Coding : Jurnal Komputer dan Aplikasi
Volume 10, No. 02 (2022), hal 249-261

p-ISSN : 2338-493X
e-ISSN : 2809-574X

ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE *FAILURE MODE AND EFFECTS ANALYSIS* (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas)

[1]Tutik, [2]Nurul Mutiah, [3]Ibnur Rusi
[1,2,3]Jurusan Sistem Informasi, Fakultas MIPA UniversitasTanjungpura Jalan
Prof. Dr. H. Hadari Nawawi, Pontianak
Telp./Fax.: (0561) 577963
email:[1]tutik@student.untan.ac.id,[2]nurul@sisfo.untan.ac.id,[3]ibnurrusi@sisfo.untan.ac.id

Abstrak

Penerapan teknologi informasi merupakan hal penting untuk menunjang proses operasional serta mencapai visi, misi dan tujuan organisasi. Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Sambas merupakan salah satu organisasi yang menerapkan teknologi informasi untuk melakukan berbagai proses bisnis. Proses bisnis pada Diskominfo menggunakan teknologi informasi tidak terlepas dari risiko dan belum adanya dokumentasi mengenai keamanan informasi. Tujuan penelitian ini untuk mengetahui faktor yang mempengaruhi risiko aset keamanan informasi, mengidentifikasi, menilai serta memberikan rekomandasi mitigasi risiko pada Diskominfo. Metode Failure Mode and Effect Analysis digunakan untuk melakukan identifikasi proses bisnis, penyebab kegagalan, dampak kegagalan, dan pencegahan terjadinya kegagalan serta memberikan penilaian berdasarkan tingkat keparahan (severity), tingkat kejadian (occurance) dan tingkat deteksi (detection). Sedangkan ISO/IEC 27001:2013 digunakan untuk memberikan rekomandasi mitigasi risiko berdasarkan dengan klausul objektif. Pengumpulan data penelitian ini dilakukan melalui wawancara dengan pihak Diskominfo Kabupaten Sambas yang diperoleh yaitu terdapat 23 risiko aset keamanan informasi dengan 11 potensi kegagalan pada perangkat keras, 4 potensi kegagalan pada perangkat lunak, 2 potensi kegagalan pada data, 2 potensi kegagalan pada sumber daya manusia, dan 5 potensi kegagalan pada jaringan. Hasil pengkategorian risiko tersebut didapatkan 1 risiko kategori tingkat tinggi (high), 4 risiko kategori tingkat sedang (moderate), 7 risiko kategori tingkat rendah (low), dan 11 risiko kategori sangat rendah (very low). Serta rekomandasi mitigasi terdapat 6 klausul ISO/IEC 27001:2013 diantaranya yaitu Kebijakan Keamanan Informasi, Keamanan Sumber Daya Manusia, Kontrol Akses, Keamanan Fisik dan Lingkungan, Keamanan Operasional serta Keamanan Komunikasi.

Kata Kunci—*Manajemen Risiko, Keamanan Informasi, FMEA, Diskominfo, ISO/IEC 27001:2013*

1. PENDAHULUAN

Penerapan teknologi informasi saat ini merupakan salah satu kebutuhan penting sebuah organisasi untuk menunjang kegiatan operasional serta membantu meningkatkan efisiensi dan efektifitas proses kegiatan organisasi. Hal ini juga didukung dengan adanya pengelolaan teknologi informasi yang memadai untuk mencapai agar keberadaan teknologi informasi menunjang visi, misi dan tujuan organisasi. Dengan adanya penggunaan teknologi informasi pada organisasi, tidak terlepas dari adanya risiko. Salah satu penyebab dampak pada teknologi informasi adalah keamanan informasi [1]. Keamanan informasi adalah sesuatu yang sangat penting untuk dicermati bagi manajemen teknologi informasi dan perlu untuk dilakukan penilaian keamanan informasi yang sudah ditetapkan [2].

Ancaman risiko keamanan informasi yang terjadi seperti bencana alam, kebocoran data, serta gangguan lain yang berpeluang menyebabkan dampak pada aset informasi pada sebuah organisasi. Sebaiknya, aset informasi perlu untuk pengelolaan yang tepat, salah satunya dengan mengimplementasikan penilaian risiko dan mitigasi risiko yaitu manajemen risiko keamanan informasi.

Penerapan dari manajemen risiko keamanan informasi tersebut digunakan dalam mendukung

p-ISSN : 2338-493X
e-ISSN : 2809-574X

kelancaran sistem yang ada serta mencegah terjadinya gangguan.

Salah satu cara dalam melakukan identifikasi dan menilai model kegagalan teknologi informasi dari aset informasi adalah menerapkan metode *Failure Mode And Effect Analysis* (FMEA). Metode *Failure Mode And Effect Analysis* yakni proses terorganisasi untuk mencegah terjadinya kegagalan dengan menganalisis dan mengidentifikasi serta mampu memprioritaskan sumber penyebab masalah kegagalan. Sedangkan ISO/IEC 27001:2013 digunakan untuk menghasilkan rekomendasi mitigasi untuk perbaikan risiko.

Salah satu instansi yang mengimplementasikan teknologi informasi adalah Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Sambas. Belum adanya dokumentasi mengenai aset keamanan informasi dan perlu adanya pengelolaan seperti *hardware*, *software*, *network*, *data* dan *people* yang merupakan aset penting pada Dinas Komunikasi dan Informatika Kabupaten Sambas. Sehingga perlu adanya manajemen risiko keamanan informasi untuk mencegah, mengontrol dan meminimalisir risiko-risiko yang terjadi.

Berdasarkan uraian dari latar belakang diatas, maka penulis menjadikan topik penelitian berjudul "Analisis dan Manajemen Risiko Keamanan Informasi Menggunakan Metode *Failure Mode And Effects Analysis* (FMEA) dan Kontrol ISO/IEC 27001:2013 (Studi kasus pada Dinas Komunikasi dan Informatika Kabupaten Sambas)". Dengan penerapan manajemen risiko keamanan informasi berguna untuk mengidentifikasi risiko terhadap aset informasi di Dinas Komunikasi dan Informatika Kabupaten Sambas serta mampu memberikan rekomendasi mitigasi sesuai dengan hasil identifikasi risiko dan harapan organisasi yaitu pada Dinas Komunikasi dan Informatika Kabupaten Sambas.

2. LANDASAN TEORI

2.1 Risiko

Dalam kehidupan selalu terdapat unsur ketidakpastian, yang menyebabkan adanya pengaruh positif ataupun pengaruh negatif.. Ketidakpastian yang dapat menyebabkan dan menimbulkan dampak negatif serta memiliki adanya peluang kerugian disebut juga dengan risiko. Risiko adalah adanya penyimpangan yang mungkin terjadi dari tujuan sehingga menimbulkan kerugian [3].

2.2 Risiko Teknologi Informasi

Teknologi informasi adalah salah satu aset penting yang apabila terancam akan menimbulkan dampak dan terganggunya aktivitas operasional bagi suatu organisasi.

Risiko teknologi informasi merupakan ancaman yang dapat memberikan eksploitasi adanya kerentanan pada aset-aset keamanan teknologi informasi serta dapat membawa dampak kerugian pada organisasi [4].

2.3 Manajemen Risiko

Manajemen risiko merupakan usaha yang dilakukan untuk memperhitungkan segala dampak negatif dan menerapkan prosedur agar dapat meminimalisir risiko yang terjadi [5].

Adapun tujuan dari manajemen risiko untuk mengurangi atau meminimalkan adanya kemungkinan kegagalan yaitu dengan cara dihadapi dan dimitigasi terhadap teknologi informasi tersebut.

2.4 Aset Informasi

Aset salah satu komponen penting yang perlu untuk dilindungi, dijaga dan perlu adanya pengelolaan bagi suatu instansi atau organisasi. Aset informasi adalah sumber daya yang dapat menunjang proses operasional yang sangat berharga bagi perusahaan atau organisasi yang perlu untuk dikelola baik informasi dan supaya lebih dapat dimanfaatkan dengan efektif. Adapun aset informasi terdiri dari beberapa elemen yang terdiri dari *software*, *hardware*, *people*, *data* dan *network*.

2.5 Keamanan Informasi

Keamanan informasi yakni usaha yang dilakukan untuk memberikan perlindungan terhadap informasi dari segala bentuk ancaman dan memastikan adanya upaya untuk meminimalisir/memitigasi ancaman [6].

Aspek keamanan informasi mencakup 3 hal[7]. yaitu meliputi :

a. Kerahasiaan (*Confidientiality*) adalah segala aspek dari informasi yang bersifat rahasia dari pengguna yang tidak berkepentingan dan hanya orang tertentu atau orang yang berwenang saja yang bisa mengakses informasi tersebut.

b. Integritas (*Integrity*) adalah menjamin adanya konsistensi dan keutuhan dari informasi dengan tidak melakukan perubahan atau modifikasi terhadap proses dan penyimpanan informasi dari pihak berwewenang untuk menjaga tingkat keakuratan data dan kelengkapan data.

c. Ketersediaan (*Availibility*) adalah menjamin informasi ada pada saat diperlukan dan memastikan bahwa informasi bisa diakses tanpa adanya gangguan dari pihak lain.

p-ISSN : 2338-493X
e-ISSN : 2809-574X

2.6 Metode Failure Mode And Effects Analysis (FMEA)

Metode *Failure Mode and Effect Analysis* (FMEA) merupakan metode melakukan analisis maupun mengidentifikasi terhadap potensi yang dapat dikelompokkan berdasarkan permasalahan pada sistem yang mempunyai tingkat prioritas tertinggi terhadap kegagalan. Adapun ada beberapa langkah dalam melakukan analisis dengan FMEA [8], diantaranya yaitu:

1. Melakukan identifikasi proses bisnis.
2. Melakukan brainstorming risiko potensial.
3. Menetapkan tingkat keparahan (severity).
4. Menetapkan tingkat kejadian (occurrence).
5. Menetapkan tingkat deteksi (detection).
6. Menghitung tingkat prioritas risiko atau RPN (risk priority number).

Sebelum menghasilkan tingkat prioritas risiko maka nilai dikalikan dari *severiry*, *occurance*, dan *detection*.

a. tingkat keparahan *(Severity)*

Tingkat keparahan *(Severity)* adalah analisa untuk menghitung tingkatan yang berhubungan dengan seberapa besar dampak kegagalan terjadi pada sistem.

b. Tingkat kejadian (*Occurrence)*

Tingkat kejadian atau *occurrence* adalah tingkatan yang menunjukan untuk memprediksi peluang kejadian seberapa sering (intensitas risiko) terjadi pada sistem.

c. Tingkat Deteksi (*Detection)*

Tingkat deteksi atau *detection* merupakan pengukuran pencegahan dengan memperkirakan adanya kemungkinan pemicu kegagalan sistem yang terdeteksi.

$$RPN = S \times O \times D \quad (1)$$

Keterangan:
RPN = *Risk Priority Number*
S = *Severity*
O = *Occurance*
D = *Detection*

Selanjutnya setelah menghasilkan nilai RPN, maka nilai dapat diurutkan berdasarkan tingkatan level menurut FMEA. Berikut ini adalah klasifikasi level risiko berdasarkan RPN.

Tabel 1. Klasifikasi level risiko berdasarkan RPN

Level	Nilai RPN
Very Low (Sangat rendah)	0-20
Low (Rendah)	21-80
Moderate (Sedang)	81-120
High (Tinggi)	121-199
Very High (Sangat tiggi)	Lebih dari 200

2.7 ISO/IEC 27001

ISO/IEC 27001 merupakan salah satu seri yang dikeluarkan oleh *The International Organizationfor for Standardization* yang didalamnya berisi tentang spesifikasi atau persyaratan yang harus dipenuhi dalam membangun dan pengelolaan keamanan informasi melalui Sistem Manajemen Keamanan Informasi (SMKI).

2.8 ISO/IEC 27001:2013

ISO/IEC 27001:2013 digunakan pihak internal organisasi maupun pihak ekternal organisasi untuk melakukan penilaian risiko. Standar ISO/IEC 27001:2013 ini memiliki fungsi sebagai acuan untuk melakukan kontrol terhadap pengelolaan, penerapan serta untuk meningkatkan manajemen keamanan informasi[9].

ISO/IEC 27001:2013 mempunyai pengendalian keamanan informasi yaitu terdiri dari 14 Klausul dan 114 kontrol. Adapun 14 Klausul ISO/IEC 27001:2013 dapat dilihat pada tabel 2 berikut.

Tabel 2. ISO/IEC 27001:2013

A.5	Kebijakan Keamanan/*Security Policy*
A.6	Organisasi Keamanan Informasi/ *Organization of Information Security*
A.7	Keamanan Sumber Daya Manusia/ Human Resource Security
A.8	Manajemen Aset/ *Asset Manajement*
A.9	Kontrol Akses/ *Access Control*
A.10	Kriptografi/ Crypgraphy
A.11	Keamanan Fisik dan Lingkungan/ *Physical and Environmental Security*
A.12	Keamanan Operasi/ *Operations Security*
A.13	Keamanan Komunikasi/ *Communications Security*
A.14	Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi/ *System Acquisition, Development and Maintenance.*
A.15	Hubungan Pemasok/ *Supplier Relationships*
A.16	Manajemen Insiden Keamanan Informasi/*Informations Security Incident Manajement*
A.17	Aspek Keamanan Informasi Manajemen Kontinuitas Bisnis /*Information Security Aspects of Business Continuity Manajement*
A.18	Kepatuhan /*Compliance*

(Sumber : ISO/IEC 27001,2013**)**

p-ISSN : 2338-493X
e-ISSN : 2809-574X

2.9 Business Process Model and Notation (BPMN)

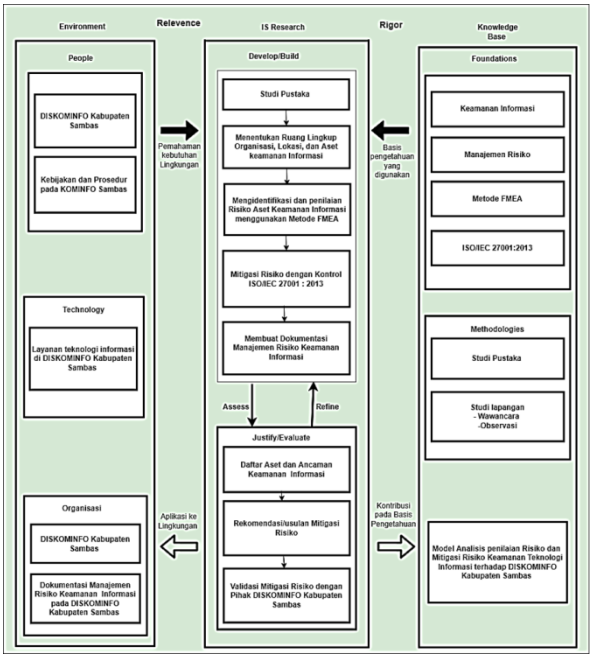
Business Process Model and Notation atau biasanya disingkat BPMN yaitu notasi berbasis diagram alur yang mendeskripsikan mengenai proses bisnis yang dikeluarkan oleh *Open Manajement Group* [10].

2.10 Archimate

Archimate merupakan salah satu standar bahasa permodelan arsitektur perusahaan yang mendukung deskripsi, analisis, dan visualisasi proses bisnis. Tujuan utama menggunakan archiMate yaitu merepresentasikan arsitektur perusahaan secara grafis agar mudah dipahami.

3. METODOLOGI PENELITIAN

Metodologi penelitian ini menggunakan *framework Is Research*, yang dapat dilihat pada gambar 1 dibawah ini.



Gambar 1. Metodologi Penelitian

3.2 Tahap Awal

3.2.1 Studi Pustaka

Studi pustaka yakni proses tahap awal pelaksanaan dalam mendukung pengerjaan penelitian dengan cara mempelajari dan mencari referensi yang menjadi dasar terkait dengan topik penelitian melalui buku, internet, dan jurnal penelitian sebelumnya. Studi pustaka yang dilakukan penulis untuk mengumpulkan dan mempelajari berbagai topik penelitian yaitu yang berhubungan dengan analisis dan manajemen risiko, keamanan Informasi, teknologi informasi, analisis manajemen berdasarkan Metode *Failure Mode And Effects Analysis* (FMEA) serta menggunakan Kontrol ISO/IEC 27001:2013.

3.3 Identifikasi dan Analisa

3.3.1 Studi Lapangan

Studi lapangan penelitian dilaksanakan pada Dinas Komunikasi dan Informatika Kabupaten Sambas, yang meliputi :

a. Observasi

Tempat observasi yang dilakukan oleh peneliti yaitu pada Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Sambas.

b. Wawancara

Adapun tujuan dari wawancara dilakukan untuk memperoleh terkait teknologi informasi dari narasumber yang terpercaya yaitu berkaitan dengan informasi yang dibutuhkan dalam proses melakukan analisis.

3.3.2 Menentukan Aset Teknologi Informasi

Sebelum pada tahap penilaian risiko maka proses identifikasi ini dilakukan untuk mendapatkan daftar-daftar aset teknologi informasi yang mempunyai risiko kritis terhadap keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Sambas.

3.3.3 Penilaian Risiko

Penilaian risiko dari tingkatan hasil dari tingkat keparahan (*severity),* tingkat kejadian (*occurrence)* dan tingkat deteksi (*Detection*) tersebut yang akan selanjutnya digunakan dalam perhitungan RPN (*Risk Priority Number).* Proses penilaian risiko yang menggunakan *Failure Mode And Effect Analysis* (FMEA) akan memperoleh skor penilaian dari nilai tertinggi (*High)* hingga yang terendah (low).

3.3.4 Mitigasi Risiko

Mitigasi risiko dilakukan dengan penerapan dari metode *Failure Mode And Effect Analysis* (FMEA) terhadap aset keamanan informasi yang kritis dan mempunyai ancaman. Mitigasi ini dilakukan berdasarkan standar dan diskusi secara langsung dengan *stakeholder* pada Dinas Komunikasi dan Informatika Kabupaten Sambas. Mitigasi risiko ini dilakukan sesuai dengan standar ISO/IEC 27001:2013.

3.4 Tahap Akhir

3.4.1 Rekomendasi Mitigasi Risiko

Mitigasi risiko ini didapatkan dari hasil identifikasi dan analisis terhadap teknologi informasi. Rekomendasi ini didapatkan daftar-

p-ISSN : 2338-493X
e-ISSN : 2809-574X

daftar dari hasil aset teknologi informasi beserta dengan mitigasi risiko yang akan dilakukan yang selanjutnya akan didiskusikan kembali dengan pihak Dinas Komunikasi dan Informatika Kabupaten Sambas.

3.4.2 Validasi

Validasi dilakukan dengan tujuan untuk menilai aset keamanan informasi dengan standar kontrol ISO/IEC 27001:2013 sesuai pada lingkungan Dinas Komunikasi dan Informatika Kabupaten Sambas. Hal ini dimaksudkan agar mitigasi dan kontrol terhadap aset informasi sesuai dengan tujuan di lingkungan Dinas Komunikasi dan Informatika Kabupaten Sambas.

4. Analisis dan Perancangan

4.1 Analisis Risiko

Menganalisis risiko aset keamanan informasi yaitu untuk menentukan aset keamanan informasi dengan penggunaan dari metode *Failure Mode And Effect Analysis* (FMEA). Penentuan aset informasi ini terdiri dari beberapa komponen yang mendukung proses operasional yaitu mencakup sumber daya manusia (*people*), perangkat keras (*hardware*), dan perangkat lunak (*software*), jaringan (*network*) dan data (*data*) pada Dinas Komunikasi dan Informatika Kabupaten Sambas.

4.2 Tahapan Analisis Failure Mode And Effect Analysis (FMEA)

Analisis risiko menggunakan metode *Failure Mode And Effect Analysis*(FMEA) yaitu salah satu metode terstruktur dalam menganalisa melakukan identifikasi serta mencegah proses mode kegagalan dari penyebab sebelum terjadi maupun meminimalisir masalah yang sudah terjadi serta memberikan penilaian terhadap ancaman yang ada. Berikut adalah analisis risiko tahapan identifikasi dan penilaian aset teknologi informasi menggunakan *Failure Mode And Effect Analysis* (FMEA) pada Dinas Komunikasi dan Informatika Kabupaten Sambas :

4.2.1 Tahap 1 - Proses Bisnis

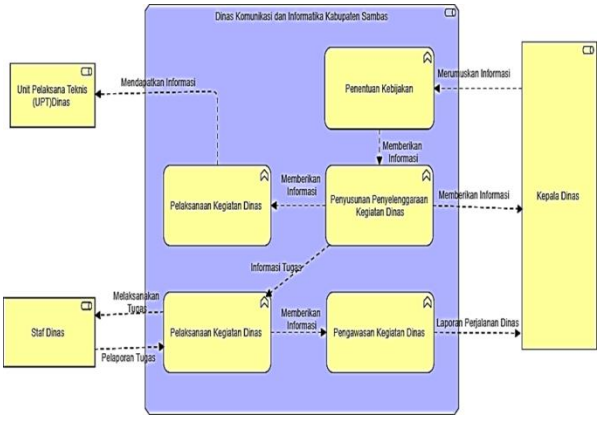
Langkah pertama yang dilakukan pada tahap *Failure Mode And Effect Analysis* (FMEA) adalah proses bisnis sebuah organisasi yaitu dengan membuat alur proses bisnis.

a. Fungsi Bisnis (*Business Function*)

Salah satu proses bisnis yang dilaksanakan pada Dinas Komunikasi dan Informatika Kabupaten Sambas ini menggunakan analisis dengan permodelan *archimate* fungsi bisnis.

Fungsi bisnis (business function) merupakan sebuah unit dari perilaku yang menjelaskan berupa tindakan (behavior) berdasarkan sumber pengetahuan, sumber daya dan lain sebagainya.

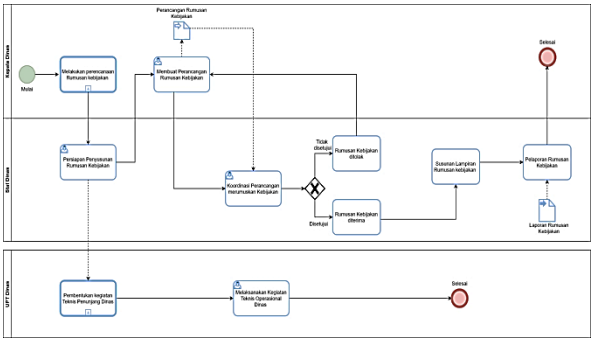
Dibawah ini menunjukan fungsi bisnis (*business function*) dengan menggunakan permodelan *archimate* yang terdapat pada Dinas Komunikasi dan Informatika Kabupaten Sambas.



Gambar 2. Fungsi Bisnis

b. Business Process Model and Notatio (BPMN)

Business Process Model and Notation (BPMN) merupakan penggambaran secara logika dengan permodelan dari setiap langkah proses bisnis dengan notasi grafikal. *Business Process Model and Notation* (BPMN) yang dianalisis melalui tugas pokok dan fungsi (tupoksi) ini yang terdiri dari keempat proses bisnis yaitu Proses Bisnis Penentuan Kebijakan, Proses Bisnis Penyusunan Penyelenggaraan Kegiatan, Proses Bisnis Pelaksanaan Kegiatan Dinas, dan Proses Bisnis Pengawasan Kegiatan.



Gambar 3. Proses Bisnis Penentuan Kebijakan

Pada gambar 3 diatas merupakan salah satu dari 4 proses bisnis yaitu proses bisnis penentuan kebijakan pada Dinas Komunikasi dan

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Informatika Kabupaten Sambas.

4.2.2 Brainstroming Risiko Potensial

Brainstorming risiko ini dilakukan pembahasan mengenai adanya kemungkinan peluang risiko keamanan informasi dari proses bisnis yang dijalankan pada Dinas Komunikasi dan Informatika Kabupaten Sambas. Adapun brainstroming peluang risiko ini terjadi pada *hardware*, *software*, *people*, *network* dan *data*.

Tabel 3. Peluang Risiko

Proses Bisnis
Pelaksanaan kebijakan di bidang pengelolaan dan informasi publik, penyelenggaraan e-goverment, hubungan media dan informatika, serta statistik dan persandian.
Peluang Risiko
Hardware - Terjadinya kerusakan fisik maupun adanya pencurian perangkat pada komputer/PC, server, dll. - Pusat data di server terkena *hack* dari pihak luar dinas. - Server mengalami akses yang lambat. - Kurangnya media penyimpanan / *Storage*. - Terjadinya bencana alam seperti banjir, kebakaran, dan lain sebagainya.
Software - Adanya kerusakan pada sistem. - Adanya pembobolan sistem atau aplikasi yang tidak sah - Terjadinya bencana alam seperti banjir, kebakaran, dan lain sebagainya.
People - Staf kurang memperhatikan pentingnya keamanan informasi karena kurangnya pelatihan dan belum sepenuhnya menguasai keterampilan/*skill* mengenai keamanan informasi. - Tidak adanya peraturan akses terhadap informasi. - Kurangnya kebijakan keamanan. - Terjadinya kerusakan pada sistem sehingga mengakibatkan aktivitas kerja. - Adanya kemungkinan penggunaan informasi untuk penipuan.
Network - Internet mengalami akses yang kurang stabil. - Terjadinya bencana alam seperti banjir, kebakaran, dan lain sebagainya.
Data - Kehilangan data-data penting karena adanya serangan virus. - Kehilangan data akibat data tidak ter-*backup.* - Adanya pencurian dan modifikasi data - Terjadinya bencana alam seperti banjir, kebakaran, dan lain sebagainya.

Pada tebel 3 diatas, merupakan salah satu peluang risiko yang diambil dari 12 pelung risiko dari hasil *brainstrming* risiko.

4.2.3 Tahap 3 – Menentukan Nilai - Nilai Risiko dari *Severity, Occurance*, dan *Detection*

Setelah dilakukan *brainstorming* risiko pada tahap sebelumnya, pada tahapan ini diberikan penilaian untuk kriteria dari tingkat keparahan (*severity),* tingkat kejadian (*occurrence),* dan tingkat deteksi (*detection*) pada masing-masing risiko dengan menggunakan lembar kerja dari *Failure Mode and Effect Analysis* (FMEA). Parameter kriteria dari *severity*, *occurance* dan *detection* dapat pada tabel berikut.

Tabel 4. Tingkat keparahan(Severity)

Peringkat	**Dampak**	**Dampak Severity**
10	**Berbahaya ; Tanpa peringatan**	Mengakibatkan proses organisasi berhenti dalam jangka waktu yang lama > 1 minggu.
9	**Berbahaya ; Dengan peringatan**	Dapat menimbulkan proses pengorganisasian terhenti selama waktu yang cukup lama > 1 hari.
8	**Sangat tinggi (*very high)***	Menimbulkan proses organisasi terhenti dalam waktu yang sebentar<1 hari.
7	**Tinggi (*high)***	Menimbulkan proses organisasi terhenti dalam waktu 1 hari.
6	**Sedang (*Moderate)***	menyebabkan layanan gagal berfungsi sebagaimana mestinya.
5	**Rendahh (*low*)**	Menimbulkan komplain.
4	**Sangat Rendah (*very low)***	Menimbukan gangguan yang cukup berpengaruh/ menyebabkan sedikit kerugian.
3	**Sedikit (*minor*)**	Menyebabkan sedikit terjadinya gangguan maupun menyebabkan sedikit masalah yang bisa diperbaiki tanpa adanya kehilangan sesuatu.
2	**Sangat Sedikit (*very minor*)**	Tidak diperhatikan, namun memberikan dampak kecil terhadap kinerja.
1	**Tidak ada (*none*)**	Tidak diperhatikan, tidak mempengaruhi terhadap kinerja.

*(**Sumber** : Dyadem Press,2003)*

Tabel 5. Tingkat Kejadian (Occurrance)

Per	**Dampak**	**Kemungkinan terjadi**

p-ISSN : 2338-493X
e-ISSN : 2809-574X

ing kat		
10	**Sangat tinggi (*very high)* ; Kegagalan hampir tidak bisa untuk dihindari**	Lebih dari 1 kali / hari.
9		1 kali / hari.
8	**Tinggi (*high)*; Kegagalan sering terjadi atau proses sebelumnya dilakukan mengimbukan sering terjadi gagal**	1 kali / 2-4 hari.
7	**Sedang (*Moderate)* ; Cukup sering terjadi**	1 kali / 1 minggu.
6		1 kali / 2 minggu.
5		1 kali / 1 bulan.
4	**Rendah (*Low)* : Cukup jarang terjadi**	1 kali / 3 bulan.
3		1 kali /6 bulan.
2	**Sangat Rendah (*Very Low)***	1 kali/ 1 tahun.
1	**Hampir tidak mungkin terjadi**	1 kali / beberapa tahun

(**Sumber** : *Dyadem Press,2003*)

Tabel 6. Tingkat Deteksi (Detection)

Peringkat	Dampak	Deteksi
10	**Hampir tidak mungkin**	Potensi penyebab tidak dapat diidentifikasi atau dikendalikan .
9	**Sangat sulit**	Sangat sulit untuk mendeteksi risiko, sangat sulit kendalikan.
8	**Sulit**	Sulit terdeteksi atau sulit terkontrol.
7	**Cukup sulit**	Cukup sulit untuk dideteksi, atau cukup sulit untuk dikendalikan
6	**Normal**	Bisa dideteksi dengan usaha ekstra atau bisa dikontrol dengan usaha ekstra
5	**Sedang**	Dapat dideteksi, dapat dikontrol.
4	**Cukup mudah**	Lumayan mudah untuk dideteksi atau lumayan mudah untuk dikontrol.
3	**Mudah**	Mudah dideteksi, mudah dikontrol.
2	**Sangat Mudah**	Sangat mudah untuk dideteksi, sangat mudah dikontrol.
1	**Hampir pasti**	Terlihat jelas, sangat mudah pengendaliannya.

*(**Sumber** : Dyadem Press,2003)*

4.2.4 Hasil RPN

Setelah pemberian penilaian risiko dari tingkat keparahan (*severity)*, tingkat kejadian (*occurrence)*, dan tingkat deteksi (*detection*) dari pihak Dinas Komunikasi dan Informatika Kabupaten Sambas dengan melakukan pengisian lembar kerja dari *Failure Mode and Effect Analysis* (FMEA) yaitu terdapat 23 risiko. Berikut hasil *Risk Priority Number* (RPN) dengan oleh pihak dinas komunikasi dan informatika Kabupaten Sambas.

Tabel 7. Hasil RPN

No	Kategori	Nama Komponen	Potensi Kegagalan	S	O	D	RPN	Level	Tingkatan Risiko
1	Perangkat Keras (Hardware)	Komputer/PC	Rentan terhadap debu atau kelembaban	3	2	3	18	Very Low	14
2		Komputer/PC	Terjadinya bencana alam (banjir, petir, ke	6	1	3	18	Very Low	13
3		Kabel UTP	Peletakan kabel yang sembarangan	3	1	1	3	Very Low	22
4		Kabel UTP	Kabel digigit oleh hintang pengerat (tikus)	1	1	1	1	Very Low	23
5		Server	Tidak adanya proses kontrol dan pemelih	3	3	3	27	Low	10
6		Server	Terjadinya bencana alam (kebakaran, pet	3	1	3	9	Very Low	20
7		Server	Tidak berfungsinya pendingin ruangan (AC	3	3	3	27	Low	11
8		Server	Kapasitas penyimpanan yang sudah penuh	4	3	3	36	Low	9
9		Kabel Listrik	Terjadinya arus pendek pada listrik.	2	3	2	12	Very Low	17
10		Kabel Listrik	Beban listrik terlalu berat untuk menampur	2	1	2	4	Very Low	21
11		Kabel Listrik	Terjadinya pemadaman listrik.	6	4	7	168	High	1
12	perangkat Lunak (Software)	Kegagalan Software	Penggunaan dari lisensi software sudah me	4	2	3	24	Low	12
13		Serangan Virus atau Malware	Antivirus tidak dapat mencegah dan mend	6	3	5	90	Moderate	3
14		Serangan Virus atau Malware	Penggunaan Antivirus versi lama	6	3	3	54	Low	7
15	Data	Kehilangan Data	Tidak melakukan backup data	6	2	4	48	Low	8
16		Pencurian Data atau adanya modifikasi data	Sistem keamanan yang masih sangat rendal	2	2	3	12	Very Low	18
17	Sumber Daya Manusia (People)	Kesalahan manusi/ Human Error	Profesionalitas kinerja	5	4	5	100	Moderate	2
18		Kesalahan manusi/ Human Error	Sumber daya manusia yang kurang kompe	5	3	5	75	Low	6
19	Jaringan (Network)	Koneksi jaringan terputus	Rusaknya perangkat jaringan	7	3	4	84	Moderate	5
20		Koneksi jaringan terputus	Gangguan jaringan pada provider	7	4	3	84	Moderate	4
21		Serangan Hacker	Lemahnya sistem keamanan informasi sen	5	1	3	15	Very Low	16
22		Server Down	Banyak yang mengakses server dalam sa	3	2	3	18	Very Low	15
23		Kesalahan Alamat IP	Kesalahan dalam melakukan konfigurasi a	3	1	3	9	Very Low	19

Hasil RPN menunjukkan bahwa tingkatan risiko kategori sangat rendah (*Very Low*) ditunjukan dengan warna hijau dimana terdapat 11 ancaman risiko yaitu masuk dengan rentang 0-20 nilai RPN diantaranya yaitu komputer/ PC rentan terhadap debu atau

p-ISSN : 2338-493X
e-ISSN : 2809-574X

kelembaban, terjadinya bencana alam (banjir, petir, kebakaran dan lain sebagainya) pada komputer/ PC, peletakan kabel yang sembarangan, kabel digigit oleh binatang pengerat(tikus), terjadinya bencana alam (banjir, petir, kebakaran dan lain sebagainya) pada server, terjadinya arus pendek pada kabel listrik, beban listrik terlalu berat untuk menampung penggunaan alat-alat digital, Sistem keamanan yang masih sangat rendah sehingga pihak yang tidak mempunyai kewenangan dapat dengan mudah mengakses data-data penting, lemahnya sistem keamanan informasi serta adanya celah sistem yang dapat di hack dari pihak luar dinas, banyaknya yang mengakses server dalam satu waktu, kesalahan dalam melakukan konfigurasi access point.

Adapun terdapat 7 ancaman risiko dalam kategori rendah (*Low*) yang ditunjukkan dengan warna biru dimana dengan rentang 21-80 nilai RPN diantaranya yaitu server yang tidak memiliki kontrol dan pemeliharaan secara rutin, tidak berfungsinya pendingin ruangan (AC) pada ruangan server, kapasitas penyimpanan yang sudah penuh yang terdapat pada server, penggunaan dari lisensi software sudah melewati batas waktu yang ditentukan, penggunaan antivirus versi lama, tidak melakukan backup data, serta sumber daya manusia yang kurang kompeten.

Dalam kategori sedang (*Moderate*) terdapat 4 ancaman risiko yang ditunjukan degan warna jingga dalam rentang 81-120 nilai RPN yaitu antivirus tidak dapat mencegah dan mendeteksi virus yang masuk pada sistem sehingga dapat merusak sistem tersebut akibat dari serangan virus atau malware, adanya kesalahan manusia akibat dari profesionalitas kinerja, koneksi jaringan terputus akibat rusaknya perangkat jaringan, serta koneksi jaringan terputus akibat gangguan jaringan pada provider dan terdapat 1 ancaman risiko masuk dalam kategori tinggi (*High*) yang ditunjukan dengan warna kuning dalam rentang 121-199 nilai RPN yaitu terjadinya pemadaman listrik. Sedangkan tidak ada ancamanan dalam kategori sangat tinggi (*Very High*) dengan rentang lebih dari 200 yang terdapat pada Dinas Komunikasi dan Informatika Kabupaten Sambas.

5. HASIL DAN PEMBAHASAN

5.1 Rekomendasi Mitigasi Standar ISO/IEC 27001:2013

Setelah melakukan analisis mengenai manajemen risiko keamanan informasi yaitu menggunakan *Failure Mode And Effect Analysis* (FMEA) di Dinas Komunikasi dan Informatika Kabupaten Sambas, selanjutnya dilakukan pemetaan pemilihan klausul dan kontrol keamanan untuk rekomendasi mitigasi risiko menggunakan standar ISO/IEC 27001:2013 yang disesuaikan dengan risiko yang terjadi di Dinas Komunikasi dan Informatika Kabupaten Sambas yaitu perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia (*people*) jaringan (*network*) dan data (*data*).

Tabel 8. Rekomandasi Mitigasi ISO/IEC 27001:2013

No	**Risiko** Kabel; Terjadinya pemadaman listrik	
1.	**Klausul** A.11 Keamanan Fisik dan Lingkungan	
	Kontrol Keamanan	**Rekomandasi**
	A.11.2.2 Utility Pendukung	Mengontrol serta melindungi baik dari adanya kegagalan sumber daya maupun dari gangguan lainnya yang berasal dari internal maupun eksernal dinas
	A.11.2.4 Pemeliharaan Peralatan	Aset yang berada pada dinas harus dipelihara dengan benar serta memastikan adanya ketersediaan dan integritasnya yang berkelanjutan.

Pada tabel diatas merupakan sebagian dari Hasil rekomendasi mitigasi risiko disesuaikan berdasarkan kontrol ISO/IEC 27001:2013. Bahwa pada Dinas Komunikasi dan Informatika Kabupaten Sambas yaitu terdapat 6 (klausul) ISO 27001:2013 Sistem Manajemen Keamanaan Informasi (SMKI) yang disesuaikan dengan risiko yang terjadi pada Dinas Komunikasi dan Informatika Kabupaten Sambas yaitu terdapat klausul 5 yaitu mengenai kebijakan keamanan informasi, klausul 7 mengenai sumber daya manusia, klausul 9 mengenai kontrol aset, klausul 11 mengenai keamanan fisik dan lingkungan, klausul 12 keamanann operasi, dan klausul 13 keamanan komunikasi.

5.2 Dokumen Sistem Manajemen Keamanan Informasi (SMKI)

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Pemilihan dan penyesuaikan klausul dan kontrol objektif rekomandasi mitigasi risiko dari tingkat tertinggi ke tingkat terendah yang terdapat pada Dinas Komunikasi dan Informatika Kabupaten Sambas menggunakan ISO/IEC 27001:2013, maka selanjutnya pembuatan kebijakan perancangan dokumen Sistem Manajemen Keamanan Informasi (SMKI) untuk Dinas Komunikasi dan Informatika Kabupaten Sambas.

Tabel 9. Dokumen Sistem Manajemen Keamanan

Dinas Komunikasi dan Informatika Kabupaten Sambas	
Nomor Dokumen	**2**
Dokumen Terkait	**Sumber Daya Manusia (SDM)**
Tujuan	a. Untuk memastikan pegawai/staf memiliki tanggung jawab terhadap keamanan informasi. b. Untuk memastikan pegawai/staf mengetahui dan memenuhi tanggung jawab mengenai keamanan informasi. c. Untuk melindungi kepentingan organisasi sebagai bagian dari proses pemberhentian atau perubahan hubungan kerja pada dinas Komunikasi dan Informatika Kabupaten Sambas.
Ruang Lingkup	Adapun ruang lingkup dari keamanan sumber daya manusia ini meliputi : a. Sebelum bekerja b. Selama bekerja c. Pemutusan hubungan kerja dan perubahan pekerjaan
Referensi	a. ISO/IEC 27001: 2013 b. Dokumen Susunan Organisasi dan Tata Kerja (SOTK) Dinas Komunikasi dan Informatika Kabupaten Sambas
Rincian Kebijakan	Adapun rincian dari kebijakan keamanan sumber daya manusia yaitu: **A. Sebelum bekerja** a. Syarat dan ketentuan kerja yaitu perjanjian semua staf/pegawai dinas harus dinyatakan dengan tanggung jawab setiap staf/pegawai mengenai keamanan informasi. **B. Selama bekerja** a. Tanggung jawab Manajemen yaitu perjanjian semua staf/pegawai dinas harus dinyatakan dengan tanggung jawab setiap staf/pegawai mengenai keamanan informasi. b. Kesadaran, Pendidikan, dan Pelatihan Keamanan Informasi yaitu perlu adanya pendidikan dan pelatihan keamanan informasi untuk staf/pegawai, serta setiap staf/pegawai memiliki kesadaran dan tanggung jawab dalam melindungi keamanan informasi dalam bekerja. c. Proses Disiplin yaitu harus ada proses disiplin pada setiap staf/pegawai dinas agar tidak terjadi pelanggaran mengenai keamanan informasi. **C. Pemutusan Hubungan Kerja dan Perubahan Pekerjaan** a. Pemutusan hubungan kerja dan perubahan pekerjaan yaitu staff/pegawai yang dimutasi atau melakukan melakukan pemutusan hubungan kerja tetap harus menjaga keamanan informasi yang ada pada Dinas Komunikasi dan Informatika Kabupaten Sambas.

Dokumen Sistem Manajemen Keamanan Informasi (SMKI) Dinas Komunikasi dan Informatika Kabupaten Sambas	
Nomor Dokumen	**3**
Dokumen Terkait	**Kontrol Akses**
Tujuan	a. Untuk melakukan pembatasan akses ke informasi dan fasilitas pemprosesan informasi. b. Untuk memastikan adanya akses pengguna yang mempunyai kewenangan dan untuk melakukan pencegahan dalam hak akses yang tidak sah ke sistem maupun layanan. c. Untuk memberikan kesadaran kepada pegawai/staf untuk bertanggung jawab dalam menjaga informasi otentifikasi yang ada.

p-ISSN : 2338-493X
e-ISSN : 2809-574X

	d. Untuk melakukan pencegahan hak akses yang tidak sah ke sistem dan aplikasi.
Ruang Lingkup	Adapun ruang lingkup dari kontrol akses ini meliputi : a. Persyaratan bisnis untuk kontrol akses b. Manajemen akses pengguna c. Tanggung Jawab Pengguna d. Kontrol akses sistem dan aplikasi
Referensi	a. ISO/IEC 27001: 2013
Rincian Kebijakan	Adapun rincian dari kebijakan kontrol akses yaitu: **A. Persyaratan Bisnis untuk Kontrol Akses** a. Kebijakan kontrol akses yaitu hanya staf/pegawai tertentu yang mempunyai kewajiban dalam mengakses keamananan informasi di dinas. **B. Kontrol Akses Sistem dan Aplikasi** a. Pembatasan Akses Informasi yaitu informasi dan fungsi sistem informasi dapat diakses dengan melakukan pembatasan sesuai dengan kebijakan kontrol akses. b. Prosedur *Log-on* yang aman yaitu jika diisyaratkan oleh kebijkan kontrol akses, maka akses ke sistem dan aplikasi harus diperiksa dengan langkah-langkah log-on yang aman. c. Sistem Manajemen Kata Sandi (*Password*) yaitu sistem manajemen kata sandi (*password*) harus menyediakan prinsip yang interaktif dan efektif kata sandi (*password*) yang berkualitas.

Dokumen Sistem Manajemen Keamanan Informasi (SMKI) Dinas Komunikasi dan Informatika Kabupaten Sambas	
Nomor Dokumen	**4**
Dokumen Terkait	**Keamanan Fisik dan Lingkungan**
Tujuan	a. Untuk melakukan pencegahan akses fisik yang tidak sah, baik dari kerusakan dan gangguan terhadap informasi organisasi dan fasilitas pemprosesan informasi pada Dinas Komunikasi dan Informatika Kabupaten Sambas. b. Untuk melakukan pencegahan dari adanya kehilangan, kerusakan, maupun dari pencurian aset serta adanya gangguan operasional organisasi.
Ruang Lingkup	Adapun ruang lingkup dari keamanan fisik dan lingkungan ini meliputi : a. Area Aman b. Peralatan
Referensi	a. ISO/IEC 27001: 2013
Rincian Kebijakan	Adapun rincian dari kebijakan fisik dan lingkungan yaitu: **A. Area Aman** a. Perimeter keamanan fisik yaitu perimeter keamanann harus ditetapkan dan digunakan untuk melindungi area yang berisi informasi sensitif atau kritis dan fasilitas pemprosesan Informasi. b. Mengamankan Kontor, Ruangan, dan fasilitas Yaitu menjaga keamanan fisik untukbaik yang ada pada kantor, ruangan, dan fasilitas harus dirancang dan ditarapkan. c. Melindungi dari Ancaman eksternal dan Lingkungan Yaitu melindungi keamanan fisik dari bencana alam, serangan berbahaya, atau kecelakaan yang harus dirancang dan diterapkan. d. Melindungi terhadap ancaman dari Luar dan Lingkungan Sekitar yaitu melindungi keamanan fisik dari bencana alam, serangan berbahaya, atau kecelakaan yang harus dirancang dan diterapkan. **B. Peralatan** a. Utility Pendukung yaitu mengontrol serta melindungi baik dari adanya kegagalan sumber daya maupun dari gangguan lainnya dari dinas. b. Keamanan Kabel yaitu kabel listrik dan telekomunikasi yang mengalirkan data atau layananan informasi membantu dalam melindungi dari adanya intersepsi, interferensi, arau kerusakan. c. Pemeliharaan Peralatan yaitu memelihara alat dengan benar untuk memastikan adanya ketersediaan dan intergritasnya secara terus-menerus.

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Dokumen Sistem Manajemen Keamanan Informasi (SMKI) Dinas Komunikasi dan Informatika Kabupaten Sambas	
Nomor Dokumen	**5**
Dokumen Terkait	**Keamanan Operasional**
Tujuan	a. Untuk melakukan penjagaan dalam pengoperasian yang benar dan aman pada aset pada saat pemprosesan informasi. b. Untuk melakukan penjagan bahwa informasi dan fasilitas pemprosesan informasi memerlukan perlindungan dari serangan malware. c. Untuk melakukan perlindungan dari adanya kehilangan data. d. Untuk merekam peristiwa dan menghasilkan bukti. e. Untuk melakukan penjagaan integritas sistem operasional. f. Untuk melakukan pencegahan terhadap eksploitasi kerentanan teknis. g. Untuk mengecilkan adanya dampak kegiatan audit pada sistem operasional.
Ruang Lingkup	Adapun ruang lingkup dari kebijakan keamanan operasional ini meliputi : a. Prosedur dan tanggung jawab operasional b. Perlindungan dari Malware c. Backup d. Logging and Monitoring e. Kontrol Perangkat lunak operasional f. Manajemen kerentanan teknis g. Pertimbangan audit sistem informasi
Referensi	a. ISO/IEC 27001: 2013
Rincian Kebijakan	Adapun rincian dari Keamanan Operasional yaitu: **A. Perlindungan dari Malware** a. Kontrol terhadap malware yaitu kesadaran pengguna dalam melindungi pemprosesan informasi dengan mengkontrol, mendeteksi, dan mencegahan dari adanya malware. **B. Backup** a. Cadangan Informasi Yaitu mencadangkan salinan informasi yang dilakukan secara berkala. **C. Kontrol perangkat lunak Operasional** a. Instalasi Perangkat Lunak Pada Sistem Operasional Yaitu adanya prosedur yang harus diimplementasikan untuk melakukan kontrol instalasi perangkat lunak pada sistem operasional.

Dokumen Sistem Manajemen Keamanan Informasi (SMKI) Dinas Komunikasi dan Informatika Kabupaten Sambas	
Nomor Dokumen	**6**
Dokumen Terkait	**Keamanan Komunikasi**
Tujuan	a. Untuk dapat melindungi informasi didalam jaringan serta melindungi fasilitas pemprosesan informasi dengan aset pendukungnya. b. Untuk melakukan penjagaan terhadap keamanan informasi yang akan ditransfer dalam suatu organisasi dengan entitas eksternal organisasi.
Ruang Lingkup	Adapun ruang lingkup dari kebijakan keamanan komunikasi ini meliputi : a. Manajemen keamanan jaringan b. Transfer Informasi
Referensi	a. ISO/IEC 27001: 2013
Rincian Kebijakan	Adapun rincian dari keamanan komunkasi yaitu: **A. Manajemen Keamanan jaringan** a. Kontrol Jaringan yaitu melakukan kontrol dan mengendalikan jaringan dalam menjaga keamanan baik pada sistem dan aplikasi pada dinas. b. Keamanan layanan jaringan yaitu proses keamanan, kualitas layanan, serta syarat dalam manajemen dari seluruh layanan jaringan harus disertakan pada sebuah perjanjian layanan jaringan, baik layanan yang disediakan sendiri atau dialihdayakan.

Adapun hasil dari analisis dan rekomandasi mitigasi 6 dokumen sistem manajemen keamanan informasi tersebut yaitu Klausul 5 mengenai Kebijakan dan Keamanan Informasi, Klausul 7 mengenai Keamanan Sumber Daya Manusia, Klausul mengenai 9

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Kontrol Akses, Klausul 11 mengenai Keamanan Fisik dan Lingkungan, Klausul 12 mengenai Keamanan Operasional, Klausul 13 mengenai Keamanan Komunikasi.

6. PENUTUP

6.1 Kesimpulan

Dari uraian pada bab sebelumnya, didapatkan kesimpulan yakni sebagai berikut :

1. Setelah diterapkan manajemen risiko pada aset teknologi informasi pada Dinas Komunikasi dan Informatika Kabupaten Sambas didapatkan 23 komponen aset keamanan informasi serta faktor penyebab peluang risiko yang mempengaruhi keamanan informasi.
2. Metode *Failure Mode and Effect Analysis* (FMEA) yang dilakukan untuk identifikasi dan penilaian risiko pada aset keamanan informasi dengan beberapa tahapan diantaranya yaitu proses bisnis, *Brainstroming* Risiko, menetukan nilai *severity*, *occurance*, *detection* serta didapatkan tingkat prioritas risiko atau *Risk Priority Number* (RPN). Risiko aset teknologi informasi memiliki hasil *Risk Priority Number* (RPN) yaitu kategori tingkat tinggi (*high*) terdapat 1 risiko, risiko kategori tingkat sedang (*moderate*) terdapat 4 risiko, risiko kategori tingkat rendah (*low*) terdapat 7 risiko, dan risiko kategori sangat rendah (*very low*) terdapat 11 risiko.
3. Hasil yang sudah dilakukan pada tahap sebelumnya dan disesuaikan dengan rekomandasi mitigasi menggunakan standar ISO/IEC 27001:2013 maka didapatkan beberapa klausul dari ISO/IEC 27001:2013 diantaranya klausul 5 mengenai Kebijakan dan Keamanan Informasi, klausul 7 mengenai Keamanan Sumber Daya Manusia, klausul 9 mengenai Kontrol Akses, klausul 11 mengenai Keamanan Fisik dan Lingkungan, Klausul 12 mengenai Keamanan Operasional, dan Klausul 13 mengenai Keamanan Komunikasi.

6.2 Saran

1. Bagi Dinas Komunikasi dan Informatika Kabupaten Sambas

Diketahui bahwa pada DinasKomunikasidan Informatika Kabupaten Sambasbelum adanya dokumentasi manajemen risiko keamanan informasi maka perlu adanya kebijakan dan prosedur yang jelas dan terdokumentasi . Pada penelitian ini didapatkan hasil dari analisis risiko dengan Failure Mode and Effect Analysis (FMEA) dan rekomandasi mitigasi risiko dengan kontrol standar ISO/IEC 27001:2013 diharapkan dapat mengetahui tingkat efektifitas serta dapat diminimalisir risiko sedini mungkin pada DinasKomunikasidanInformatika Kabupaten Sambas.

2. Bagi Program Studi Sistem Informasi

Diharapkan dengan adanya penelitian ini dapat dijadikan sebagai acuan untuk pembelajaran mengenai Analisis dan Manajemen Risiko Keamanan Informasi Menggunakan Metode *Failure Mode and Effect Anaysis* (FMEA) dan Kontrol ISO/IEC 27001:2013.

3. Bagi Peneliti Selanjutnya

Diharapkan untuk peneliti selanjutnya dapat melakukan penelitian mengenai analisis dan manajemen risiko keamanan informasi dengan menggunakan metode selain dari *Failure Mode And Effect Analysis* (FMEA) dan ISO/IEC 27001:2013, seperti NIST CSF, CIS Controls, HITRUST Common Security Framework, COSO, dan sebagainya sehingga dapat memberikan perbandingan dan melakukan perkembangan mengenai efektivitas hasil dari penilaian risiko sebelumnya.

Daftar Pustaka

[1] Bernard, P. (2011). *Foundations of ITIL 2011 Edition.* Zaltbommel: Van Haren Publishing

[2]Disterer, G. (2012). ISO/IEC 27000,27001, and 27002 for Information Security Manajement. *Journal of Information Security*.

[3] Kasidi. (2010). *Manajemen Risiko.* Bogor: Ghalia Indonesia.

[4] ISACA. (2009). *The Risk IT Framework.* ISACA.

[5] Vaughan, E. J., & Vaughan, T. M. (2013). Fundamentals of Risk and Insurance. New York: Wiley.

[6] Whitman, M. E., & M Mattord, H. J. (2010). *Management of Information Security Third Edition.* Buston: Course Technology.

[7] Supradono, B. (2009). Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE (Operationally Critical Threat,Asset, and Vulnerability Evaluation). *2(1)*.

p-ISSN : 2338-493X
e-ISSN : 2809-574X

[8] MC Demott, R., & Dkk. (2009). *The Basic of FMEA edition 2.* New York: Taylor and FrancisGroup.

[9] ISO/IEC. (2008). *Information technology – Security techniques-Information security risk management ISO/IEC FIDIS 27005:2008.*

[10] Object Management Group. (2011). *Business Process Model and Notation Versi 2.0.* Object Management Group.