BAB 2
TINJAUAN PUSTAKA

Pada bab ini akan dijelaskan mengenai tinjauan pustaka atau dasar teori dari penelitian pada tugas akhir. Pada bab ini akan berisi mengenai Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Penajam Paser Utara, Aset Informasi, Keamanan Informasi, Manajemen Risiko, Perbandingan Metode, OCTAVE-S , FMEA, ISO/IEC 27001:2013, dan Penelitian Terdahulu.

2.1 Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Penajam Paser Utara

Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Penajam Paser Utara dibentuk berdasarkan Peraturan Bupati Penajam Paser Utara nomor 43 Tahun 2017 Tanggal 30 Oktober 2017 tentang Susunan Organisasi, Tata Kerja, Tugas Pokok dan Fungsi Dinas Komunikasi dan Informatika Penajam Paser Utara (Perbud, 2017).

Adapun visi dan misi dari Diskominfo Penajam Paser Utara yaitu (Dinas Komunikasi dan Informatika) :

A. Visi

Mewujudkan Pelayanan Prima dengan Berbasis Pada Teknologi Informasi.

B. Misi

1. Meningkatkan Pelayanan Berbasis E-Gov
2. Meningkatkan Sistem Informasi Daerah
3. Meningkatkan Sistem Keamanan Informasi Daerah
4. Meningkatkan Kualitas Pelayanan Data dan Statistik
5. Mewujudkan Media Layanan Publik di Kecamatan

2.1.1 Tugas Pokok dan Fungsi Dinas Komunikasi dan Informatika

Dinas Komunikasi dan Informatika memiliki tugas yaitu melaksanakan kegiatan di pemerintahan bidang komunikasi dan informatika. Tugas pokok dan DISKOMINFO dibagi menjadi tugas pokok dan fungsi kepala dinas, dan masing-

masing bidang yang ada di Dinas Komunikasi dan Informatika Penajam Paser Utara (Perbud, 2017).

1. Tugas Pokok dan Fungsi Kepala Dinas

Dinas Komunikasi dan informatika dipimpin oleh seorang Kepala Dinas yang mempunyai tugas pokok yaitu untuk dapat memimpin, mengatur, mengkoordinasikan dan bertanggung jawab dalam melaksaakan tugas di pemerintahan daerah. Kepala Dinas dalam melaksanakan tugasnya untuk menyelenggarakan fungsi :

- Perumusan dan penetapan Rencana Strategis Organisasi berdasarkan RPJMD pemerintah Daerah, tugas, permasalahan dan kebijakan
- Perumusahan upaya dalam meningkatkan dan mengembangkan kebijaksanaan pada DISKOMINFO
- Perumusan pedoman kerja sebagai arah dalam melaksanakan tugas
- Pendistribusian tugas kepada sekretariat dan kepala di masing-masing bidang

2. Tugas Pokok dan Fungsi Bidang Aplikasi Informasi dan Persandian

Bidang aplikasi informasi dan persandian memiliki tugas pokok yaitu mengadakan pengkajian terkait material kebijakan teknis dan fasilitias aplikasi informasi dan persandian. Adapun fungsi dalam melaksanakan tugas Bidang Aplikasi Informatika dan Persandian dibawah ini :

- Menjadi pengarah dalam menyusun rencana kegiatan di bidang aplikasi informasi dan persandian
- Penyusunan rencana program perumusan renstra organisasi pada DISKOMINFO
- Perumusan peningkatan dan pengembangan program bidang aplikasi informasi dan persandian
- Pendistribusian tugas ke kepala seksi pada bidang aplikasi informasi dan persandian

3. Tugas Pokok dan Fungsi Bidang Informasi, Komunikasi Publik dan Kehumasan

Bidang informasi, komunikasi pubik dan kehumasan memiliki tugas melaksanakan penyusunan kebijakan teknis dan fasilitasi informasi, komunikasi dan kehumasan. Dalam menjalankan tugasnya bidang ini pengadakan fungsi:

- Sebagai arahan dalam penyusunan rencana kegiatan yang berdasarkan penugasan, permasalahan, dan kebijakan
- Penyusunan rencana berdasarkan usulan sebagai bahan perumusan Renstra Organisasi Perangkat Daerah
- Pendistribusian tugas ke masing-masing kepala seksi berdasarkan peraturan Bupati
- Sebagai pengendali dalam pelaksanaan tugas admistratif dan teknis operasional

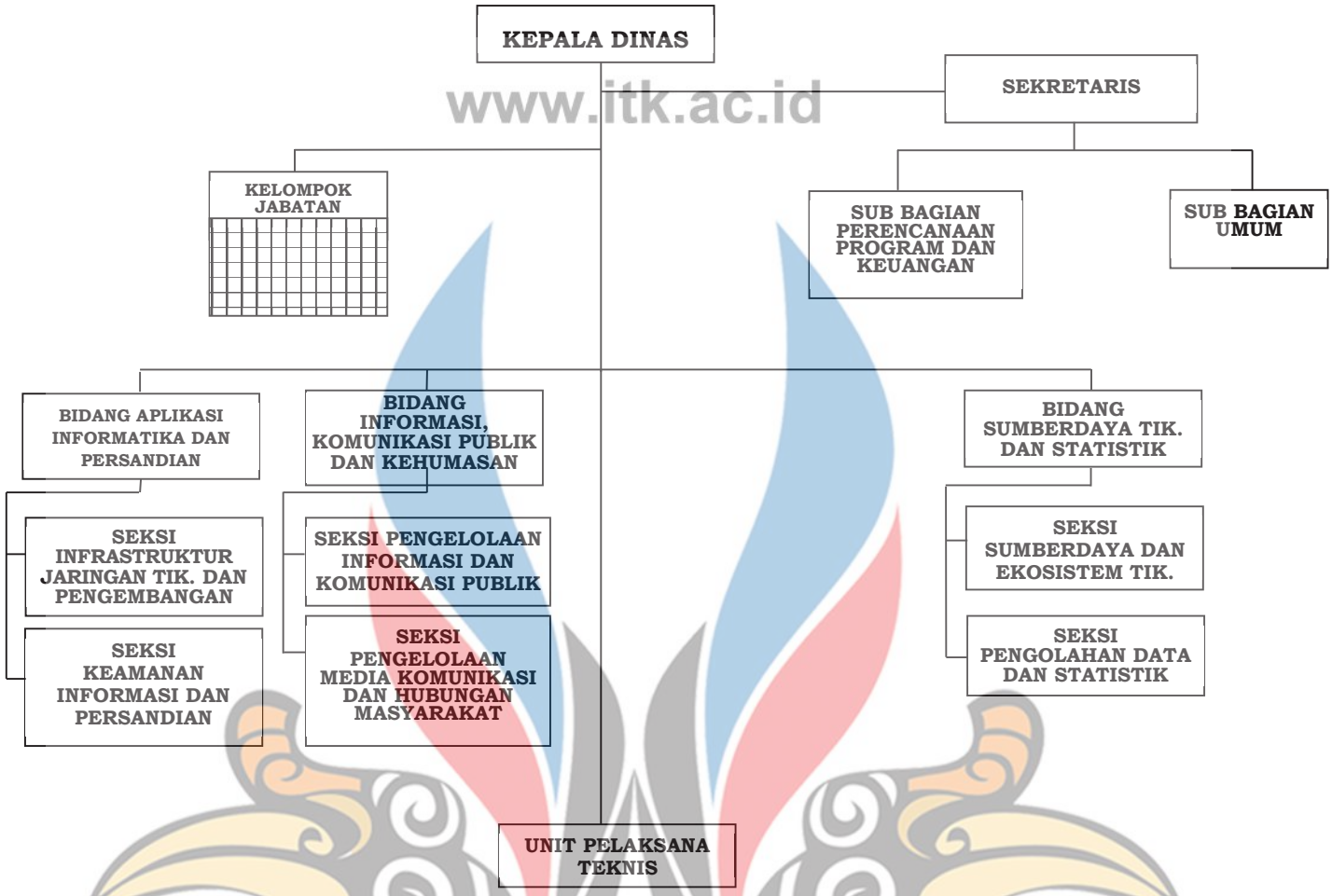
4. Tugas Pokok dan Fungsi Bidang Sumberdaya TIK dan Statistik

Bidang Sumberdaya TIK dan Statistik memiliki tugas pokok sebagai pengendali dalam perencanaan program pembangunan pengembangan sumber daya dan ekosistim TIK serta monitoring,evaluasi dan statistik. Bidang ini menyelenggarakan fungsi :

- Memberi arahan dalam Menyusun rencana kegiatan yang didasarkan oleh tugas, permasalahan dan kebijakan
- Penyusunan rencana program untuk perumusan Renstra Organisasi Perangkat Daerah Dinas Komunikasi dan Informatika
- Melakuakan perumusan sebagai upaya dalam peningkatan dan pengembangan program bidang sumberdaya TIK dan statistic

2.1.2 **Struktur Organisasi Dinas Komunikasi dan Informatika**

Adapun struktur organisasi Dinas Komunikasi dan Informatika Penajam Paser Utara yaitu pada **Gambar 2.1** (Perbud, 2017).



Gambar 2.1 Struktur Organisasi (Perbud, 2017)

Dari **Gambar 2.1** merupakan struktur organisasi Dinas Komunikasi dan Informatika Penjam Paser Utara, susunan Organisasi Dinas Komunikasi dan Informatika dikeplai oleh Kepala Dinas dan membawahi secretariat. Sekretariat yang membawahi Sub Bagian Perencanaan Program dan Keuangan dan Sub Bagian Umum. Kemudian Kelompok Jabatan fungsional. Setelah itu bidang yang ada pada DISKOMINFO yaitu Bidang Aplikasi Informatika dan Persandian yang membawahi Seksi Infrastruktur Jaringan TIK dan Pengembangan E-Government dan Seksi Keamanan Informasi dan Persandian. Setelah itu Bidang Informasi, Komunikasi Publik dan Kehumasan yang membawahi Seksi Pengelolaan Informasi dan Komunikasi Publik dan Seksi Pengelolaan Media Komunikasi dan Hubungan Masyarakat. Bidang Sumberdaya dan Statistik yang membawahi Seksi Sumberdaya dan Ekosistem TIK dan Seksi Pengolahan Data dan Statistik. Setelah itu Unit Pelaksana Teknis (UPT).

2.2 Aset Informasi

Aset ialah suatu sumber daya yang berperan penting dan dimiliki oleh sebuah perusahaan atau organisasi. Aset memberikan dukungan pada organisasi dalam mencapai tujuannya (Dewi, dkk., 2016). Aset informasi merupakan kumpulan dari informasi-informasi yang didefinisikan dan dikelola menjadi satu sehingga dapat dengan mudah untuk dipahami, dibagikan, dilindungi dan dimanfaatkan secara efektif. aset informasi memiliki nilai, risiko, konten dan siklus hidup yang dapat dengan mudah diatur dan dikenali (Digital Continuity Project, 2011).

Pada penelitian ini aset informasi mengarah pada penjelasan mengenai elemen suatu sistem informasi. Elemen sistem informasi disusun dari elemen-elemen pendukung yaitu perangkat keras (*hardware*), perangkat lunak (*software*), manusia (*people*), data, dan jaringan (*network*). Elemen tersebut memiliki keterikatan satu dengan yang lain untuk mencapai suatu tujuan yang telah ditetapkan. Setiap komponen akan dijelaskan sebagai berikut (Rachmawan, 2017).

1. Perangkat Keras (*Hardware)*

   Perangkat keras *(hardware*) ialah sebuah alat yang memiliki peranan penting sebagai tempat sistem operasi digunakan untuk mengolah atau memproses suatu informasi. *Hardware* bekerja berdasarkan dari perintah yang telah ditentukan. *Hardware* misalnya komputer, server, printer, dan monitor.

2. Perangkat Lunak (*Software)*

   Perangkat lunak (*software*) ialah beberapa perintah yang telah ditentukan dan dijalankan oleh mesin komputer dalam melaksanakan tugasnya. Tujuan dari software adalah untuk pengolahan data agar menghasilkan informasi yang dapat digunakan.

3. Manusia (*People)*

   Manusia (*people*) merupakan suatu faktor penting yang tidak dapat dilepaskan dari bagian suatu organisasi. Manusia memiliki peran dalam menentukan perkembangan suatu organisasi karena manusia juga merupakan aset yang dimiliki oleh organisasi. Adapun yang harus diperhatikan dalam aset manusia yaitu keahlian teknis, pengetahuan bisnis, dan orientasi dalam memecahkan permasalahanan.

4. Data

Data merupakan kumpulan dari kejadian nyata atau fakta yang memberi sebuah gambaran yang luas tentang suatu keadaan. Dalam teknologi informasi data berada pada *database.* Pada *database* inilah data disimpan dengan tujuan sebagai informasi yang dapat digunakan dalam mendukung organisasi untuk kegiatan operasional.

5. Jaringan *(network)*

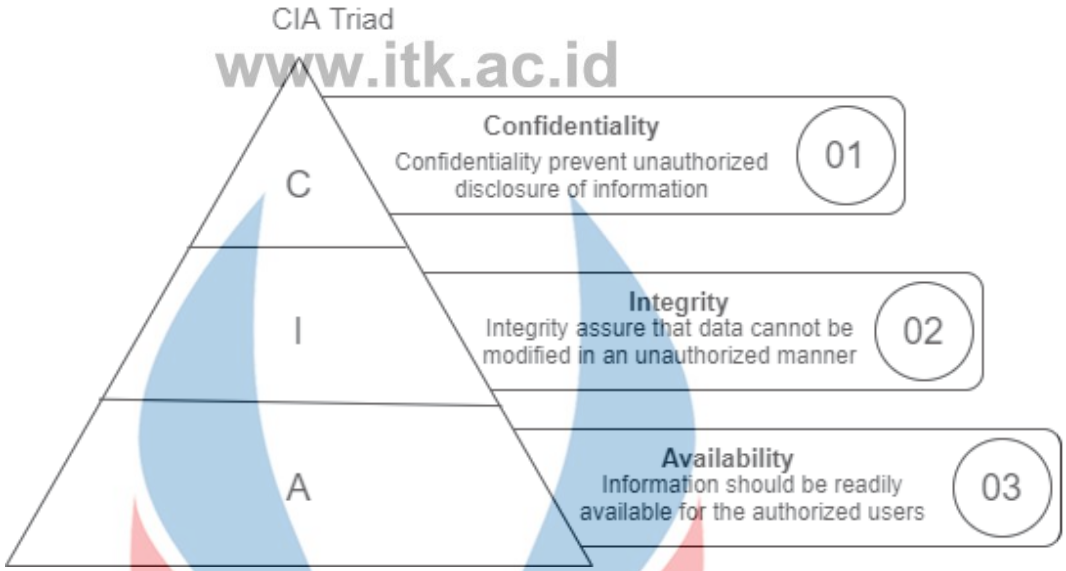
   Jaringan komputer merupakan hubungan antara beberapa komputer satu dengan yang lainnya agar dapat saling berbagi data dan informasi, mempermudah komunikasi dan membantu dalam memberikan akses informasi dengan cepat.

2.3 Keamanan Informasi

Dalam sebuah organisasi tentu memiliki aset. Informasi merupakan salah satu yang dimiliki oleh organisasi. Informasi merupakan nilai tertentu yang harus dilindungi dan dijaga oleh organisasi atau perusahaan agar tidak mengalami kerusakan yang disebabkan oleh kebocoran sistem keamanan informasi dan perlindungan dari ancaman ini juga bertujuan agar keberlangsungan bisnis dapat selalu terjaga.

Keamanan informasi merupakan suatu perlindungan dari acaman yang mungkin terjadi dan tidak diinginkan seperti adanya akses dari pihak-pihak yang tidak berwenang, terjadinya pengungkapan, perubahan, penghancuran atau gangguan yang tidak sah terhadap informasi dan sistem (Sofana & Primartha, 2019).

Adapun aspek-aspek atau *key objectives* dari keamanan informasi yang digambarkan pada diagram dan disebut dengan CIA Triad pada **Gambar 2.1** (Sofana & Primartha, 2019).



Gambar 2.2 Aspek keamanan informasi (Sofana & Primartha, 2019).

Adapun aspek-aspek keamanan informasi berdasarkan **Gambar.21** (Sofana & Primartha, 2019):

1. *Confidentiality*

Confidentialilty atau kerahasiaan mengarah kepada perlindungan informasi dari akses yang tidak sah atau memberikan batasan kepada orang-orang yang tidak diberikan hak akses. *Confidentiality* memastikan bahwa yang diberikan izin dalam mengakses sistem maka akan dapat melakukannya dan yang tidak diberikan izin akses maka tidak akan dapat melakukan akses informasi. Tujuannya agar informasi yang dimiliki dapat dicegah agar tidak terjadi kebocoran informasi kepada pihak-pihak yang tidak bertanggung jawab.

2. *Integrity*

Integrity atau keutuhan mengarah kepada perlindungan informasi dari perusakan yang berasal dari orang yang tidak memiliki hak dalam akses. Diperlindungan ini agar pihak-pihak yang tidak memiliki izin akses tidak akan dapat mengubah informasi yang ada. *Integrity* memastikan bahwa informasi dan sistem informasi itu akurat, lengkap dan tidak rusak.

3. *Availability*

Availability atau ketersediaan mengarah kepada perlindungan informasi dan sistem informasi dari gangguan yang berasal dari orang yang tidak memiliki izin akses. *Availability* memastikan bahwa pengguna atau *user* yang memiliki izin akses

akan dapat melakukan akses informasi secara tepat waktu dan juga dapat mengaksesnya dengan cepat.

2.4 Manajemen Risiko

Menurut KBBI risiko adalah akibat yang tidak menyenangkan dimana dapat memberi kerugian atau membahayakan. Risiko berasal dari kata Italia "risicare" yang mana artinya suatu pilihan dalam kondisi yang tidak pasti atau risiko merupakan suatu ketidakpastian yang dapat mempengaruhi organisasi. Risiko dapat mempengaruhi secara negatif dalam mencapai tujuan suatu organisasi. Manajemen risiko dianggap sebagai lapisan tengah pada struktur sebuah tata kelola. Tujuan dari manajemen risiko ialah untuk melakukan identifikasi dan meminimalisir sebuah risiko yang dapat memberi pengaruh dalam mencapai keberhasilan organisasi (Anderson dkk, 2017).

Pengertian manajemen risiko berdasarkan dari *Institute Risk Management* (IRM) yaitu proses yang memberikan bantuan kepada organisasi agar dapat memahami, melakukan evaluasi dan juga melakukan pengambilan tindakan dari risiko yang muncul. Organisasi melakukan hal ini agar dapat menaikkan kemungkinan keberhasilan dan mengurangi kemungkinan dari kegagalan organisasi (Hopkin, 2010).

Pengertian manajemen risiko berdasarkan dari *Business Cotinuity Insitute* yaitu budaya, proses dan struktur yang diimplementasikan oleh organisasi secara efektif untuk mengelola pelung dan menghindari kegagalan yang mungkin dapat terjadi pada organisasi (Hopkin, 2010).

2.5 Perbandingan Metode

Dalam melakukan manajemen risiko keamanan ada beberapa metode yang dapat digunakan seperti metode NIST 800-30,OCTAVE, ITIL dan COBIT . Namun tidak semua metode dapat digunakan, sehingga metode yang akan digunakan harus di lakukan penyesuaian dengan apa yang dibutuhkan.

NIST (*National Institute of Standard and Technology*) merupakan suatu organisasi pemerintah yang ada di Amerika Serikat. NIST 800-30 merupakan suatu metode yang digunakan untuk memanajemen risiko keamanan informasi dengan tujuan agar dapat menangani risiko yang akan terjadi pada organisasi. NIST 800-

30 digunakan untuk melakukan analisis risiko, melakukan penilaian dan memitigasi risiko yang berfokus pada sistem informasi. Metode ini juga fokus terhadap teknologi dan dilakukan oleh ahli pimpinan (Mahardika, 2017).

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan metode yang banyak digunakan dalam melakukan penelitian untuk menganalisis dan mengidentifikasi risiko. OCTAVE digunakan untuk melakukan analisis risiko teknologi informasi yang berfokus pada dua aspek yaitu aspek organisasi dan teknologi. OCTAVE berfungsi dalam bagian perencanaan yaitu dengan melakukan identifikasi dan analisis risiko yang berkaitan dengan teknologi informasi dari aspek keamanan pada suatu organisasi. OCTAVE merupakan suatu metode *self-directed evaluation* atau evaluasi yang dapat dilakukan sendiri (Nawangsih, 2017). Dalam metode OCTAVE terdapat metode penyederhanaan dari OCTAVE yaitu metode OCTAVE-S. OCTAVE-S dan OCTAVE pada dasarnya memiliki output yang sama. Perbedaan OCTAVE dan OCTAVE-S adalah metode OCTAVE digunakan pada organisasi yang besar sedangkan OCTAVE-S digunakan untuk organisasi kecil. Pada metode OCTAVE-S terdapat kriteria yaitu untuk fungsi pada teknologi informasi dilakukan secara *outsource,* infrastruktur teknologi informasi yang dimiliki relatif sederhana dimana dalam suatu organisasi paling tidak terdapat satu orang yang mengerti, keterbatasan pemahaman untuk menggunakan alat dalam melakukan evaluasi risiko terhadap aset informasi dan beberapa layanan teknologi informasi yang berasal dari pihak ketiga (Wijayanti, 2018).

ITIL (*Information Technology Infrastructure Library*) adalah suatu *framework* yang digunakan untuk memanajemen layanan TI dan menjadi panduan dalam melakukan penyusunan langkah-langkah operasional. Penggunaan ITIL dapat memberikan peningkatan kepuasan pelanggan suatu perusahaan *dan quality control* akan meningkat. Konsep ITIL bersifat komprehensif dan mencakup secara keseluruhan lifecycle yang menyebabkan sulit untuk dipahami (Sembilla dkk, 2018) .

COBIT (*Control Objectives for Information and Related Technology*) merupakan sebuah *framework* yang berhubungan dengan tata kelola teknologi informasi. COBIT mendefinisikan komponen dan faktor desain untuk membuat dan

mempertahankan sistem tata kelola. Prinsip COBIT yaitu prinsip yang berhubungan dengan persyaratan utama sistem tata kelola TI dan prinsip untuk kerangka kerja tata kelola yang digunakan untuk memabngun sistem tata kelola suatu perusahaan (Thenu dkk, 2020).

Tabel 2.1 merupakan perbedaan antara metode OCTAVE dengan metode NIST (Alberts dkk, 2005):

Tabel 2.1Perbedaan Antar Metode

OCTAVE	NIST	COBIT	ITIL
Mengevaluasi organisasi	Mengevaluasi sistem	Mengevaluasi tata kelola TI	Mengevaluasi layanan TI
Fokus kepada praktik keamanan	Fokus kepada teknologi	Fokus pada kendali serta pengukuran tata kelola TI dan manajemen organisasi	Fokus kepada tata kelola teknologi informasi
Permasalahan strategi	Permasalahan taktis	Permasalahan taktis	Permasalahan taktis

Pada penelitian ini akan digunakan metode OCTAVE-S untuk melakukan analisis risiko keamanan informasi karena metode ini menilai terjadinya suatu risiko dari berbagai perspektif organisasi. Pemilihan metode ini berdasarkan dari kesesuaian kebutuhan dan keadaan organisasi yaitu DISKOMINFO. Kriteria yang ada pada OCTAVE-S sesuai dengan keadaan DISKOMINFO saat ini, dimana seperti fungsi-fungsi teknologi informasi yang dilakukan secara *outsource* dan terdapat layanan-layanan teknologi informasi yang dimiliki oleh DISKOMINFO berasal dari pihak ketiga hal ini dikarenakan DISKOMINFO masih dalam organisasi kecil, infrastruktur teknologi informasi yang dimiliki sederhana dan dimengerti oleh satu orang pada suatu organisasi, dan keterbatasan pemahaman mengenai alat untuk melakukan evaluasi risiko terhadap aset informasi dimana di DISKOMINFO saat ini belum pernah melakukan evaluasi risiko dikarenakan

kurangnya pelatihan yang diberikan untuk meningkatkan kemampuan di bidang teknologi informasi kepada sumber daya manusia di DISKOMINFO.

2.6 OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)

OCTAVE merupakan suatu metode dalam perencanaan keamanan untuk melakukan penilaian yang strategis berdasarkan risiko dan teknik. OCTAVE adalah suatu pendekatan mandiri yang dilakukan oleh organisasi untuk menetapkan strategi keamanan organisasi atau perusahaan. OCTAVE-S merupakan bentuk penyederhanaan dari OCTAVE. Perbedaan antara metode OCTAVE dan OCTAVE-S adalah pada metode OCTAVE digunakan pada organisasi besar sedangkan OCTAVE-S adalah kebalikan dari metode OCTAVE yaitu digunakan pada organisasi yang kecil yaitu kurang dari 100 orang. Untuk melakukan analisis risiko dengan menggunakan OCTAVE-S harus mengetahi secara luas tentang bisnis dan proses keamanan organisasi sehingga dapat melakukan aktivitas analisis risiko dengan lebih akurat. Metode OCTAVE didasarkan pada dua aspek yaitu risiko operasional dan praktik keamanan. Metode OCTAVE digunakan oleh organisasi agar dapat membuat suatu keputusan yang berkaitan dengan keamanan informasi yang berdasarkan *confidentiality, integrity, dan availability*. semua aspek risiko seperti aset, ancaman, kerentanan, dan dampaknya kepada organisasi akan di perhitungkan dalam pengambilan keputusan. Metode OCTAVE-S walaupun memiliki "look and feel" yang berbeda dengan metode OCTAVE, namun hasil yang akan dicapai adalah sama yaitu strategi perlindungan untuk organisasi (Alberts dkk, 2005).

Terdapat dua aspek unik pada OCTAVE-S yaitu sebagai berikut (Alberts dkk, 2005).

1. Evaluasi yang dilakukan dengan menggunakan OCTAVE-S dapat dilakukan sendiri atau *self-directed evaluation.* Dalam melakukan evaluasi dengan metode ini dengan membentuk tim yang menjadi bagian dari organisasi dan mengerti terkait bisnis dan juga proses keamanan organisasi. Oleh karena itu, OCTAVE-S tidak memerlukan pengumpulan data formal atau *data gathering workshop* untuk memulai evaluasinya.

2. Pada metode OCTAVE-S, sedikit mengeksplorasi terkait infrastruktur komputasi karena OCTAVE-S digunakan oleh organisasi kecil dan biasanya organisasi ini bekerjasama dengan pihak ketiga untuk layanan TI yang dimiliki.

Adapun fase-fase yang ada pada OCTAVE-S yaitu sebagai berikut (Alberts dkk, 2005):

1. Fase 1 : Melakukan pembangunan profil ancaman berdasarkan aset

   Pada tahap ini, tim analisis melakukan identifikasi pada aset-aset penting organisasi dan praktik keamanan yang telah dilakukan oleh organisasi. tim analisis kemudian akan menentukan ancaman yang ada dan akan membuat profil ancaman untuk aset yang telah diidentifikasi.

   Adapun **Tabel 2.2** yang merupakan proses dan aktivitas yang ada pada tahap 1 (Alberts dkk, 2005).

Tabel 2.2 Proses dan Aktivitas pada Tahap 1

Tahap	Proses	Aktivitas
Tahap 1: Melakukan pembangun profil ancaman berdasarkan asset	Proses 1 : melakukan identifikasi informasi organisasi	• Melakukan penetapan kriteria evaluasi terhadap dampak • Identifikasi aset yang dimiliki organisasi • Mengidentifikasi praktik keamanan yang saat ini dilakukan organisasi
	Proses 2 : membuat profil ancaman	• Melakukan pemilihan pada asset yang kritis • Melakukan pengidentifikasi terhadap kebutuhan keamanan bagi aset kritis • Melakukan identifikasi terhadap ancaman aset kritis

		• Menganalisis proses terkait teknologi

2. Fase 2 : Melakukan identifikasi kerentanan dan kelemahan infrastruktur

   Tahap ini, tim analisis melakukan analisis terhadap bagaimana orang-orang menggunakan infrastruktur teknologi informasi untuk mengakses aset yang penting atau kritis dan tim akan mengidentifikasi jalur atau pola akses dan komponen teknologi yang berkaitan dengan aset kritis.

   Adapun **Tabel 2.3** yang merupakan proses dan aktivitas yang ada pada tahap 2 (Alberts dkk, 2005).

Tabel 2.3 Proses dan Aktivitas pada Tahap 2

Tahap	Proses	Aktivitas
Tahap 2 : Melakukan identifikasi kerentanan dan kelemahan infrastruktur	Melakukan pemeriksaan pada infrastruktur teknologi informasi yang berkaitan dengan aset kritis	• Melakukan pemeriksaan pada pola akses atau jalur akses • Menganalisis proses terkait teknologi

3. Fase 3 : Melakukan pengembangkan strategi dan rencana keamanan

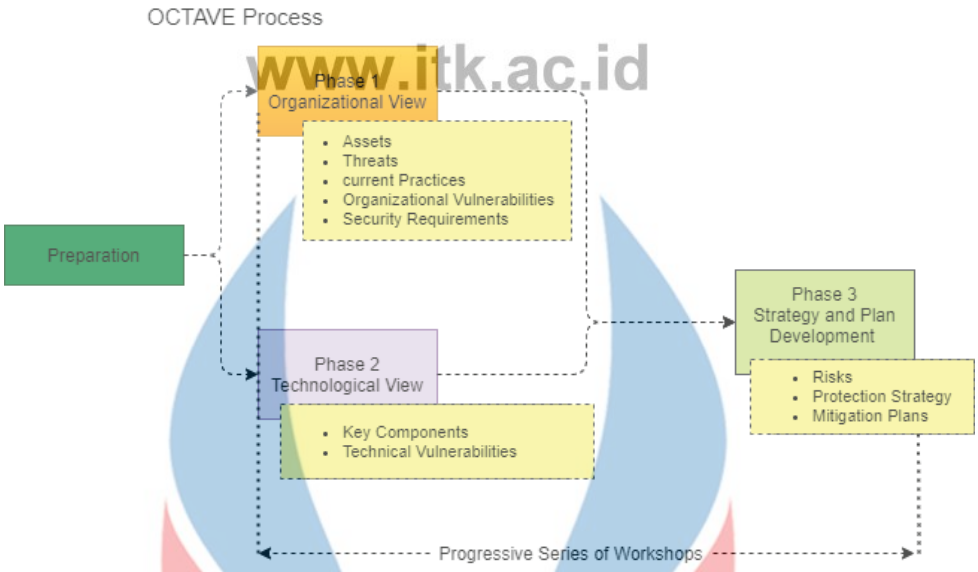
   Tahap ini, tim analisis akan melakukan identifikasi risiko terkait aset penting organisasi dan memutuskan langkah yang dapat dilakukan untuk mengatasi risiko tersebut. Berdasarkan analisis yang berasal dari informasi yang telah dikumpulkan, tim kemudian akan melakukan pembuatan strategi keamanan bagi organisasi dan rencana mitigasi risiko. Lembar kerja OCTAVE-S yang akan digunakan sangat berkaitan dengan praktik OCTAVE.

   Adapun **Tabel 2.4** yang merupakan proses dan aktivitas yang ada pada tahap 3 (Alberts dkk, 2005).

Tabel 2.4 Proses dan Aktivitas pada Tahap 3

Tahap	Proses	Aktivitas
Tahap 3 : Melakukan pengembangkan strategi keamanan dan perencanaan	Pertama melakukan identifikasi dan menganalisis risiko	• Mengevaluasi dampak ancaman • Menentukan kemungkinan kriteria dari evaluasi • Melakukan evaluasi terhadap ancaman yang mungkin terjadi
	Kedua melakukan pengembangkan strategi keamanan dan perencanaan mitigasi	• Mendeskripsikan alur strategi keamanan • Memilih pendekatan mitigasi • Mengembangkan perencanaan mitigasi risiko • Mengidentidikasi perubahan pada strategi keamanan • Mengidentifikasi langkah selanjutnya

Adapun **Gambar 2.3** yang menggambarkan fase-fase evaluasi menggunakan metode OCTAVE (Alberts dkk, 2003).



Gambar 2.3 fase-fase evaluasi OCTAVE (Alberts dkk, 2003)

Adapun contoh *worksheet* OCTAVE-S yang mana *worksheet* ini digunakan untuk menyajikan informasi dan menjadi panduan dalam melakukan pengumpulan data. Dalam *worksheet* yang disediakan oleh OCTAVE-S dibagi menjadi worksheet untuk pertanyaan terbuka, pertanyaan tertutup dan *worksheet* yang digunakan untuk menyajikan informasi. Pada **Gambar 2.4** merupakan contoh *worksheet* yang digunakan untuk pertanyaan terbuka. Pada **Gambar 2.5** merupakan contoh *worksheet* yang digunakan untuk pertanyaan tertutup. Pada **Gambar 2.6** merupakan *worksheet* yang digunakan untuk menyajikan informasi yang telah dikumpulkan.

Step 1

Productivity			Productivity
Impact Type	Low Impact	Medium Impact	High Impact
Staff Hours	Staff work hours are increased by less than _____% for _____ to _____ day(s).	Staff work hours are increased between _____% and _____% for _____ to _____ day(s).	Staff work hours are increased by greater than _____% for _____ to _____ day(s).
Other:			
Other:			
Other:			

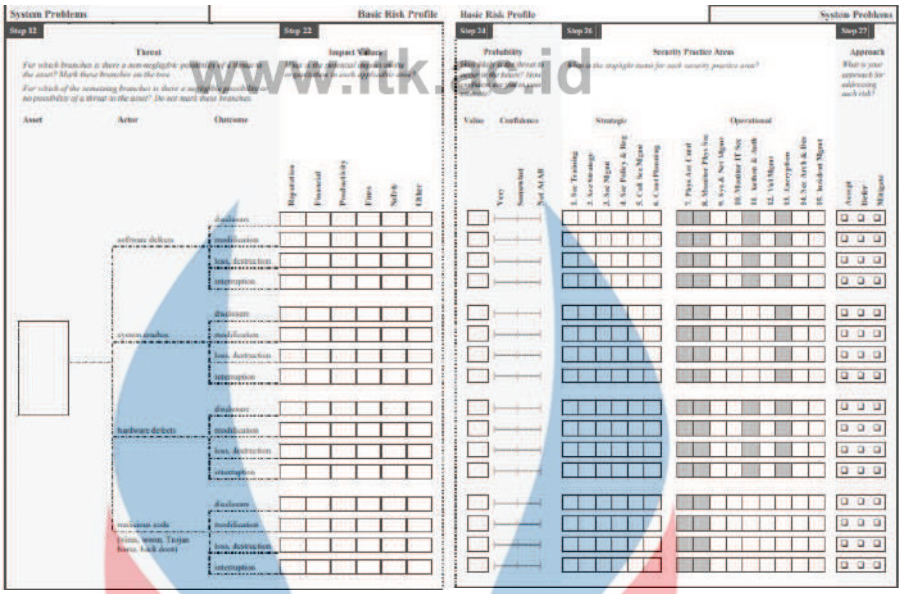
Gambar 2.4 Contoh *Worksheet* Pertanyaan Terbuka

1. Security Awareness and Training

Step 3a

Statement	To what extent is this statement reflected in your organization?
Staff members understand their security roles and responsibilities. This is documented and verified.	Very Much Somewhat Not At All Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Very Much Somewhat Not At All Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Very Much Somewhat Not At All Don't Know
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Very Much Somewhat Not At All Don't Know

Gambar 2.5 Contoh *Worksheet* Pertanyaan Tertutup



Gambar 2.6 Contoh *Worksheet* Menyajikan Informasi

2.7 FMEA (*Failure Mode and Effects*)

FMEA merupakan metode yang terstruktur yang digunakan untuk melakukan identifikasi pada mode kegagalan (failure mode) dan melakukan banyak pencegahan yang memungkinkan (Budiarto, 2017). FMEA merupakan suatu cara yang sistematis untuk mengidentifikasi kemungkinan mode kegagalan, item atau fungsi dari suatu sistem, proses atau layanan dan melakukan evaluasi dari dampak mode kegagalan pada tingkat yang lebih tinggi. FMEA bertujuan untuk menentukan penyebab dari mode kegagalan dan apa yang harus dilakukan untuk mengurangi kemungkinan kegagalan tersebut (Pentti & Atte, 2002).

Untuk melakukan penilain risiko dengan FMEA untuk mendapatkan RPN (*Risk Priority Number*) berdasarkan dari perkalian 3 variabel dari faktor penilaian risiko yaitu Severity (didapatkan dari seberapa besar dampak kegagalan), Occurrence (Intensitas kegagalan), dan Detection (kemampuan untuk kontrol) (Putri & Kusumawati, 2017).

Adapun tahapan dari FMEA yaitu (McDermott dkk, 2009):

1. Melakukan tinjauan terhadap proses atau produk
2. Melakukan identifikasi terhadap mode kegagalan
3. Membuat daftar dampak potensial dari setiap mode kegagalan
4. Menentukan tingkat *severity* dari mode kegagalan
5. Menetapkan tingkat occurrence dari mode kegagalan

6. Menetapkan tingkat detection dari mode kegagalan
7. Menghitung angka prioritas risiko dari setiap dampaknya
8. Memprioritaskan mode kegagalan untuk pengambilan tindakan
9. Mengambil tindakan untuk mengurangi atau menghilangi mode kegagalan yang memiliki risiko tinggi
10. Melakukan perhitungan RPN untuk mendapatkan hasil perhitungan dari *severity (S), occurrence (O), dan detection (D).*

FMEA dapat digunakan sebagai *tools* untuk menilai sebuah risiko dan agar hasil yang didapatkan dari penilaian dapat akurat, maka perlu untuk melakukan penentuan nilai dalam melakukan penilaian risiko. Penentuan nilai yaitu terdapat *severity, occurrence dan detection*. Berikut akan dijabarkan pembahasan dari ketiga penentuan nilai.

a. Penentuan nilai *severity* (S)

Severity atau penentuan nilai berdasarkan dampaknya. Pengukuran nilai *severity* dilihat dari seberapa sering terjadinya gangguan atau kejadian yang dapat memberi pengaruh terhadap aspek-aspek organisasi. Pada **Tabel 2.5** dibawah ini merupakan suatu parameter yang digunakan untuk menentukan nilai tingkat dampak (Nawangsih, 2017).

Tabel 2.5 Parameter Nilai *Severity*

Dampak	Dampak dari efek	Rangking
Berbahaya (sangat serius)	Rangking sangat tinggi yang dapat memberi efek terhadap keselamatan pelanggan tau karyawan	10
Berbahaya dengan peringatan	Aktivitas yang dilakukan illegal atau melanggar peraturan	9
Sangat tinggi	Produk/item atau jasa yang menjadi tidak dapat beroperasi atau kehilangan fungsinya dan tidak layak digunakan	8
Tinggi	Memberikan efek sangat tidak puas pelanggan karena adanya produk/item atau jasa yang mengalami penurunan kinerja	7

Sedang	Memberikan efek tidak puas pelanggan karena adanya salah satu produk/item atau jasa yang tidak beroperasi	6
Rendah	Produk/item atau jasa dapat beroperasi namun ada salah satu yang kinerjanya menurun dan ini memberikan efek adanya keluhan pelanggan	5
Sangat rendah	Produk/item atau jasa dapat beroperasi namun terdapat sedikit kerugian	4
Akibat ringan	Adanya kegagalan kecil namun dapat ditangani	3
Akibat sangat ringan	Adanya gangguan pada kinerja namun tidak disadar atau hanya untuk pelanggan yang sangat teliti	2
Tidak ada akibat	Tidak memberikan pengaruh yang signifikan	1

b. Penentuan nilai *occurrence* (O)

Occurrence atau penentuan nilai berdasarkan keseringan terjadinya gangguan yang dapat memberikan kegagalan. Pada **Tabel 2.6** dibawah ini merupakan suatu parameter yang digunakan untuk menentukan nilai tingkat kemungkinan terjadinya risiko (Nawangsih, 2017).

Tabel 2.6 Parameter Nilai *Occurrence*

Kemungkinan terjadinya kegagalan	Kemungkinan terjadi	Rangking
Very high (hampir tidak dapat dihindari)	Lebih dari 1 kali di setiap harinya	10
	Terjadi 1 kali setiap 3-4 hari	9
High (terjadinya berulang kali)	Terjadi 1 kali dalam seminggu	8
	Terjadi 1 kali dalam sebulan	7
Medium (terjadi dalam waktu tertentu atau hanya sesekali)	Dalam 3 bulan terjadi 1 kali	6
	Dalam 6 bulan terjadi 1 kali	5

Low (jarang terjadi atau relative kecil)	Dalam setahun terjadi 1 kali	4
	Terjadi 1 kali dalam 1-3 tahun	3
Terkendali (tidak pernah terjadi)	Terjadi 1 kali dalam 3-6 tahun	2
	Terjadi 1 kali dalam 6-50 tahun	1

c. Penentuan nilai *detection* (D)

Detection atau penentuan nilai berdasarkan bagaimana organisasi mampu untuk mengontrol dan mengendalikan gangguan yang terjadi. Pada **Tabel 2.7** dibawah ini merupakan suatu parameter yang digunakan untuk menentukan nilai deteksi pada suatu risiko (Nawangsih, 2017).

Tabel 2.7 Parameter Nilai *Detection*

Deteksi	Kriteria Deteksi	Rangking
Hampir tidak mungkin	Metode deteksi tidak ada	10
Sangat kecil	Ada metode deteksi namun tidak cukup waktu untuk melaksanakan rencana kontingensi	9
Kecil	Ada metode untuk mendeteksi namun tidak dapat dibuktikan bahwa dapat melakukan secara tepat waktu	8
Sangat rendah	Ada metode untuk mendeteksi namun tidak andal untuk melakukan deteksi secara tepat waktu	7
Rendah	Ada metode untuk mendeteksi namun tingkat efektifitas rendah	6
Sedang	Ada metode untuk mendeteksi namun deteksi yang diberikan di tingkat efektifitas di rata-rata	5
Cukup tinggi	Ada metode untuk mendeteksi dan kemungkinan untuk melakukan deteksi kegagalan cukup tinggi	4

Tinggi	Ada metode untuk mendeteksi dan kemungkinan untuk melakukan deteksi kegagalan tinggi	3
Sangat tinggi	Ada metode untuk mendeteksi dan cukup waktu untuk menjalankan rencana kontingensi dan sangat efektif untuk melakukannya	2
Hampir pasti	Ada metode untuk mendeteksi dan cukup waktu untuk dapat menjalankan rencana kontingensi dan hamper pasti untuk melakukannya	1

d. Penentuan level risiko (RPN)

Setelah dilakukan penentuan nilai terhadap *severity, occurrence*, dan *detection* maka tahap selanjutnya dapat dilakukan penentuan nilai RPN (*Risk Priority Number*.) Adapun rumus yang digunakan untuk melakukan perhitungan nilai RPN, dimana *severity (S), Occurrence (O) dan Detection (D)* dihitung dengan mengkalikannya dan didapatkan hasil RPN yang digunakan untuk menentukan level risikonya (Putri & Kusumawati, 2017):

RPN = S x O x D

S : Severity atau nilai dampak

O : Occurrence atau nilai kemungkinan

D: Detection atau nilai deteksi

Hasil dari penilaian risiko yang telah dilakukan kemudian akan diberikan rangking dengan menentukan prioritas dan level risikonya (Putri & Kusumawati, 2017).

Pada **Tabel 2.8** merupakan skala penentuan nilai RPN dimana terdapat level risiko yaitu *very high, high, medium, low dan very low.* Penentuan level risiko

berdasarkan dari hasil yang didapatkan setelah dilakukan penilaian risiko pada setiap penentuan nilai severity, occurrence dan detection (Nawangsih, 2017).

Tabel 2.8 Skala Penentuan Nilai RPN

Level Risiko	Skala Nilai RPN
Very High	>=200
High	>=120 - <200
Medium	>=80 - <80
Low	>=20 - <80
Very Low	0 - <20

Pada penelitian ini FMEA digunakan untuk mendukung metode OCTAVE-S dalam melakukan penilaian risiko. Hal ini dikarenakan FMEA mengidentifikasi penyebab kegagalan sistem serta prosesnya, efek dari kegagalan sistem, dan tingkat kritis yang berasal dari dampak suatu kegagalan. Sehingga identifikasi yang dilakukan dengan menggunakan FMEA akan lebih tepat dan efektif dalam penilaian risiko untuk memberikan rekomendasi mitigasi yang akan dihasilkan untuk DISKOMINFO. Mitigasi risiko yang akan diberikan dilihat dari segi level risiko yang memiliki kategori *very high, high, medium, low dan very low*.

2.8 ISO/IEC 27001:2013

ISO (*the International Organization for Standardization) dan IEC (the International Electrotechnical Commission*) adalah suatu organisasi yang membuat suatu sistem khusus untuk standardisasi di seluruh dunia. Standar ini merupakan standard internasional yang bertujuan untuk menerapkan, memelihara, menetapkan, dan meningkatkan sistem manajemen keamanan informasi. Penerapan sistem manajemen keamanan komuikasi ialah suatu keputusan strategis untuk sebuah organisasi. Adapun hal yang mempengaruhi suatu organisasi dalam menerapkan sistem manajemen keamanan informasi yaitu tujuan dan kebutuhan , persyaratan keamanan, dan struktur pada organisasi. Standard ISO/IEC 27001:2013 adalah standard yang dapat diterapkan secara internal dan eksternal dalam menilai

kemampuan organisasi untuk memenuhi syarat keamanan informasi organisasi (ISO/IEC 27001:2013, 2013).

Standard ini memiliki 14 klausal. Berikut merupakan klausal ISO/IEC 27001:2013 yang ditunjukan pada **Tabel 2.9** (ISO/IEC 27001:2013, 2013).

Tabel 2.9 Klausal ISO/IEC 27001:2013

A.5	Information Security Policies/Kebijakan Keamanan Informasi Merupakan suatu klausal yang menjelaskan mengenai prosedur keamanan informasi dimana bertujuan untuk memberi sebuah petunjuk dan dukungan terkait keamanan informasi yang disesuaikan dengan hukum dan peraturan yang berhubungan.
A..6	Organization of Information Security/Keamanan Informasi Organisasi Merupakan suatu klausal yang menjelaskan mengenai keamanan informasi organisasi yang bertujuan dalam pembangunan kerangka kerja manajemen untuk mengontrol pelaksanaan dan pengoperasian keamanan informasi didalam sebuah organisasi.
A.7	Human Resource Security/Keamanan Sumber Daya Manusia Merupakan suatu klausal yang menjelaskan mengenai keamanan SDM yang bertujuan untuk memastikan bahwa SDM memahami tanggung jawab mereka dan peran masing-masing dan untuk memastikan bahwa dapat memenuhi keamanan informasi mereka dan melindungi kepentingan organisasi.
A.8	Asset Management/Manajemen Aset Merupakan suatu klausal yang menjelaskan manajemen aset yang memiliki tujuan untuk melakukan identifikasi aset yang dimiliki organisasi dan tanggung jawab perlindungan yang sesuai seperti perlindungan informasi penting bagi organisasi dan mencegah adanya tindakan modifikasi,pengungkapan, penghapusan atau penghancuran informasi yang tersimpan pada sebuah media.
A.9	Access Control/Kontrol Akses

	Merupakan suatu klausal yang menjelaskan mengenai kontrol akses dimana bertujuan untuk membatasi akses informasi, memastikan akses pengguna yang sah.
A.10	Cryptography/ Teknologi Kriptografi Merupakan suatu klausal yang menjelaskan mengenai teknologi kriptografi dimana bertujuan untuk menentukan jika penggunaan kriptografi sudah tepat dan juga efektif dalam menjaga keaslian, kerahasiaan dan integritas informasi.
A.11	Physical and Environmental Security/ Keamanan Fisik dan Lingkungan Merupakan suatu klausal yang menjelaskan mengenai keamanan fisik dan lingkungan dengan tujuan untuk menghindari akses fisik yang tidak sah, kerusakan dan gangguan pada informasi dan fasilitas informasi organisasi
A.12	Operations Security/Keamanan Operasional Merupakan suatu klausal yang menjelaskan mengenai keamanan operasional yang bertujuan untuk memastikan operasi pemrosesan informasi sudah benar dan aman, melindungi dari kehilangan data, memastikan integritas sistem operasional, mencegah eksploitasi kerentanan teknis dan untuk meminimalisir ancaman dari kegiatan audit.
A.13	Communication Security/Keamanan Komunikasi Merupakan suatu klausal yang memiliki tujuan untuk memastikan bahwa informasi pada jaringan dan fasilitias pemprosesan informasi terlindungi
A.14	System Acquisition, Development and Maintenance/sistem akuisisi, Pengembangan dan Pemeliharaan Merupakan suatu klausal yang bertujuan untuk menentukan bahwa keamanan informasi telah disusun dan diimplementasikan dalam pembangunan *life cycle* sistem informasi dan memastikan bahwa data telah mendapatkan perlindungan
A.15	Supplier Relationships/ Hubungan supplier

	Merupakan suatu klausal yang bertujuan untuk menetapkan perlindungan dan mempertahankan tingkat keamanan informasi dan pemberian akses dan layanan kepada *supplier*.
A.16	Information Security Incident Management/Keamanan Manajemen insiden Merupakan suatu klausal yang bertujuan memastikan pendekatan yang konsisten dan efektif untuk pengelolaan keamanan informasi insiden.
A.17	Information Security Aspects of Business Continuity Management/Keamanan aspek manajemen kelangsungan bisnis Merupakan klausal yang menjelaskan bahwa didalam sistem manajemen kelangsungan bisnis keamanan informasi harus ditanamkan pada suatu organisasi
A.18	Compliance/Kepatuhan Merupakan klausal yang menjelaskan mengenai tindakan dalam menghindari pelanggaran hukum, undang-undang, aturan atau kontrak yang memiliki hubungan dengan keamanan informasi. Ini dilakukan untuk memastikan jika keamanan informasi pada suatu organisasi telah dilaksaakan sesuai dengan kebijakan dan prosedur yang berlaku.

Pada penelitian ini ISO/IEC 27001: 2013 digunakan sebagai acuan untuk menentukan pengendalian atau memberikan mitigasi risiko yang telah diidentifikasi dengan menggunakan metode OCTAVE-S dan penilaian risiko menggunakan metode FMEA. Standard ini dipilih karena metode ini bersifat fleksibel untuk dikembangkan dan disesuaikan dengan kebutuhan, tujuan, dan syarat keamanan organisasi serta diakui secara nasional dan internasional karena adanya sertifikat implementasi sistem manajemen keamanan informasi (Kominfo, 2016).

2.9 Penelitian Terdahulu

Berikut adalah rangkuman hasil penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang telah dilakukan.

Tabel 2.10 Penelitian terdahulu

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
1	Ritzkal, Arief Goeritno, A. Hendri-Hendrawan	2016	ISO/IEC 27001:2013	Keamanan pada jaringan hotspot yang lemah dimana hotspot ini dikelola secara mandiri	Berdasarkan analisis keamanan dengan ISO 27001:2013 pada jaringan hotspot di fakultas Teknik setelah dilakukannya pengambilan sampel dengan melakukan pembagian kuisioner maka didapatkan hasil yaitu berdasarkan dari ISO 27001 klausal 11 terkait kontrol akses, dibuktikan bahwa keamanan masuk dalam Kategori tidak aman
2	Alvina hendika Putri dan Yupie Kusumawati	2017	OCTAVE dan FMEA	Belum diterapkannya manajemen risiko untuk mitigasi risiko aset TI yang dimiliki oleh SMC RS	Berdasarkan analisis risiko yang dilakukan dengan menggunakan metode OCTAVE diperoleh risiko yang paling

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
				Telogorejo. Dampak yang terjadi adalah aset TI yang kurang terawat hingga mengalami kerusakan dan adanya serangan yang menyebabkan kacaunya sistem kerja jaringan	sering terjadi yaitu kontrol dan maintenance aset teknologi informasi yang dimiliki oleh RS Telogorejo. Dan didapatkan level risiko yaitu level low dan very low.
3	Yuca Akbar Maulana	2017	OCTAVE-S	Belum pernah dilakukannya analisis risiko dan perencanaan mitigasi pada aplikasi tele-presence milik Dinkominfo Kabupaten Malang	Didapatkan hasil penelitian dengan menggunakan metode octave-s untuk praktik keamanan yang dilakukan organisasi sebesar 51% Kategori baik, 19% Kategori cukup dan 10% Kategori kurang dan didapatkan 29 cabang ancaman aktif berdasarkan

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
					dari hasil identifikasi risiko
4	Rinaldi Pratama, Dedy Syamsuar, Yesi Novaria Kunang	2018	OCTAVE-S	Belum pernah dilakukan evaluasi risiko keamanan informasi pada sistem informasi manajemen tindak lanjut hasil pengawasan inspektorat daerah	Diperoleh aset kritis yaitu Sistem Informasi Manajemen Tindak Lanjut Hasil Pengawasan yang dimiliki oleh Inspektorat Daerah Kab. OKU, diperoleh 6 area praktik keamanan yang mempunyai kelemahan. Dan diberikan saran perbaikan yang dapat dilakukan
5	Rima Rizqi Wijayanti	2018	Octave-S dan ISO/IEC 27001:2013	Belum pernah dilakukannya penilaian analisis risiko dan kurangnya kebijakan terkait keamanan informasi	Didapatkan hasil setelah dilakukan analisis risiko dengan menggunakan metode Octave-S yaitu manajemen risiko yang dilakukan berada pada posisi sedang. Universitas

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
					Muhammadiyah Tangerang mengalami risiko yang dapat menyebabkan kerusakan atau terhentinya sistem informasi yang tentu saja akan memberikan dampak pada proses bisnisnya yang mengakibatkan kinerja universitas akan menurun.
6	Saut Pintubipar Saragih	2018	OCTAV E-S	Belum pernah dilakukannya analisis risiko pada sistem informasi manajemen pelatihan Kesehatan yang dimiliki oleh BAPELKES. Dampak yang mungkin terjadi pada	Hasil yang didapatkan setelah dilakukannya evaluasi keamanan sistem informasi dengan metode octave-s didapatkan banyak kelemahan di sisi keamanan sistem informasi yang menyebabkan

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
				sistem informasi yang dimiliki adalah risiko yang mungkin terjadi adanya kesalahan yang dilakukan oleh user sistem informasi akan berakibat besar bagi siste informasi secara keseluruhan dan dapat mengakibatkan kerugian baik secara finansial ataupun penurunan kinerja sistem	keugian bagi organisasi secara finansial, produktifitas hingga reputasi organisasi
7	Via Aprillia Prabawati, Aditya Rachmadi, Andi Reza Perdanakusuma	2019	OCTAVE-S dan FMEA	Belum pernah dilakukannya pengukuran terhadap ancaman risiko maupun menerapkan	Diperoleh aset-aset yang penting pada Unit Pengelola Sistem informasi dan Kehumasan yaitu FILMKOM Apps

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
				manajemen risiko	dan Infrastruktur Data dan Jaringan. Diperoleh hasil analisis risiko dengan OCTAVE-S terdapat 3 area praktik keamanan yang memiliki stoplight kuning dan merah dan diberikan rekomendasi pada area praktik keamanan yang berstatus stoplight kuning dan pernah sebagai langkah perbaikan.
8	Fadzri Ahdi Anshori, Suprapto dan Andi Reza Perdanakusuma	2019	OCTAVE dan ISO 27001	Pada penelitian ini didapatkan permasalahan bahwa belum adanya kebijakan terkait keamanan informasi dan	Didapatkan 12 aset kritis, 28 risiko yang mungkin terjadi pada aset kritis, dan berdasarkan identifikasi risiko dan penilaian risiko didapatkan 11 kontrol

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
				manajemen risiko	berdasarkan ISO 27001 yang akan digunakan sebagai mitigasi dan rekomendasi pencegahan risiko pada kepolisian daerah Banten.
9	Dadan Rahmat	2019	ISO/IEC 27001:2013	Belum adanya sistem manajemen keamanan informasi dan pernah terjadinya permasalahan yaitu terjadinya penyerangan pada website yang dimiliki dan berhasil menembus keamanan	Penelitian yang telah dilakukan didapatkan hasil perhitungan ancaman dengan nilai yang dikategorikan medium dan keamanan yang paling dominan yaitu pada aset server, jaringan dan sistem akdemik yang diharapkan dapat memiliki jaminan dalam aspek keamanan informasi
10	Maria Anjelina Tugas,	2019	ISO 27001:2013	Belum dilakukannya analisis manajemen	Hasil analisis yang didapatkan setelah dilakukan penelitian yaitu

No	Peneliti	Tahun	Metode	Permasalahan	Hasil
	Wasum, dan Abdul Aziz			keamanan sistem informasi akademik . permasalahan yang didapatkan adalah keamanan pada pengendalian akses jaringan yang memungkinkan terjadinya risiko penyerangan yang dapat menyebabkan kerugian bagi organisasi	untuk kebijakan pengelolaan aset sudah dilaksanakan dengan baik yaitu dengan hasil presentase perhitungan 65%