bagian TIK adalah 28 (Tinggi), dan risiko dampak dari inseden yang terjadi mencapai 200, ini menyiratkan bahwa pengembangan TIK tingkat tidak bisa dilakukan.
9	Muh. Faturachman Husin, Hans F. Wowor, dan Stanlet Kavouw	Metode : Indeks KAMI 3.1, ISO 27001 : 2013 Hasil : Diketahui bahwa tingkat pengembangan keamanan data di Perguruan Tinggi Sam Ratulangi secara umum masih rendah dan perlu ditingkatkan meskipun pekerjaan/tingkat ketergantungan pada Inovasi Data dan Korespondensi cukup tinggi. Gagasan untuk pengembangan juga mengakomodasi kekurangan yang ditemukan dalam kerangka kerja keamanan data.
10	Asep Ririh Riswaya, Ashwin Sasongko, dan Asep Maulana	Metode : Indeks KAMI 4.0, ISO 27001 : 2013 Hasil : Diketahui bahwa penilaian menghasilkan area elektronik memiliki skor 21, yang berarti bahwa area elektronik dalam organisasi ini tinggi menurut file AS 10 hingga 15 rendah, 16 hingga 34 tinggi dan 35 hingga 50 kunci. Namun, status ketersediaannya bernilai 117, yang berarti masih belum masuk akal untuk ditegaskan pada SNI ISO/IEC 27001 untuk jaminan inklusi yang memenuhi syarat, nilainya mencapai 273 hingga 445.

Pada penelitian pertama, membicarakan masalah-masalah di DPTSI Surabaya dengan upaya dapat dilakukan untuk bekerja pada sifat keamanan data, Dinas Korespondensi dan Informatika membuat metode penilaian yang dapat membantu mempermudah penilaian keamanan pada informasi yang digunakan oleh instansi yaitu Indeks KAMI. Penggunaan metode tersebut dapat sekaligus membantu asosiasi dalam menerapkan ISO/IEC 27001 dan menjamin keamanan data yang dilakukan.

Pada penelitian ke-2, membahas tentang permasalahan di UPTD XYZ Bina Binaan yang langsung berada di bawah pengawasan Dinas Persekolahan Daerah Unik Yogyakarta karena banyaknya informasi data yang terdapat di UPTD XYZ dalam mengurus administrasi publik, penting untuk menilai keamanan data untuk mengukur tingkat ketersediaan, pengembangan dan puncak dari keamanan data. pada UPTD XYZ. Data yang terkandung dalam UPTD XYZ dapat berupa dokumen halus, situs, pesan, dan struktur lain yang bersifat mendidik. Hasil dari penilaian yang telah diselesaikan adalah sebagai informasi yang dapat memberikan ide untuk lebih mengembangkan keamanan kerangka data kepada kepala UPTD XYZ

Pada penelitian ke-3, membahas tentang permasalahan di Dinas Persuratan dan Data (DISKOMINFO) Malang dengan alasan Dinas Korespondensi dan Data memberikan Pedoman Pastoral Nomor 4 Tahun 2016 tentang Keamanan Data Kerangka Pelaksana untuk membantu keamanan data di kantor-kantor pemerintahan. Diidentifikasi dengan pedoman ini, sebagai kantor yang ditempati dengan area data, penting untuk menilai tingkat keamanan data. Dalam pemeriksaan ini, penilaian dilakukan dengan memanfaatkan Data Security Record (KAMI) 4.0 yang menunjukkan derajat status dan perkembangan keamanan data di kantor pemerintahan.

Pada penelitian ke-4, berbicara tentang masalah di kantor provinsi Ditjen Kustodian Jawa Timur, tempat penilaian dilakukan. Berdasarkan KMK No. 479/KMK.01/2010, pengaturan dan prinsip keamanan data kerangka kerja pelaksana di dalam Layanan Uang mengacu pada ISO/IEC 27001:2005. ISO/IEC 27001:2005 adalah arsip standar global tentang keamanan data kerangka kerja dewan atau Keamanan Data Kerangka kerja eksekutif (ISMS) yang memberikan

gambaran keseluruhan tentang apa yang harus dilakukan dengan tujuan akhir untuk menilai, melaksanakan, dan mengikuti data keamanan dalam organisasi bergantung pada "praktik terbaik". dalam mendapatkan data File. Penilaian dilakukan di berbagai wilayah yang menjadi tujuan pelaksanaan keamanan data dengan tingkat percakapan yang juga memenuhi semua sudut pandang keamanan yang dicirikan oleh norma ISO/IEC 27001:2005.

Pada penelitian ke-5, berbicara tentang masalah di PT. Koordinasi Kaki Tangan Indotama yaitu untuk lebih mengembangkan administrasi kepada pembeli, salah satu dukungannya adalah aksesibilitas data yang cepat dan tepat. Maka penting untuk menilai keamanan kerangka data di PT Indotama Mitra Koordinasi. Catatan KAMI adalah aplikasi yang digunakan untuk mengukur perkembangan dan puncak keamanan data yang telah disesuaikan dengan standar ISO/IEC 27001:2009 yang dibuat oleh Layanan Korespondensi dan Data. Tahap utama dalam penilaian daftar KAMI adalah untuk mengevaluasi tingkat ketergantungan TIK di kantor, dan efek samping dari tingkat ketergantungan akan digunakan sebagai insentif cutoff untuk penilaian lima wilayah dalam catatan KAMI. Evaluasi ini digunakan untuk melihat sejauh mana tingkat perkembangan keamanan data di PT Indotama Kaki Koordinasi.

Pada penelitian ke-6, berbicara tentang isu-isu dalam gagasan studi penulisan yang disurvei tentang keamanan data dan Menurut Eloff dan Von Solms, seluruh asosiasi bergantung pada aset inovasi datanya. Pereira dan Santos berpendapat bahwa aset inovasi data adalah untuk ketahanan asosiasi, tetapi juga untuk pengembangan dan perluasan asosiasi di pasar dunia yang sangat serius. Dengan cara ini, keamanan data harus diawasi dan dikendalikan dengan tepat untuk melindungi data dari berbagai bahaya. Hal ini dilakukan untuk menjamin koherensi bisnis, membatasi bahaya bisnis, serta meningkatkan keuntungan dari spekulasi dan pembukaan bisnis.

Pada penelitian ke-7, berbicara tentang isu-isu di salah satu e-government atau Organisasi Pemerintah Kota Denpasar di bawah Kantor Korespondensi dan Data Denpasar dengan dukungan untuk mencanangkan program kota cerdas dalam pembangunan menuju 100 daerah perkotaan cemerlang Indonesia yang dimulai oleh Dinas Perhubungan dan Data Republik Indonesia. Sehingga dalam

pelaksanaan e-government di Denpasar, Dinas Persuratan dan Data Republik Indonesia juga menghimbau kepada seluruh Instansi Pemerintah untuk melaksanakan Kerangka Pengamanan Data melalui Pedoman Pastoral No. 4 Tahun 2016.

Pada penelitian ke-8, mengkaji permasalahan di Perguruan Tinggi Yudharta Pasuruan, disadari bahwa inovasi data yang diterapkan di sebuah asosiasi/yayasan akan mempengaruhi sejauh mana asosiasi/instansi tersebut telah mencapai visi dan misi atau tujuan utamanya. Oleh karena itu, UYP memanfaatkan SIAKAD untuk menangani informasi skolastik mahasiswa, narasumber dan informasi staf. hanya sebagai uang. Kemudian, pada saat itu untuk menjamin apa pun kecuali, penilaian keamanan data dilengkapi dengan eksplorasi ini untuk secara tepat melindungi informasi dan data kampus dari bahaya dari celah keamanan lain. Hasil dari estimasi dan penilaian yang menggunakan daftar KAMI ini diyakini dapat dimanfaatkan oleh UYP sebagai model penilaian dan perbaikan sejauh kerangka data dan keamanan organisasi.

Pada penelitian ke-9, membicarakan permasalahan di Perguruan Tinggi Sam Ratulangi karena Perguruan Tinggi Sam Ratulangi (UNSRAT) dikenal sebagai lembaga edukatif yang belum melakukan normalisasi kerangka data. Sebelum dilakukan normalisasi, penting dilakukan penilaian keamanan data *framework* di unit kerja untuk mendapatkan gambaran keadaan penyiapan dan pengembangan keamanan data pemanfaatan Data Security File.

Pada penelitian ke-10, membicarakan permasalahan di STMIK Mardira Indonesia karena disadari bahwa salah satu upaya yang dapat dilakukan oleh asosiasi untuk mengatasi gangguan keamanan data adalah dengan menjalankan Kerangka Kerja Pelaksana Keamanan Data (SMKI).