Jurnal Manajemen dan Teknologi Informasi (JMTI)
Volume 14, Issue 1, 2024, pp. 48-57
ISSN 2721-7604 (Online); ISSN 2087-5312 (Print)
DOI: 10.59819

ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAK) UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMM) MENGGUNAKAN ISO 31000

Arifatun Nikmat Rahmatika[1], Muhammad Fajar Apriyadi[2], Muhammad Alfian Kahfi[3], Offy Novanindra Aibi[4]
[1]Universitas Islam Negeri Sunan Ampel Surabaya; 09040620048@student.uninsby.ac.id
[2]Universitas Islam Negeri Sunan Ampel Surabaya; 09010620009@student.uninsby.ac.id
[3]Universitas Islam Negeri Sunan Ampel Surabaya; 09010620008@student.uninsby.ac.id
[4]Universitas Islam Negeri Sunan Ampel Surabaya; 09010620013@student.uninsby.ac.id

ARTICLE INFO

Article history:
Received April 16, 2024
Revised April 23, 2024
Accepted April 25, 2024
Available online April 30, 2024

Keywords: Information technology risk management, ISO 31000, Academic Informatiomn Systems (SIAK), Muhammadiyah Sukabumi University (UMMI), UMMI SIAK System

Abstract. The study aims to analyze information technology risk management on Academic Information Systems (SIAK) of Muhammadiyah Sukabumi University (UMMI) using the ISO 31000 approach. The SIAK is one of the systems connected to a vast network and with such connections, risk affecting the continuity of the academic process can arise. To manage such risks, effective information technology risk management is required. The research uses the ISO 31000 method in identifying, assessing, andining risk. Through qualitative analysis, the risk affecting UMMI can be identified and evaluated. The results show that the risk associated with the assets of the swifts systems is one of the critical risks tha requires a constant network connection and power supply. By implementing good information technology risk managementUMMI can prevent, manage and maintain SIAK systems and their supporting assets to operate optimally. This research has contributed to improving the understanding and application of information technology risk management in the academic community. Its is hoped that the results of this research can be a benchmark for other educational institutions in managing risks on their academic information systems

PENDAHULUAN

Pada saat ini penerapan TIK di perguruan tinggi hampir semua terhubung ke jaringan luas (internet) termasuk di Universitas Muhammadiyah Sukabumi (UMMI). Salah satu sistem yang terhubung ke jaringan luas di UMMI adalah Sistem Informasi Akademik (SIAK). Dengan terhubungnya SIAK ke jaringan luas maka proses bisnis bidang akademik di UMMI menjadi lebih cepat dan mudah. Namun memunculkan hal lain juga, yaitu mendatangkan peluang terjadinya ancaman pada SIAK UMMI. Sistem Informasi Akademik (SIAK) di Universitas Muhammadiyah Sukabumi (UMMI) terdiri dari beberapa komponen yaitu perangkat keras dan jaringan computer, perangkat lunak yang terdiri dari aplikasi dan basis data SIAL, serta pengguna SIAK UMMI. Ketiga komponen tersebut merupakan aset yang penting dalam keberlangsungan proses akademik di UMMI

Pada tahun 2015 telah dilakukan penelitian di UMMI dalam upaya menerapkan tata Kelola teknologi informasi yang baik dalam mengelola teknologi informais di UMMI dengan menggunakan standar COBIT 5. Namun pelaksanaan tata Kelola teknologi informasi di UMMI masih bersifat umum karena komponen yang dibangun baru pada tahap kebijakan pengelolaan teknologi informasi. Untuk mengelola teknomogi informasi pada sistem informasi akademik secara khusus harus dilakukan sistem manajemen teknologi informasi dan salah satu bagiannya yaitu melakukan manajemen risiko teknologi informasi. Penerapan SIAK tidak terlepas dari kendala dan risiko yang terjadi. Risiko yang muncul dapat mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal dan mengganggu proses bisnis

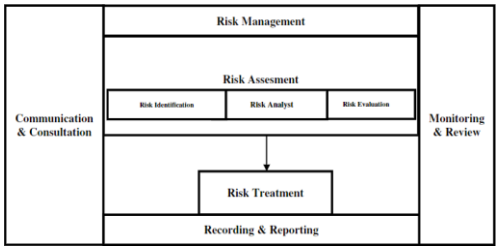
Penelitian ini menggunakan metode ISO 31000 yang meliputi identifikasi risiko, penilaian risiko dan pemeliharaan terhadap sistem dan aset pendukung kinerja sistem di masa depan. Hasil dari penelitian ini didapatkan risiko aset sistem swifts yang membutuhkan koneksi jaringan dan asupan Listrik yang konstan agar perangkat dapat berjalan untuk mendukung jalannya sistem secara optimal. Suatu Perusahaan maupun organisasi memerlukan adanya manajemen risiko. Manajemen risiko adalah suatu sistem tentang bagaimana sebuah organisasi dipimpin, diarahkan dan dikendalikan (lead, direct, control) untuk meningkatkan kinerja organisasi demi kepentingan pemegang sahan, pemangku kepentingan dan pertumbuhan ekonomi nasional. Peningkatan kinerja ini dilaksanakan dalam kerangka hukum dan norma-norma etika yang berlaku

Pada penelitian ini penulis mengambil salah satu metode untuk manajemen risiko yang sesuai untuk penanganan permasalahan diatas. Metode yang dipilih yaitu ISO 31000 yang dapat digunakan untuk organisasi, perusahaan public, perusahaan swasta, organisasi nirlaba, kelompok ataupun perseorangan. Standar ini digunakan selama masa hidup organisasi dan untuk berbagai kegiatan, proses, fungsi, proyek, produk, jasa, aset, operasi dan pengambilan keputusan. Terdapat lima kegaitan risiko yang termasuk dalam proses manajemen risiko yaitu komunikasi dan konsultasi, menentukan konteks, asesmen risiko, perlakuan risiko dan monitoring serta review. Identifikasi risiko, analisis risiko dan evaluasi risiko ketiga hal tersebut termasuk dalam bagian asesmen risiko

METODE

Penelitin ini menerapkan analissi risiko secara kualitatif dengan pendekatan studi kasus pada SIAK UMMI. Analisis kualitatif merupakan analisis yang cepat dan relative mudah untuk digunakan untuk jangkauan identifikasi dampak (impact) dan kemungkinan (likelihood) yang luas yang dapat digunakan Analisa risiko kualitatif dianggap sebagai tahapan yang paling efektif dan hemat biaya sebab melalui analisa ini, organisasi atau perusahaan dapat melakukan improvisasi terhadap performansi proyek dengan berfokus pada risiko yang memiliki tingkat prioritas tinggi (high priority risk). Metode pengumpulan data maupun informasi yang diperlukan yaitu dengan studi Pustaka. Penelitian ini menggunakan metode ISO 31000 yang meliputi identifikasi risiko, penilaian risiko dan pemeliharaan risiko yang bertujuan melakukan pencegahan, penanganan dan pemeliharaan terhadap sistem dan aset pendukuung kinerja sistem di masa depan

Metode yang dipilih yaitu ISO 31000 yang dapat digunakan untuk organisasi, perusahaan publik, perusahaan swasta, organisasi nirlaba, kelompok ataupun perseorangan. Standar ini digunakan selama masa hidup organisasi dan untuk berbagai kegiatan, proses, fungsi, proyek, jasa, aset, operasi dan pengambilan keputusan. Terdapat lima kegiatan risiko yang termasuk dalam proses manajemen risiko, perlakuan risiko dan monitoring serta review. Identifikasi risiko, analisis risiko dan evaluasi risiko ketiga hal tersebut termasuk dalam bagian assesmen risiko



Gambar 1. Manajemen Risiko ISO 31000

Berdasarkan gambar tersebut maka proses manajemen risiko ISO 31000 terdiri dari serangkaian aktivitas sebagai berikut:

1. Komunikasi dan Konsultasi (Communication and Consultation)
   Pada penelitian ini komunikasi dan konsultasi dengan pemangku kepentingan sangat penting karena mereka dapat memberikan pertimbangan dan penilaian terhadap risiko yang didasarkan atas persepsi mereka terhadap risiko tersebut
2. Penetapan Konteks (Establishing the Context)
   Terdapat empat konteks yang perlu ditentukan dalam penetapan konteks, yaitu konteks internal, konteks eksternal, konteks manajemen risiko dan kriteria risiko
3. Penilaian Risiko
   ISO 31000 : 2009 mendefinisikan asesmen risiko sebagai keseluruhan proses identifikasi risiko, analisis risiko dan evaluasi risiko
4. Identifikasi Risiko (Risk Identification)
   Identifikasi pada penelitian ini menggunakan wawancara langsung dengan pihak yang bertanggung jawab yang mencakup penilaian berdasarkan pengalaman dan pencatatan. Berikut ini adalah proses identifikasi risiko :
   a. Identifikasi teknologi informasi yang dimiliki oleh organisasi
   b. Identifikasi ancaman pada setiap teknologi informasi
   c. Identifikasi kemungkinan risiko yang diakibatkan oleh adanya ancaman
   d. Identifikasi dampak yang akan diterima oleh organisasi tersebut
5. Analisis Risiko (Risk Analysis)
   Penelitian ini menerapkan analisis risiko secara kualitatif yang dianggap sebagai tahapan yang paling efektif dan hemat biaya sebab melalui analisa ini, organisasi atau perusahaan dapat melakukan improvisasi terhadap performansi proyek dengan berfokus pada risiko yang memiliki tingkat prioritas tinggi. Prioritas risiko ini pada akhirnya dapat digunakan pula sebagai dasar dalam melakukan analisis risiko kuantitatif apabila diperlukan. Ketika peluang atau probabilitas serta dampak telah diidentifikasi, maka kemudian akan dilakukan evaluasi untuk mengetahui risiko yang menjadi prioritas untuk ditangani terlebih dahulu

Likelihood Rating	Kriteria	Keterangan	Frekuensi
1	*Rare*	Risiko hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Risiko jarang terjadi	1 – 2 tahun
3	*Possible*	Risiko kadang-kadang terjadi	7 – 12 bulan / tahun
4	*Likely*	Risiko sering terjadi	4 -6 bulan/ tahun
5	*Certain*	Risiko pasti terjadi	1 -3 bulan / tahun

Gambar 2. Kriteria Likelihood

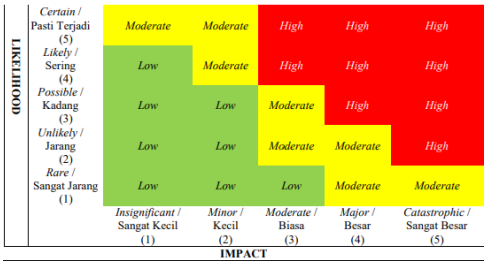
Impact Rating	Kriteria	Keterangan
1	*Insignificant*	Tidak mengganggu operasional dan aktivitas perusahaan
2	*Minor*	Proses bisnis dan aktivitas mengalami gangguan, namun tidak menghambat tugas pokok atau aktivitas inti perusahaan
3	*Moderate*	Proses bisnis mengalami gangguan sehingga sebagian aktivitas terhambat dan mengalami penundaan
4	*Major*	Menghambat hampir seluruh proses bisnis dan aktivitas perusahaan
5	*Catastrophic*	Proses bisnis mengalami gangguan total sehingga aktivitas perusahaan berhenti total dan proses bisnis tidak tercapai

Gambar 3. Kriteria Impact

6. Evaluasi Risiko (Risk Evaluation)
   Tahap ini melakukan risk evaluation atau membandingkan risiko yang sudah dihitung diatas dengan kriteria risiko yang sudah distandarkan apakah risiko itu low yang berarti risiko rendah

atau dapat diterima, moderate berarti sedang atau perlu diwaspadai atau high yang berarti tinggi atau tidak dpaat diterima, serta memprioritaskan mitigasi atau penangannya

Tabel 1. Matriks Evaluasi Risiko



Keterangan :

H : *High Risiko* (Risiko Tinggi)

M : *Moderate Risk* (Risiko Sedang)

L : *Low Risk* (Risiko Rendah)

Tabel 2. Level Risiko

Level Risiko	Keterangan
High Risk - Risiko Tinggi	Risiko yang berbahaya yang harus diatasi secepatnya.
Moderate Risk - Risiko Sedang	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan.
Low Risk - Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil.

7. Perlakuan Risiko (Risk Treatment)
   Bertujuan untuk menyeleksi dari penerapan solusi agar tepat untuk mengatasi risiko yang ada
8. Monitoring dan Review
   Bertujuan untuk peninjauan dan memastikan peningkatan kualitas yang efektif baik dari proses bisnis, pelaksanaan, sampai dengan hasilnya

HASIL DAN PEMBAHASAN

1. Penilaian Risiko (Assessment Risiko)
   Pada tahap ini merupakan tahap penilaian risiko di SIAK UMMI. Pada proses penilaian risiko SIAK UMMI ini terdiri dari 3 tahap yaitu : identifikasi risiko (risk identification), analisis risiko (risk analysis), evaluasi risiko (risk evaluation)
   a. Identifikasi Risiko
      Ada tahap ini dilakukan pengindentifikasian risiko yang mungkin ada pada SIAK UMMI. Hasil akhir dari identifikasi risiko pada SIAK UMMI adalah daftar prioritas risiko teknologi informasi mulai dari yang terkecil sampai yang terbesar atau sebaliknya. Hasil dari identifikasi aset yang akan dijadikan objek penelitian untuk manajemen risiko keamanan informasi pada SIAK UMMI disajikan pada tabel berikut

Tabel 3. Daftar Aset Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi

No	Kode Aset	Nama Aset
A : Aset Perangkat Keras dan Jaringan pada SIAK UMM		
1	A-001	Komputer server SIAK UMMI
2	A-002	Komputer klien (di perkantoran UMMI)
3	A-003	Perangkat keras jaringan komputer: Mikrotik atau router, Modem, Akses poin, Switch atau hub, Fiber Optik, Kabel UTP
B : Aset Perangkat Lunak pada SIAK UMMI		

4	B-001	Sistem operasi
5	B-002	Aplikasi SIAK UMMI
6	B-003	MySql (*Database management system)*
7	B-004	Web browser
8	B-005	Aplikasi Email UMMI
C : Aset Sumber Daya Manusia pada SIAK UMMI		
9	C-001	Pengelola SIAK UMMI
10	C-002	Pengguna Akhir SIAK UMMI
D : Aset Data dan Informasi yang berhubungan dengan SIAK UMMI		
11	D-001	Data akademik UMMI yang tercetak
12	D-002	Data akademik UMMI yang bersifat elektronik dan tersimpan di media penyimpanan komputer klien
13	D-003	Data akademik UMMI yang tersimpan pada basis data SIAK

b. Identifikasi Kemungkinan Risiko

Kemungkinan risiko setelah melakukan identifikasi aset terhadap SIAK UMMI, hal yang selanjutnya dilakukan yaitu identifikasi kemungkinan risiko untuk mengidentifikasi berbagai kemungkinan risiko yang muncul terhadap aset-aset SIAK UMMI yang terdiri dari berbagai faktor seperti alam atau lingkungan, manusia serta sistem dan infrastruktur

Tabel 4. Daftar Kemungkinan Risiko Pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi

Kode Resiko	**Kemungkinan Resiko**
E-001	Kebakaran
E-002	Gangguan koneksi internet
E-003	Menebak password
E-004	Registri error
E-005	Bruteforce login
E-006	Aplikasi basis data error
E-007	Adware ,malware, spyware
E-008	Spam
E-009	Kesalahan penggunaan perangkat lunak
E-010	Penyebaran informasi atau data rahasia dan penting
E-011	Dokumen Hilang
E-012	Korupsi data
E-013	Penyadapan

c. Identifikasi Risiko

Risiko setelah melakukan tahapan identifikasi kemungkinan risiko, langkah selanjutnya adalah melakukan identifikasi dampak risiko. Proses ini akan mengidentifikasi dampak seperti apa yang akan dialami oleh SIAK UMMI jika kemungkinan-kemungkinan yang sudah diidentifikasi sebelumnya terjadi

Tabel 5. Daftar Dampak Risiko Pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi

Kode Aset	Kemungkinan Resiko	Dampak Resiko
A-001	Kebakaran	Tidak hati-hati dalam penggunaan api di lingkungan UMMI
A-002	Gangguan koneksi internet	Koneksi internet di UMMI tidak stabil
A-003	Menebak password	Password untuk akses point terlalu mudah atau disebar sembarangan
B-001	Registry error	Kurangnya pemeliharaan sistem operasi pada komputer klien dan server di lingkungan UMMI secara berkala
B-002	Bruteforce login	Belum ada ketentuan batasan jika pengguna gagal login pada aplikasi SIAK UMMI
B-003	Aplikasi basis data error	Aplikasi basis data yang digunakan untuk SIAK UMMI tidak diperbarui
B-004	Adware, malware, spyware	Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI
B-005	Spam	Belum diterapkan filtering terhadap aplikasi Email UMMI
C-001	Kesalahan penggunaan perangkat lunak	Kurangnya pelatihan dalam penggunaan aplikasi SIAK UMMI
C-002	Penyebaran informasi atau data rahasia dan penting	Belum adanya kebjiakan tentang kerahasiaan data SIAK UMMI
D-001	Dokumen Hilang	Kebijakan penyimpanan dokumen tidak dilaksanakan dengan benar
D-002	Korupsi data	Tidak adanya perlindungan terhadap file SIAK UMMI yang tersimpan di komputer
D-003	Penyadapan	Tidak adanya perlindungan terhadap basis data SIAK UMMI

2. Analisis Risiko

Setelah melakukan tahap identifikasi risiko, tahap selanjutnya yaitu melakukan tahapan analisis risiko. Pada tahap ini dilakukan penilaian terhadap kemungkinan risiko pada tahap identifikasi risiko sebelumnya, dengan menggunakan tabel kriteria likelihood. Pada gambar 2 likelihood terdapat 3 kriteria yang berdasarkan frekuensi kejadian kemungkinan risiko terjadi. Setelah mendapatkan kriteria kemungkinan gambar 2 dan kriteria dampak gambar 3. Maka selanjutnya penilaian terhadap kemungkinan risiko berdasarkan gambar 2 dan 3. Selanjutnya penilaian likelihood dan impact pada tabel 6

Tabel 6. Penilaian Likelihood dan Impact

Kode Resiko	Kemungkinan Risiko	*Likelihood*	*Impact*
A-001	Kebakaran	1	5
A-002	Gangguan koneksi internet	3	4
A-003	Menebak password	2	2

B-001	Registry error	2	3
B-002	Bruteforce login	3	2
B-003	Aplikasi basis data error	3	3
B-004	Adware, malware, spyware	1	3
B-005	Spam	2	3
C-001	Kesalahan penggunaan perangkat lunak	3	3
C-002	Penyebaran informasi atau data rahasia dan penting	3	2
D-001	Dokumen Hilang	3	3
D-002	Korupsi data	2	3
D-003	Penyadapan	1	3

3. Evaluasi Risiko

Tahap terakhir dalam risk assessment adalah tahap evaluasi risiko. Dalam tahap ini menggunakan acuan berupa matriks risiko, dimana dalam matriks tersebut dibedakan kedalam 3 risk level yaitu low, medium dan high. Kemungkinan risiko yang telah ditentukan nilai likelihood dan nilai impact pada proses sebelumnya akan dibedakan lagi menyesuaikan matriks yang ada

Tabel 7. Matriks Evaluasi Risiko

LIKELIHOOD						
	Certain/ Pasti Terjadi (5)					
	Likely / Sering (4)					
	Possible / Kadang (3)		B-002 C-002	B-003	A-002 C-001 D-001	
	Unlikely / Jarang. (2)		A-003	B-001 B-005 D-002		
	Rare Hampir Tidak Pernah. (1)			B-004 D-003		A-001
		Insignificant / Sangat Kecil (1)	Minor / Kecil (2)	Moderate / Biasa (3)	Major / Besar(4)	Catastrophic / Sangat Besar (5)
IMPACT						

Setelah kemungkinan-kemungkinan risiko dimasukan ke dalam matriks evaluasi berdasarkan kemungkinan dan dampak, kemudian akan dijabarkan dari 13 kemungkinan risiko ke dalam level of risk dengan tingkatan high, medium dan low

Tabel 8. Risk Level Kemungkinan Risiko

Kode Resiko	Kemungkinan Risiko	*Likelihood*	*Impact*	Risk Level
A-002	Gangguan koneksi internet	*3*	*4*	Hight
C-001	Kesalahan penggunaan perangkat lunak	*3*	*3*	Hight
D-001	Dokumen Hilang	*3*	*3*	Hight
B-003	Aplikasi basis data error	*3*	*3*	Medium
B-001	Registry error	*2*	*3*	Medium
B-005	Spam	*2*	*3*	Medium

D-002	Korupsi data	*2*	*3*	Medium
A-001	Kebakaran	*1*	*5*	Medium
A-003	Menebak password	*2*	*2*	Low
B-002	Bruteforce login	*3*	*2*	Low
B-004	Adware, malware, spyware	*1*	*3*	Low
C-002	Penyebaran informasi atau data rahasia dan penting	*3*	*2*	Low
D-003	Penyadapan	*1*	*3*	Low

Pada tabel tersebut merupakan hasil dari risk evaluation dimana dari 13 kemungkinan risiko terdapat 3 (gagasan koneksi internet, kesalahan penggunaan perangkat lunak, dokumen hilang) merupakan level of risk dengan tingkatan high, terdapat risiko lainnya sejumlah 5 (aplikasi basis data error, registry error, spam, korupsi data, kebakaran) merupakan level of risk tingkatan medium, serta risiko berjumlah 5 (menebak password, bruteforce login, adware, malware, spyware, penyebaran informasi atau data rahasia dan penting, penyadapan) merupakan level of risk tingkatan low

4. Perlakuan Risiko

Setelah melakukan tahap identifikasi risiko, langkah selanjutnya yaitu perlakuan risiko. Pada tahap ini penulis memberikan sarana mengenai perlakuan risiko untuk kemungkinan risiko yang ada pada SIAK UMMI. Diharapkan dapat mengurangi dan digunakan untuk pencegahan terhadap kemungkinan risiko yang mungkin akan muncul

Tabel 9. Usulan Perlakuan Risiko

Kode Resiko	Kemungkinan Risiko	Risk Level	Perlakuan Risiko
A-002	Gangguan koneksi internet	Hight	Diperlukanya pengecekan jaringan secara berkala dan menambahkan router penguat sinyal agar sistem dapat diakses.
C-001	Kesalahan penggunaan perangkat lunak	Hight	Melakukan pelatihan terhadap karyawan dan melakukan pemetaan kemampuan masing-masing individu.
D-001	Dokumen Hilang	Hight	Untuk mencegah hal ini terjadi maka perlu memperbanyak tenaga security terlatih, Memperbanyak titik-titik pemasangan CCTV.
B-003	Aplikasi basis data error	Medium	Menyediakan antivirus, melakukan update dan monitoring software dan database antivirus
B-001	Registry error	Medium	Menyediakan antivirus, melakukan update dan monitoring software dan database antivirus
B-005	Spam	Medium	Membuat dan menjalankan SOP agar tahu lebih jelas peraturan di bidang kerjanya
D-002	Korupsi data	Medium	Untuk mencegah hal ini, pegawai harus melakukan proses penyimpanan data dengan baik.
A-001	Kebakaran	Medium	Tempatkan infrastruktur perangkat dan jaringan yang aman dan jauh dari kemungkinan kebakaran.
A-003	Menebak password	Low	Untuk mencegah risiko kesalahan teknis perlu melakukan pelatihan terhadap sumber daya manusia.

B-002	Bruteforce login	Low	Melakukan Pengecekan data secara berkala dan melakukan back up
B-004	Adware, malware, spyware	Low	Menyediakan cadangan hardware yang baru jika sewaktu waktu hardware memang tidak bisa digunakan lagi
C-002	Penyebaran informasi atau data rahasia dan penting	Low	Untuk meminimalisir hal ini maka perlu dilakukan teguran lisan, apabila masih melakukan kesalahan yang sama maka akan diberikan teguran secara tertulis
D-003	Penyadapan	Low	Untuk melindungi data dari penyadapan perlu dilakukan privasi data dengan perlindungan security software yang up to date, install software antivirus dan menggunakan fitur keamanan untuk website seperti layanan SSL/HTTPs.

5. Monitoring dan Review

   Hasil yang diperoleh dari proses monitoring dan review yaitu berupa kritik dan saran yang membangun dari pihak-pihak yang terlibat langsung dengan pengelolaan SIAK UMMI. Proses pelaksanaan manajemen risiko dikelola dan dimonitoring dengan baik. Seluruh proses kegiatan dilakukan oleh para pihak yang terlibat yaitu kepala pimpinan divisi dan karyawan serta semua pihak lain yang terkait baik internal maupun eksternal SIAK UMMI. Semua pihak yang terkait pelaksanaan proses monitoring dan review dilakukan dengan mengadakan pertemuan dan rapat berkala yang dilaksanakan guna mengkomunikasikan dan melaporkan terkait implementasi teknologi informasi termasuk kendala/kemungkinan risiko yang berpotensi menghambat proses bisnis perusahaan. Termasuk membahas bagaiamana melakukan penanganan dan pencegahan risiko yang uncul yang bertujuan untuk meminimalisir risiko di masa yang akan datang

SIMPULAN

Berdasarkan dari penelitian yang sudah dilakukan, analisis risiko teknologi informasi menggunakan ISO 31000 pada SIAK UMMI dijalankan dengan menggunakan tahapan-tahapan yang dimulai dari tahap komunikasi dan konsultasi, menentukan konteks, penilaian risiko, tahap analisis risiko, tahap evaluasi risiko, tahap perlakuan risiko serta monitoring dan review dan dari hasil analisis risiko yang telah dilakukan terdapat 13 kemungkinan risiko Dimana terdapat 3 (gangguan koneksi internet, kesalahan penggunaan perangkat lunak, dokumen hilang) merupakan level of risk dengan tingkatan high, terdapat risiko lainnya sejumlah 5 (aplikasi bisnis data error, registry error, spam, korupsi data, kebakaran) merupakan level of risk tingkatan medium, serta risiko berjumlah 5 (menebak password, bruteforce login, hardware, malware, spyware, penyebaran informasi atau data rahasia dan penting, penyadapan) merupakan level of risk tingkatan low

DAFTAR PUSTAKA

Nice, F., dan Imbar, R. (2016). Analisis risiko teknologi informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada website swifts menggunaakn ISO 31000. Jurnal JUISI. 2 (2), 1-11

R. Sarno and I. Iffano, Sistem Manajemen Keamanan Informasi Berbasis ISO 27001, Surabaya: ITSPress, 2009

Pramanda, R., Astuti, E., dan Azizah, D. (2018). Pengaruh kemudahan dan kemanfaatan penggunaan teknologi informasi terhadap kinerja karyawan. Jurnal Administrasi Bisnis. 39 (2), 117-126

Undang-Undang Nomor 9 Tahun 1969 tentang Penetapan Undang-Undang Nomor 1 Tahun 1969 tentang Bentuk-Bentuk Usaha Negara

Ajeng Retna Maharani (2018). Perancangan Manajemen Risiko Operasional Di Pt.X dengan Menggunakan Metode House of Risk. Tesis Pm-147501. Institut Teknologi Sepuluh Nopember

A.Saut and K.Surendro, "Perancangan Model Penilaian Kapabilitas Proses Manajemen Resiko Keamanan Informasi Menggunakan ISO 27005 dan ISO 33020 Studi Kasus: Pusat Komunikasi Kementerian Luar Negeri, "Seminar Nasional Teknologi Informasi, 2016, paper B.6, p.26"

Adan Standarisasi Nasional, Manajemen Risiko Keamanan Informasi (ISO/IE 27005:2011), Jakarta: BSN, 2013

M. P. Mokodompit and Nurlaela, "Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799 : 2000", Jurnal Sistem Informasi Bisnis, Vol. II, No. 2, pp. 94-104, 2016