Jurnal CoreIT, Vol.5, No.1, Juni 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018

Reski Mai Candra[1], Yuli Novita Sari[2], Iwan Iskandar[3], Febi Yanto[3]
[1,2,3]Teknik Informatika,UIN Sultan Syarif Kasim Riau
Jl H.R. Soebrantas No. 155 KM.18 Simpang Baru, Pekanbaru 28293
reski.candra@uin-suska.ac.id[1], yuli.novita.sari@students.uin-suska.ac.id[2], iwan.iskandar@uin-suska.ac.id[3], febiyanto@uin-suska.ac.id[3]

***Abstrak* – Dalam merancang manajemen teknologi informasi, dibutuhkan juga manajemen risiko aset teknologi informasi, pada DISKOMINFOPS Kabupaten Indragiri Hilir belum menerapkan suatu kerangka kerja berbasis keamanan informasi dalam mengelola risiko aset teknologi informasi. Salah satu penyebabnya yaitu kurangnya pemahaman pejabat teknologi informasi dalam manajemen keamanan terhadap aset teknologi informasi, sehingga memunculkan berbagai permasalahan. Dalam mewujudkan Instansi Pemerintah yang berbasis IT memiliki manajemen risiko yang baik, perlu menerapkan standar keamanan informasi yaitu ISO 31000:2018. teridentifikasi 45 risiko secara keseluruhan untuk aset, terdapat 14 risiko level rendah, 16 risiko level menengah, dan 15 risiko level tinggi. Maka DISKOMIFOPS Kab. INHIL dapat dikategorikan memerlukan perhatian khusus terutama untuk 15 risiko tinggi yang termasuk menjadi prioritas risiko didalamnya yaitu risiko koneksi jaringan putus yang sangat sering terjadi. Berdasarkan hasil pengujian UAT untuk sistem manajemen risiko keamanan aset teknologi informasi pada DISKOMINFOPS Kab. INHIL telah berjalan sesuai fungsinya dengan hasil UAT yaitu sangat bagus (82.11%). Diharapkan sistem manajemen risiko dapat dikembangkan dengan memberikan rekomendasi hasil dari penilaian resiko yang di peroleh.**

Kata Kunci - Aset Teknologi Informasi, ISO 31000, Keamanan Informasi, Manajemen Risiko.

PENDAHULUAN

Dinas Komunikasi, Informatika, Persandian dan Statistik (DISKOMINFOPS) Kabupaten Indragiri Hilir Kota Tembilahan Provinsi Riau merupakan sebuah instansi pemerintahan yang mempunyai tugas dalam melaksanakan urusan pemerintahan di bidang komunikasi, informatika, persandian dan statistik. Menurut Direktorat Sistem Informasi [1], instansi pemerintahan yang menggunakan sistem informasi wajib mengelola keamanan informasi dalam melindungi aset teknologi informasi dari berbagai ancaman risiko. Berdasarkan wawancara yang dilakukan dengan staf IT di bidang pengelola aplikasi di Dinas, bapak Said Dedi Nirtadinata, ST menyatakan bahwa permasalahan yang terjadi terkait penerapan TI di DISKOMINFOPS Kabupaten Indragiri Hilir adalah pengelolaan infrastruktur yang ada di lingkungan dinas yang belum sesuai dengan standar keamanan terhadap aset teknologi informasi dan belum adanya kebijakan yang terstruktur mengenai penanganaan khusus dalam hal pengelolaan aset teknologi informasi serta kurangnya pemahaman pejabat IT tentang manajemen keamanan terhadap aspek dan komponen aset teknologi informasi terkait, seperti perangkat keras, perangkat lunak, dokumen, jaringan dan peralatan yang mendukung. Selain itu, infrastruktur juga belum bagus, dan *intranet* hanya digunakan di ruangan tertentu saja seperti ruang *security server* serta listrik yang padam dapat terjadi dua minggu sekali. Jika listrik padam, semua aktifitas yang berhubungan dengan listrik terhenti dan masih banyak yang belum terstruktur dengan baik. Hal tersebut mengakibatkan munculnya berbagai risiko yang mengganggu proses bisnis. Salah satu staf IT, Bapak Budi Kurniawan, ST menambahkan, bahwa dalam hal keamanan risiko aset data saja, proses *backup* datanya belum sesuai dengan standar keamanan. Hal tersebut menjadi kekurangan pada DISMONIFOPS dalam mengelola risiko.

Dalam melaksanakan tugas yang didukung dengan adanya teknologi informasi di dinas tersebut, aset teknologi informasi memiliki peranan yang sangat penting guna kelangsungan proses bisnis DISKOMINFOPS Kabupaten Indragiri Hilir karena aset teknologi informasi menjadi salah satu sarana sumber informasi mengenai DISKOMINFOPS Kabupaten Indragiri Hilir. Jika aset teknologi informasi di dinas tersebut mendapat serangan berupa ancaman dan risiko dan tidak segera dilakukan penanganan, maka akan menghambat proses bisnis dan otomatis proses bisnis di DISKOMINFOPS Kabupaten Indragiri Hilir akan tidak optimal atau bahkan proses bisnis di dinas tersebut dapat terhenti. Manajemen risiko dapat mengantisipasi kerugian dan menerapkan prosedur [2]. Oleh karena itu, mengingat

pentingnya manajemen risiko dan berdasarkan paparan beberapa permasalahan tersebut perlu membuat dan menerapkan sistem manajemen risiko keamanan pada aset teknologi informasi dengan melakukan penilaian risiko guna menindaklanjuti berdasarkan perlakuan risiko yang telah diberikan agar memperkecil risiko-risiko yang berkemungkinan terjadi di DISKOMINFOPS Kabupaten Indragiri Hilir [3].

Untuk mengetahui nilai resiko pada asset Teknologi Informasi yang ada, maka digunakanlah ISO 31000:2018 dalam sistem manajemen risiko keamanan aset teknologi informasi. ISO 31000:2018 adalah standar manajemen risiko versi terbaru yang dimodifikasi oleh ISO (*International Organization for Standardization*) telah resmi dirilis pada tanggal 14 Februari 2018 yang menggantikan standar manajemen sebelumnya yaitu ISO 31000:2009 *Risk Management – Principles and Guideline* [4][5].

METODE PENELITIAN

Metode penelitian merupakan tahap dalam melakukan proses penelitian agar hasil penelitian dapat tercapai sesuai dengan yang diinginkan. Penelitian yang dilakukan di Dinas Komunikasi, Informatika, Persandian dan Statistik (DISKOMINFOPS) Kabupaten Indragiri Hilir Riau. Metode yang dilakukan pada penelitian ini dilakukan dengan cara Observasi dan Wawancara kepada Pegawai DISKOMINFOPS. Dengan melakukan Observasi dan Wawancara agar mendapatkan Data permasalahan dan melakukan penilaian Audit kepada Aset Teknologi Informasi. Setelah mendapatkan hasil Audit, barulah bisa menilai resiko yang didapat dari Tahapan ISO 31000:2018.

HASIL DAN PEMBAHASAN

Analisa sistem pada penelitian ini merupakan pembahasan mengenai tahapan-tahapan yang dilakukan pada manajemen risiko menggunakan ISO 31000.

A. Pertanyaan Audit Klausul *Framework*

Dalam melakukan penilaian klausul *framework* manajemen risiko (klausul 5) yang diterapkan, maka dibuat pertanyaan *framework* manajemen risiko yang harus diisi untuk mengetahui sejauh mana keefektifan manajemen dalam menerapkan *framework* manajemen risiko pada DISKOMINFOPS Kabupaten INHIL dalam tingkat kematangan manajemen risiko [6][7]. Berikut merupakan pertanyaan audit klausul *framework* manajemen risiko untuk DISKOMINFOPS Kabupaten INHIL.

Keterangan:

0 = tidak ada
1 = ada hanya sebagian atau belum diterapkan
2 = ada dan telah diimplementasikan

Berikut Kesimpulan hasil dari total nilai penilaian kematangan manajemen risiko dapat dilihat pada tabel berikut:

Tabel 1. Kesimpulan Total Nilai Kematangan

Nilai	Kategori
0 – 7	*Risk Naive* (Belum Sadar Risiko)
8 – 14	*Risk Aware* (Sadar Risiko)
15 – 20	*Risk Defined* (Risiko Ditetapkan)
21 – 25	*Risk Managed* (Risiko Dikelola)
Di atas 26	*Risk Enable* (Dapat Menangani Risiko)

Berikut hasil pertanyaan audit klausul *framework* manajemen risiko.

Tabel 2. Hasil Pertanyaan Audit Klausul *Framework*

No	Pertanyaan	Respon
Klausul : 5.1 kepemimpinan Dan Komitmen		
1.	Adakah menyesuaikan dan mengimplementasikan semua komponen kerangka kerja?	1
2.	Adakah menerbitkan pernyataan atau kebijakan yang menetapkan pendekatan, rencana, atau arah tindakan manajemen risiko?	1
3.	Adakah memastikan sumber daya yang diperlukan dialokasikan untuk pengelolaan risiko?	0
4.	Adakah menetapkan kewenangan, tanggung jawab dan akuntabilitas pada tingkat yang diperlukan dalam organisasi?	0
Klausul : 5.2 Integrasi		
1.	Adakah risiko dikelola di semua bagian struktur organisasi?	0
2.	Apakah setiap orang di organisasi bertanggungjawab terhadap pengelolaan risiko?	1
Klausul : 5.3 Desain		
1.	Adakah pemeriksaan organisasi dan konteksnya?	0
2.	Adakah penegasan komitmen manajemen risiko?	0
3.	Adakah penetapan peran, wewenang, tanggung jawab, dan akuntabilitas organisasi?	1
4.	Adakah alokasi sumber daya?	0
5.	Adakah penyiapan komunikasi dan konsultasi?	1

Klausul : 5.4 Implementasi		
1.	Adakah mengembangkan rencana yang sesuai, termasuk waktu dan sumber daya?	1
2.	Adakah mengidentifikasi di mana, kapan, bagaimana, dan oleh siapa beragam jenis keputusan dibuat diseluruh organisasi?	0
3.	Adakah memodifikasi proses pengambilan keputusan yang sesuai (jika diperlukan)?	0
4.	Sudahkah memastikan pengaturan organisasi dalam mengelola risiko dipahami dengan jelas dan dipraktikkan?	0
Klausul : 5.5 Evaluasi		
1.	Adakah mengukur kinerja kerangka kerja manajemen risiko secara berkala terhadap tujuan?	1
2.	Adakah menentukan apakah kerangka kerja manajemen risiko tetap sesuai untuk mendukung pencapaian sasaran organisasi?	0
Klausul : 6. Perbaikan		
1.	Adakah organisasi secara berkelanjutan memantau dan mengadaptasi kerangka kerja?	0
2.	Apakah organisasi secara sinambung meningkatkan kesesuaian, kecukupan dan efektivitas kerangka kerja manajemen risiko?	0
Total Nilai		7

B. Penilaian Risiko

Penilaian risiko bertujuan untuk mengidentifikasi risiko aset dengan mengetahui dampak dan kemungkinan terjadinya suatu risiko aset teknologi informasi di DISKOMINFOPS Kabupaten INHIL sehingga dapat dihitung berdasarkan matriks manajemen risiko untuk mengetahui apakah risiko aset tersebut dalam kategori rendah, menengah atau tinggi [8]. Berikut hasil penilaian risiko.

1. Identifikasi Risiko

Berikut daftar risiko aset data dengan risiko-risiko yang ada pada aset data yang diidentifikasi di DISKOMINFOPS Kabupaten INHIL.

Tabel 3. Identifikasi Risiko Aset Data

No.	Nama Aset	Detail Aset	Risiko
1.	Data Sektoral	Data statistik sektoral OPD dan kecamatan dalam lingkungan inhil	Kebocoran data
			Data rusak
2.	Rencana Kerja	Data perencanaan kerja SKPD	Data hilang
			Data *error*
3.	Perjanjian Kinerja	Data perjanjian kerja dengan atasan	Data tidak sesuai fakta
4.	Rencana Strategis	Data rencana strategis (RENSTRA)	Data hilang
5.	RKT	Data rencana kinerja tahunan untuk SKPD	Data hilang
			Data tidak sesuai fakta
6.	LAKIP	Data laporan akuntabilitas kinerja instansi pemerintahan untuk bahan evaluasi	Data tidak sesuai fakta

Berikut data aset *software* dan risiko pada aset *software* yang telah diidentifikasi di DIKOSMINFOPS Kabupaten INHIL

Tabel 4. Identifikasi Risiko Aset *Software*

No.	Nama Aset	Detail Aset	Risiko
1.	E-Office	Sistem E-Office berbasis web	Penyalahgunaan hak akses
			Overload
			Backup data failure
			Kurangnya pemahaman IT
2.	Cloud InhilKab	Layanan *cloud* dalam berbagi berkas pemerintahan Kabupaten INHIL	Koneksi jaringan putus
			Database error
3.	Web Hosting	Layanan hosting web OPD INHIL	Koneksi jaringan putus
4.	Satudata Inhilkab	Website Satu data Kabupaten INHIL	Serangan virus
5.	Email Server	Layanan pengiriman email	Koneksi jaringan putus
			Server *down*
			Serangan virus
			Overload

No.	Nama Aset	Detail Aset	Risiko
6.	SimPeg	Sistem informasi manajemen kepegawaian	Lemahnya *maintenance* aplikasi
			Penyalahgunaan hak akses
7.	SKP *Online*	Sasaran kerja pegawai berbasis *online*	Koneksi jaringan putus
			Kesalahan SDM
			Kurangnya pemahaman IT
8.	SMS Gateway	Layanan SMS gateway	Koneksi jaringan putus
			Kerusakan *Software*

Berikut tabel data risiko aset *hardware* yang telah diidentifikasi di DISKOMINFOPS Kabupaten INHIL.

Tabel 5. Identifikasi Risiko Aset *Hardware*

No.	Nama Aset	Detail Aset	Risiko
1.	PC	Terdapat 25 buah PC dan di semua ruangan terdapat PC.	Gangguan listrik
			Kerusakan *hardware*
			Kesalahan SDM
			Kebakaran
			Banjir
2	Printer	Terdapat 5 buah printer yang digunakan untuk mencetak dokumen keperluan dinas	Kerusakan *hardware*
			Debu atau kotoran
3	Modem	Terdapat 10 buah modem	Kerusakan *hardware*
			Pencurian perangkat
4	*Access Point*	Terdapat 8 buah Access Point	Kerusakan *hardware*
5	AC	Terdapat 15 buah AC hampir seluruh ruangan terdapat AC	Kerusakan *hardware*
			Debu atau kotoran
6	*Switch*	Terdapat 3 buah Switch	Kerusakan *hardware*
7	*Router*	Terdapat 5 buah Router	Kerusakan *hardware*
8	UPS	Terdapat 3 buah UPS	Kerusakan *hardware*
9	Server	Terdapat 5 server, yaitu 4 server aplikasi dan 1 server database.	*Server down*
			Serangan virus

2. Analisis Risiko

Berikut merupakan tabel analisa risiko dengan nilai kemungkinan dan dampak untuk masing-masing risiko yang telah diidentifikasi.

Tabel 6. Hasil Analisis Risiko

Aset	Risiko	Kemungkinan	Dampak
Kategori Aset : Data			
Data Sektoral	Kebocoran data	2	3
	Data rusak	2	5
Rencana Kerja	Data hilang	2	5
	Data *error*	3	2
Perjanjian Kinerja	Data tidak sesuai fakta	2	3
Rencana Strategis	Data hilang	3	3
RKT	Data hilang	2	4
	Data tidak sesuai fakta	3	4
LAKIP	Data tidak sesuai fakta	2	5
Kategori Aset : *Software*			
E-Office	Penyalahgunaan hak akses	1	3
	Overload	1	2
	Backup data *failure*	1	3
	Kurangnya pemahaman IT	2	2
Cloud InhilKab	Koneksi jaringan putus	4	3
	Database error	1	5
Web Hosting	Koneksi jaringan putus	4	3
Satudata Inhilkab	Serangan virus	1	2
Email Server	Koneksi jaringan putus	4	3
	Server *down*	2	5
	Serangan virus	1	2
	Overload	1	1
Simpeg	Lemahnya *maintenance* aplikasi	1	2
	Penyalahgunaan hak akses	2	3
SKP Online	Koneksi jaringan putus	4	3
	Kesalahan SDM	2	2
	Kurangnya pemahaman IT	2	2
SMS Gateway	Koneksi jaringan putus	4	3
	Kerusakan *software*	2	5
Nama Aset : *Hardware*			
PC	Gangguan listrik	5	3

Aset	Risiko	Kemungkinan	Dampak
	Kerusakan *hardware*	1	5
	Kesalahan SDM	3	2
	Kebakaran	1	5
	Banjir	1	5
Printer	Kerusakan *hardware*	1	3
	Debu dan kotoran	3	2
Modem	Kerusakan *hardware*	1	5
	Pencurian perangkat	2	5
Access Point	Kerusakan *hardware*	3	3
AC	Kerusakan *hardware*	4	3
	Debu atau kotoran	4	2
Switch	Kerusakan *hardware*	2	3
Router	Kerusakaan *hardware*	2	3
UPS	Kerusakan *hardware*	2	3
Server	Server down	3	4
	Serangan virus	1	4

C. Evaluasi Risiko.

Berikut tabel hasil level atau tingkatan risiko berdasarkan perhitungan nilai kemungkinan risiko dan dampak risiko.

Tabel 7. Hasil Evaluasi Risiko

Aset	Risiko	Kemungkinan	Dampak	Level
Kategori Aset : Data				
Data Sektoral	Kebocoran data	2	3	Menengah
	Data rusak	2	5	Tinggi
Rencana Kerja	Data hilang	2	5	Tinggi
	Data *error*	3	2	Rendah
Perjanjian Kinerja	Data tidak sesuai fakta	2	3	Menengah
Rencana Strategis	Data hilang	3	3	Menengah
RKT	Data hilang	2	4	Menengah
	Data tidak sesuai fakta	3	4	Tinggi
LAKIP	Data tidak sesuai fakta	2	5	Tinggi
Kategori Aset : *Software*				
E-Office	Penyalahgunaan hak akses	1	3	Rendah
	Overload	1	2	Rendah
	Backup data *failure*	1	3	Rendah
	Kurangnya pemahaman IT	2	2	Rendah
Cloud InhilKab	Koneksi jaringan putus	4	3	Tinggi
	Database error	1	5	Menengah
Web Hosting	Koneksi jaringan putus	4	3	Tinggi
Satudata Inhilkab	Serangan virus	1	2	Rendah
Email Server	Koneksi jaringan putus	4	3	Tinggi
	Server down	2	5	Tinggi
	Serangan virus	1	2	Rendah
	Overload	1	1	Rendah
Simpeg	Lemahnya *maintenance* aplikasi	1	2	Rendah
	Penyalahgunaan hak akses	2	3	Menengah
SKP Online	Koneksi jaringan putus	4	3	Tinggi
	Kesalahan SDM	2	2	Rendah
	Kurangnya pemahaman IT	2	2	Rendah
SMS Gateway	Koneksi jaringan putus	4	3	Tinggi
	Kerusakan *software*	2	5	Tinggi
Nama Aset : *Hardware*				
PC	Gangguan listrik	5	3	Tinggi
	Kerusakan *hardware*	1	5	Menengah
	Kesalahan SDM	3	2	Rendah
	Kebakaran	1	5	Menengah
	Banjir	1	5	Menengah
Printer	Kerusakan *hardware*	1	3	Rendah
	Debu dan kotoran	3	2	Rendah
Modem	Kerusakan *hardware*	1	5	Menengah
	Pencurian perangkat	2	5	Tinggi
Access Point	Kerusakan *hardware*	3	3	Menengah
AC	Kerusakan *hardware*	4	3	Tinggi

Aset	Risiko	Kemungkinan	Dampak	Level
	Debu atau kotoran	4	2	Menengah
Switch	Kerusakan *hardware*	2	3	Menengah
Router	Kerusakaan *hardware*	2	3	Menengah
UPS	Kerusakan *hardware*	2	3	Menengah
Server	Server *down*	3	4	Tinggi
	Serangan virus	1	4	Menengah

.

D. Perlakuan Risiko

Perlakuan risiko atau tindakan yang diberikan mencakup opsi perlakuan risiko dan keterangan usulan perlakuan dalam proses manajemen risiko. Berikut tabel perlakuan risiko untuk masing-masing aset teknologi informasi.

Tabel 8. Perlakuan Risiko

Aset	Risiko	Level	Opsi Perlakuan Risiko	Keterangan Usulan Perlakuan Risiko
Kategori Aset : Data				
Data Sektoral	Kebocoran data	Menengah	*Risk Avoidance*	Melakukan *enkripsi* data.
	Data rusak	Tinggi	*Mitigation*	- Melakukan *backup* data secara berkala sesuai standar.
Rencana Kerja	Data hilang	Tinggi	*Mitigation*	- Melakukan *backup* data secara berkala sesuai standar. - Membatasi hak akses terhadap data.
	Data *error*	Rendah	*Mitigation*	Melakukan *backup* data secara berkala sesuai standar.
Perjanjian Kinerja	Data tidak sesuai fakta	Menengah	*Risk Avoidance*	Monitoring data secara berkala.
Rencana Strategis	Data hilang	Menengah	*Mitigation*	Melakukan *backup* data secara berkala sesuai standar.
	Data tidak sesuai fakta	Tinggi	*Risk Avoidance*	Monitoring data secara berkala.
LAKIP	Data tidak sesuai fakta	Tinggi	*Risk Avoidance*	Monitoring data secara berkala.
Kategori Aset : *Software*				
E-Office	Penyalahgunaan hak akses	Rendah	*Mitigation*	Melakukan manajemen hak akses user dengan mengganti *password* secara periodik.
	Overload	Rendah	*Mitigation*	Mengoptimalisasi *database*.
	Backup data *failure*	Rendah	*Mitigation*	Melakukan *backup* data sesuai standar.
	Kurangnya pemahaman IT	Rendah	*Mitigation*	Menerapkan pelatihan terhadap SDM.
Cloud InhilKab	Koneksi jaringan putus	Tinggi	*Mitigation*	Monitoring jaringan.
	Database error	Menengah	*Mitigation*	Melakukan *backup* data secara berkala sesuai standar.
Web Hosting	Koneksi jaringan putus	Tinggi	*Mitigation*	Monitoring jaringan.
Satudata Inhilkab	Serangan virus	Rendah	*Mitigation*	Menyediakan antivirus dan monitoring antivirus serta *backup* sistem.
Email Server	Koneksi jaringan putus	Tinggi	*Mitigation*	Monitoring jaringan.

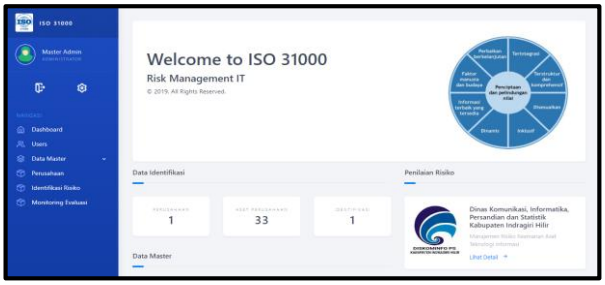
Aset	Risiko	Level	Opsi Perlakuan Risiko	Keterangan Usulan Perlakuan Risiko
	Server *down*	Tinggi	*Risk Avoidance*	Monitoring data center.
	Serangan virus	Rendah	*Mitigation*	Menyediakan antivirus dan monitoring antivirus dan *backup*
	Overload	Rendah	*Mitigation*	Melakukan *backup* data sesuai standar.
Simpeg	Lemahnya *maintenance* aplikasi	Rendah	*Risk Acceptance*	Mengoptimalkan *database.*
	Penyalahgunaan hak akses	Menengah	*Mitigation*	Melakukan manajemen hak akses user dengan mengganti *password* secara periodik.
SKP Online	Koneksi jaringan putus	Tinggi	*Mitigation*	Melakukan monitoring jaringan.
	Kesalahan SDM	Rendah	*Mitigation*	Melakukan pelatihan terhadap SDM.
	Kurangnya pemahaman IT	Rendah	*Mitigation*	Melakukan pelatihan terhadap SDM.
SMS Gateway	Koneksi jaringan putus	Tinggi	*Mitigation*	Melakukan monitoring jaringan.
	Kerusakan *software*	Tinggi	*Mitigation*	Menerapkan sesuai prosedur.
Nama Aset : *Hardware*				
PC	Gangguan listrik	Tinggi	*Mitigation*	Menyediakan genset.
	Kerusakan *hardware*	Menengah	*Mitigation*	Melakukan perawatan secara rutin.
	Kesalahan SDM	Rendah	*Mitigation*	Melakukan pelatihan terhadap SDM dan menerapkan tanggungjawab masing-masing pengguna PC.
	Kebakaran	Menengah	*Risk Avoidance*, *Mitigation*	- Menghindari sesuatu yang dapat menimbulkan kebakaran. - Melakukan *backup* data sesuai standar.
	Banjir	Menengah	*Mitigation*	- Menerapkan manajemen *Disaster Recovery Planning* (DRP) - Melakukan *backup* data sesuai standar.
Printer	Kerusakan *hardware*	Rendah	*Risk Acceptance*	Memberikan tanggung jawab kepada setiap pengguna printer untuk menggunakan sesuai prosedur.
	Debu dan kotoran	Rendah	*Mitigation*	Melakukan pemeliharaan secara rutin.
Modem	Kerusakan *hardware*	Menengah	*Mitigation*	Melakukan perawatan secara berkala.
	Pencurian perangkat	Tinggi	*Mitigation*	Memperbanyak lagi titik pemasangan CCTV.
Access Point	Kerusakan *hardware*	Menengah	*Mitigation*	Melakukan perawatan secara berkala.

Aset	Risiko	Level	Opsi Perlakuan Risiko	Keterangan Usulan Perlakuan Risiko
AC	Kerusakan *hardware*	Tinggi	*Mitigation*	-Memilih *hardware* dengan kualitas yang sudah terjamin. - Melakukan perawatan secara berkala.
	Debu atau kotoran	Menengah	*Mitigation*	Melakukan perawatan secara berkala.
Switch	Kerusakan *hardware*	Menengah	*Mitigation*	Melakukan perawatan secara berkala.
Router	Kerusakaan *hardware*	Menengah	*Mitigation*	Melakukan perawatan secara berkala.
UPS	Kerusakan *hardware*	Menengah	*Mitigation*	Melakukan perawatan secara berkala.
Server	Server *down*	Tinggi	*Risk Avoidance*, *Mitigation*	- Monitoring data center - Menggunakan pendingin ruangan yang cukup.
	Serangan virus	Menengah	*Mitigation*	- Menerapkan anti virus yang terpercaya dan *update*. - Melakukan backup server

Hasil Implementasi Sistem

A. Halaman Utama Administrator

Tampilan halaman utama administrator dapat dilihat pada gambar berikut.



Gambar 1. Halaman Utama Administrator

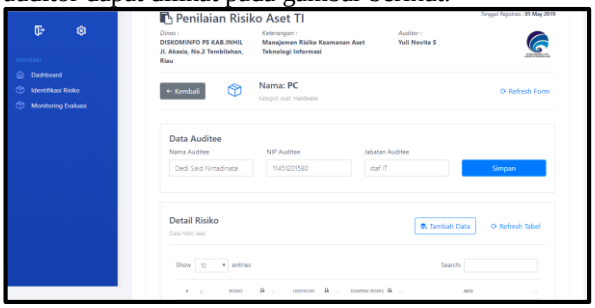
B. Halaman *Template* Identifikasi Auditor

Halaman *template* identifkasi risiko yang diakses auditor dapat dilihat pada gambar berikut.

Gambar 2. Halaman *Template* Identifikasi Auditor

C. Halaman Penilaian Risiko

Halaman penilaian risiko yang dilakukan auditor dapat dilihat pada gambar berikut.



Gambar 3. Halaman Penilaian Risiko

D. Halaman Hasil Penilaian

Halaman hasil penilaian risiko yang telah dilakukan dapat dilihat pada gambar berikut.

Gambar 4. Halaman Hasil Penilaian Risiko

E. Pengujian *Black Box*

Pengujian *black box* telah dilakukan terhadap sistem yang telah dibangun. Hasil pengujian menggunakan *black box* dapat dilihat

bahwa seluruh menu dan proses pada sistem manajemen risiko keamanan aset teknologi informasi sesuai dengan fungsinya.

F. Pengujian UAT (*User Acceptance Test*)

Terdapat 4 kategori dalam pengujian UAT yang dilakukan, yaitu kategori informatif, kategori kemudahan penggunaan, kategori ketepatan waktu dan kategori kehandalan. Sedangkan dalam menghitung masing-masing nilainya menggunakan skala *likert* untuk mengukur kesetujuan dan ketidaksetujuan terhadap suatu objek.

Perhitungan pengujian UAT dapat dilihat pada tabel berikut.

Tabel 9. Skala *Likert*

No.	Kriteria Jawaban	Bobot nilai	Kriteria Interval
1	Sangat Tidak Setuju	1	0% - 19,99%
2	Tidak Setuju	2	20% - 39,99%
3	Netral	3	40% - 59,99%
4	Setuju	4	60% - 79,99%
5	Sangat Setuju	5	80% - 100%

Perhitungan pengujian UAT menggunakan rumus perhitungan UAT yaitu sebagai berikut.

$$\textbf{Rumus} = \frac{\textbf{Total Nilai}}{\textbf{Nilai Maksimal}} \textbf{ x 100 \%}$$

Dari hasil detail pengujian UAT dengan semua kategori diatas, maka dapat diambil kesimpulan rata-rata hasil pengujian UAT sistem manajemen risiko keamanan aset teknologi menggunakan ISO 31000:2018 yaitu sebagai berikut:

$$\text{Rata – rata} = \frac{80.95+84.28+84.28+78.94}{4} \times 100\%$$
$$= 82.11\% \text{ (}\textit{Sangat Bagus}\text{)}$$

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian yang dilakukan dengan merancang dan membangun sistem manajemen risiko keamanan aset teknologi informasi menggunakan ISO 31000:2018 (studi kasus: DISKOMINFOPS Kabupaten Indragiri Hilir), maka didapatkan kesimpulan sebagai berikut:

1. Sistem manajamen risiko keamanan aset teknologi informasi telah berhasil dirancang dan dibangun sesuai proses penilaian manajemen risiko pada ISO 31000.
2. Setelah dilakukan penilaian di DISKOMINFOPS Kab. INHIL, teridentifikasi 45 risiko secara keseluruhan untuk aset, terdapat 14 risiko level rendah, 16 risiko level menengah, dan 15 risiko level tinggi. Maka DISKOMIFOPS Kab. INHIL dapat dikategorikan memerlukan perhatian khusus terutama untuk 15 risiko tinggi yang termasuk menjadi prioritas risiko didalamnya yaitu risiko koneksi jaringan putus yang sangat sering terjadi.
3. Berdasarkan pengujian UAT untuk sistem manajemen risiko keamanan aset teknologi informasi pada DISKOMINFOPS Kab. INHIL telah berjalan sesuai fungsinya dengan hasil UAT yaitu sangat bagus (82.11%).

B. Saran

Berikut merupakan saran mengenai sistem manajemen keamanan aset teknologi informasi menggunakan ISO 31000:2018.

1. Untuk manajemen risiko, pihak DISKOMINFOPS Kabupaten Indragiri Hilir perlu melakukan dengan terjadwal dan selalu memantau perkembangan setiap perlakuan risiko serta menindaklanjuti segera perlakuan risiko dengan memberi batas target tindakan agar pelaksanaan dapat sesuai dengan yang diharapkan.
2. Dalam penelitian ini, sistem yang dibangun belum menyediakan semua klausul dari ISO 31000, termasuk data histori risiko belum ada. Untuk penelitian selanjutnya, dapat diterapkan manajemen risiko dengan fitur yang lebih kompleks berdasarkan setiap klausul pada manajemen risiko ISO 31000.

REFERENSI

[1] Direktorat Sistem Informasi, "Pedoman Praktis Manajemen Keamanan Informasi Untuk Pimpinan Organisasi 10 Rekomendasi Terbaik Manajemen Keamanan Informasi," pp. 1–22, 2007.

[2] D. W. Iswari and E. K. Umar, "Perancangan Manajemen Risiko Teknologi Informasi Pada Key Supporting Process APO02, APO06 Dan APO08 Di Dinas Komunikasi Dan Informatika (DISKOMINFO) Pemerintah Kota Bandung Menggunakan Framework COBIT 5," vol. 3, no. 2, pp. 3476–3482, 2016.

[3] T. Aven, "Risk assessment and risk management : Review of recent advances on their foundation," vol. 0, pp. 1–13, 2016.

[4] K. Am, "ISO 31000:2009; ISO/IEC 31010 & ISO Guide 73:2009 International Standards for the Management of Risk," 2009.

[5] V. Sousa, N. M. De Almeida, and L. A. Dias, "Risk Management Framework for the Construction Industry According to the ISO 31000 : 2009 Standard," vol. 2, no. 4, pp. 261–274, 2012.

[6] "Risk management - guidlines ISO 31000." BSN, 2018.

[7] A. Standards, "for AS/NZS ISO 31000:2009 Risk management - Principles and guidelines," 2018.

[8] A. Novia, R. Yanuar, F. A. W. St, D. Dwi, and J. St, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Case Study : i-Gracias Telkom University)," vol. 2, no. 2, pp. 6201–6208, 2015.