ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

Analisis IT *Risk Management* di Universitas Bina Darma Menggunakan ISO31000

Yeni Erlika[1)], Muhammad Izman Herdiansyah[2)], A. Haidar Mirza[3)]

[1)2)3)]Program Pascasarjana Program Studi Magister Teknik Informatika, Fakultas Ilmu Komputer
Universitas Bina Darma Palembang
Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111
Email : yeni.erlika@student.binadarma.ac.id[1)], m.herdiansyah@binadarma.ac.id[2)], haidar.mirza@binadarma.ac.id[3)]

Abstract

The application of IT management needs to be evaluated to measure the level of IT risk management that occurs. This study aims to analyze and know the IT risk management process adopted at the University of Bina Darma Palembang using the ISO 31000 approach, and focus on evaluating IT management practices which include three stages; identification, analysis, and risk treatment. Bina Darma University is a university that has applied the use of information technology to support its business processes and in accordance with its vision and mission. The implementation of the entire system can be used to support the performance of employees, lecturers and to provide services to students, system managers namely the Directorate of Technology Systems, hereinafter referred to as DSTI. Risks that have occurred at the University of Bina Darma in terms of security standards for security, disaster recovery, to previously be able to cope with problems that occur, but there is no standard, manual, for example data backup using a hard disk. By using the risk assessment stage within the ISO 31000 framework, researchers found that Bina Darma University currently has not implemented ISO standards in dealing with their IT risk management. University management is in the process of designing to implement ISO. From interviews with IT staff and observations, researchers found that Bina Darma University had the ability to apply ISO 31000 in managing their risk. This research produces IT risk reports on current system applications.

Keywords : *IT Risk Management, ISO 31000, Assessment, Mitigation*

Abstrak

Penerapan manajemen IT perlu dilakukan evaluasi untuk mengukur tingkat penanganan risiko IT yang terjadi. Penelitian ini bertujuan untuk menganalisis dan mengetahui proses manajemen risiko IT yang diadopsi di Universitas Bina Darma Palembang menggunakan pendekatan ISO 31000, dan berfokus pada evaluasi praktik manajemen IT yang mencakup tiga tahapan; identifikasi, analisis, dan perlakuan risiko. Universitas Bina Darma merupakan perguruan tinggi yang telah mengaplikasikan penggunaan teknologi informasi sebagai pendukung proses bisnisnya dan sesuai dengan visi dan misi nya. Penerapan seluruh sistem yang ada dapat digunakan untuk mendukung kinerja pegawai, dosen maupun untuk layanan kepada mahasiswa/i, pengelola sistem yaitu Direktorat sistem teknologi selanjutnya di sebut dengan DSTI. Risiko yang pernah terjadi pada Universitas Bina Darma dari segi keamanan standart untuk keamanan, disaster recovery, untuk sebelumnya bisa menanggulangi masalah yang terjadi, tetapi tidak ada standarnya, manual, misal backup data dengan menggunakan hardisk. Dengan menggunakan tahap penilaian risiko dalam kerangka kerja ISO 31000, peneliti menemukan bahwa Universitas Bina Darma saat ini masih belum menerapkan standar ISO dalam menangani manajemen risiko IT mereka. Manajemen universitas sedang dalam proses perancangan untuk mengimplementasikan ISO. Hasil wawancara dengan staf IT dan pengamatan, peneliti menemukan bahwa Universitas Bina Darma memiliki kemampuan untuk menerapkan ISO 31000 dalam mengelola risiko mereka. Penelitian ini menghasilkan laporan risiko TI pada aplikasi sistem saat ini.

Kata kunci : *IT Risk Management, ISO 31000, Penilaian, Mitigasi*

1. Pendahuluan

Pengelolaan teknologi informasi, data yang kurang baik akan menimbulkan beberapa permasalahan yang merupakan kelemahan (*vulnerabilities*) sehingga akan menimbulkan ancaman (*threats*) dan dampak ketidakpastian pada pencapaian sasaran dan terjadi penyimpangan dari yang di harapkan baik positif maupun negatif (B.S ISO,2018). Risiko timbul dari proses yang tidak efektif dan tidak efisien, seperti hal yang dapat menggagalkan pencapaian tujuan dan menghabiskan biaya yang tidak sedikit, risiko dapat terjadi dari staff yang mengelola karena memiliki komptensi yang tidak memadai, bisa juga terjadi atas kerugian yang berhubungan erat dengan peristiwa-peristiwa tunggal yang tidak diharapkan akan tetapi berpotensi membawa dampak yang serius jika risiko tersebut benar-benar terjadi, misalnya kecurangan internal dan eksternal, kegagalan sistem, dan bencana alam (J. Lam, 2014) berdasarkan risiko yang terjadi, perlu adanya dilakukan pengelolalaan manajemen yang baik.

Cara membuat suatu pengelolaan manajemen risiko yang baik, proses identifikasi, penilaian dan prioritas risiko diikuti oleh aplikasi terkoordinasi dan ekonomis dari sumber daya untuk meminimalkan, memantau dan mengendalikan probabilitas serta dampak peristiwa yang tidak diinginkan dan mengembangkan strategi mitigasi, komunikasi risiko TI yang berpotensi menimbulkan dampak negative dan merugikan (A. M. Sucud et al., 2010) sehingga dapat memberikan pertimbangan kepada perguruan tinggi secara terstruktur dengan memperhatikan segala bentuk ketidak pastian dalam pengambilan keputusan dan tindakan yang harus diambil guna menangani risiko yang terjadi (M. H. Arief & Suprapto, 2018).

Risiko terjadi dapat melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal, baik itu risiko internal maupun risiko eksternal. Risiko internal seperti kegagalan sistem, kegagalan jaringan (*network*), kerusakan *hardware* dan *software*, kehilangan data, virus, untuk risiko eksternal terdapat pada gangguan alam seperti petir, banjir, hujan dan angin yang merusak infrastruktur TI sehingga menggungu kelangsungan proses bisnis pada perguruan tinggi. Pada dokumen ISO 31000, *International Standard Organization* (ISO) 31000 digunakan oleh orang-orang yang menciptakan dan melindungi nilai dalam organisasi dengan mengelola risiko, membuat keputusan, menetapkan dan mencapai tujuan dan meningkatkan kinerja (B.S ISO, 2018) Untuk meningkatkan kinerja, maka digunakan struktur ISO 31000, terdiri atas *principles risk management* yang membahas masalah tujuan dan sasaran manajemen risiko, *risk management framework* menetapkan mandat dan komitmen di tingkat management dan dewan senior, ini juga memerlukan deskripsi konteks organisasi internal dan eksternal, *risk management process* untuk menggambarkan penerapan manajemen risiko di tingkat unit bisnis untuk kegiatan sehari-hari penilaian risiko dan perlakuan risiko. Kelebihan ISO 31000:2018 terdiri dari kemudahan dalam menerapkan, lingkup penerapan lebih general, bukan untuk sertifikasi, dan telah diadopsi oleh banyak negara, maka dapat dikatakan, bahwa manajemen risiko merupakan unsur yang ikut menentukan keberhasilan penerapan *Good Corporate Governance* (GCG) di dalam suatu universitas (D. Ramdani, 2018).

Universitas merupakan salah satu instansi penyelenggaraan pelayanan publik, sebuah univeritas dituntut memberikan pelayanan terbaik untuk pihak yang membutuhkan informasi seperti mahasiswa, karyawan, ataupun pihak lainnya. Akan tetapi suatu universitas memiliki kesulitan tersendiri dalam memahami sudah sejauh mana standar untuk manajemen risiko di implementasikan, terlebih ketika perguruan tinggi mengimplementasikan lebih dari satu buah standar, hal ini di mungkinkan terjadi karena ruang lingkup atau fokus cakupan standar dirasa kurang luas untuk memenuhi cakupan manajemen. Dengan memiliki kontrol terhadap akses informasi organisasi dapat meminimalkan kerugian yang diakibatkan oleh hilangnya data yang disebabkan oleh penyalahgunaan akses, hal ini juga berlaku pada penerapan IT di Universitas Bina Darma (M. Gehrman, 2018).

Universitas Bina Darma merupakan perguruan tinggi yang telah mengaplikasikan penggunaan teknologi informasi sebagai pendukung proses bisnisnya dan sesuai dengan visi dan misi nya. Penerapan seluruh sistem yang ada dapat digunakan untuk mendukung kinerja pegawai, dosen maupun untuk layanan kepada mahasiswa/i, pengelola sistem yaitu Direktorat sistem teknologi selanjutnya di sebut dengan DSTI dan informasi dituntut memiliki kemampuan merancang dan mengelola sistem informasi dengan baik agar sistem informasi yang dikelola berkelanjutan dan senantiasa digunakan para pengguna. Pengelolaan sistem informasi yang tidak baik dapat berdampak pada rendahnya kualitas layanan sehingga hal tersebut dapat mempengaruhi kepercayaan user terhadap universitas dan menimbulkan risiko-risiko yang dapat merugikan perguruan tinggi.

Risiko yang pernah terjadi pada Universitas Bina Darma dari segi keamanan standart untuk keamanan, *disaster recovery*, untuk sebelumnya bisa menanggulangi masalah yang terjadi, tetapi tidak ada standarnya (legal) tidak menggunakan standar, manual, misal backup data dengan menggunakan hardisk. Di awal tahun 2018, terkena *ransome ware* karena keterlambatan dan kelalaian mengperbarui *windows server* dan pada saat itu *windows* belum menyediakan update untuk serangan *ransome ware*, pada saat itu sistem informasi akademik Universitas Bina Darma sekitar 3 jam tidak dapat akses, yang paling terkena dampak itu yaitu pelayanan akademik.

Berdasarkan latar belakang, dalam penelitian ini dibahas dan difokuskan untuk menganalisis dan implementasi IT *risk management* di perguruan tinggi menggunakan *Framework* ISO 31000 di Universitas Bina Darma Palembang.

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

A. Metodologi Penelitian

1. Desain Penelitian

Penelitian ini penulis menggunakan standar ISO 31000 sebagai desain penelitian untu melakukan penilaian risiko teknologi informasi pada management IT universitas bina darma yang dikelola oleh DSTI.

2. Metode Penentuan Informan

Teknik sampling adalah teknik pengambilan sampel untuk menentukan sampel dalam penelitian, peneliti menggunakan *purposive sampling*, dengan melakukan pengambilan sumber dengan pertimbangan tertentu misalnya orang tersebut yang dianggap paling tahu tentang apa yang diharapkan peneliti, atau mungkin sebagai penguasa sehingga memudahkan peneliti menjelajahi obyek/situasi risiko yang diteliti.

Pemilihan informan sebagai sumber data dalam penelitian ini adalah berdasarkan pada beberapa aspek, yaitu: menguasai permasalahan, memiliki data, dan bersedia memberikan informasi lengkap dan akurat, yang akan menjadi informan narasumber dalam penelitian ini adalah direktur DSTI, sub unit pengembangan sistem, sub unit teknologi informasi dan infrastruktur, sub unit layanan operasional IT (Sugiyono, 2016).

3. Metode Pengumpulan Data

Teknik yang digunakan dalam mengumpulkan informasi yang relevan dengan sistem IT dalam batas operasionalnya antara lain wawancara dengan personil dukungan sistem dan manajemen IT dapat memungkinkan personil penilaian risiko mengumpulkan informasi yang bermanfaat tentang sistem seperti bagaimana sistem di kelola dan di jalankan.

Langkah pertama yang dilakukan adalah wawancara kepada 4 orang informan. Berdasarkan struktur organisasi DSTI Universitas Bina Darma, Maka dalam penelitian ini ditentukan informan yang dianggap mengetahui semua tentang objek penelitian yaitu *software, hardware, brainware* yang ada di Universitas Bina Darma.

Kedua, menyebarkan kuesioner jenis pilihan atau checklist, jenis kuesioner yang stimulusnya berisikan pernyataan yang diharuskan di isi oleh informan (staff dan jajaran DSTI) dengan cara memilih satu diantara dua atau lebih pilihan informan terhadap pernyataan yang telah ditentukan untuk mempertegas hasil dari wawancara(Sugiyono, 2016).

4. Teknik Analisis Data

Dalam melakukan penelitian diperlukan suatu analisis data yang digunakan untuk menjawab pertanyaan dan permasalahan dalam penelitian. setelah data terkumpul dengan menggunakan metode pegumpulan data, maka peneliti mengolah dan menganalisis data dengan analisis secara kualitatif (B. Wijayantini, 2012) Jika analisis risiko sudah teridentifikasi probabilitas dan dampak dari suatu risiko, maka kita dapat mengukur potensi suatu risiko secara kualitatif dan risiko dapat diukur dengan skala 1 sampai dengan 5, yaitu:

Tabel 1. *Skala Risiko*

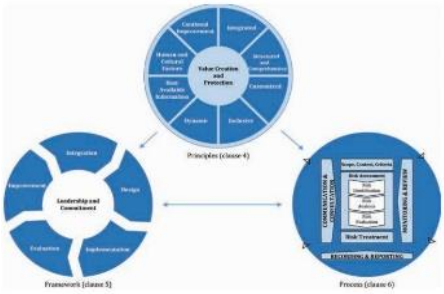
No	Keterangan	Skala
1	Sangat Besar	5
2	Besar	4
3	Sedang	3
4	Kecil	2
5	Sangat Kecil	1

Sumber: Wijayantini, 2012:61.

Pada tabel tersebut skala digunakan untuk menganalisis risiko dari dua kriteria, probabilitas yaitu seberapa sering risiko terjadi dan dampak yaitu seberapa besar dampak yang ditimbulkan jika risiko terjadi (Hery, 2016).

5. Kerangka Kerja

Framework ISO 31000 digunakan orang-orang yang menciptakan dan melindungi nilai dalam organisasi dengan mengelola risiko, membuat keputusan, menetapkan dan mencapai tujuan serta meningkatkan kinerja. ISO 31000 memiliki Prinsip manajemen risiko dalam penciptaan dan perlindungan nilai, meningkatkan kinerja, mendorong inovasi dan mendukung pencapaian tujuan. Kerangka Kerja manajemen risiko adalah untuk membantu organisasi dalam mengintegrasikan manajemen risiko ke dalam kegiatan dan fungsi yang signifikan. Proses manajemen risiko melibatkan penerapan kebijakan, prosedur, dan praktik yang sistematis untuk kegiatan berkomunikasi dan konsultasi, menetapkan konteks dan menilai, memperlakukan, memantau, meninjau, mencatat, dan melaporkan risiko. Berikut ini adalah komponen ISO 31000 yang digunakan:



Gambar 1. *Prinsip, kerangka kerja dan proses ISO 31000*

Standar ini dapat diterapkan sepanjang umur organisasi, dan untuk berbagai macam kegiatan, termasuk strategi dan keputusan, operasi, proses, fungsi, proyek, produk, layanan dan aset. Standar Internasional ini dapat diterapkan untuk semua jenis risiko, apa pun sifatnya, apakah positif atau konsekuensi negatif (B.S ISO, 2018).

2. Pembahasan

A. Analisis Kerangka Kerja ISO 31000

Berdasarkan hasil dari wawancara kepada pihak DSTI tentang risiko yang pernah terjadi dan hal apa saja yang dilakukan oleh pihak DSTI untuk menanggulangi

risiko tersebut, banyak cara yang dilakukan oleh pihak DSTI, DSTI adalah sebuah unit maka dari itu DSTI memiliki tim yang bekerjasama dalam menanggulangi kejadian tersebut, salah satunya dengan berdiskusi dengan tim dalam menentukan langkah selanjutnya untuk menanggulangi risiko.

Didalam kerangka kerja ISO 31000 kepemimpinan dan komitmen dalam direktur DSTI bertanggung jawab untuk mengelola dan mengawasi manajemen yang ada di DSTI dan memastikan bahwa manajemen risiko terintegrasi ke dalam semua kegiatan yang ada didalam Universitas Bina Darma Palembang.

Langkah pertama, dilihat dari kejadian risiko yang ada, ketika ada nya serangan terhadap sistem hal pertama yang dilakukan adalah berdiskusi, hal ini dilakukan oleh pihak DSTI yang memiliki tim untuk menyusun rencana apa yang akan di lakukan untuk mengatasi serangan yang terjadi. Berdasarkan ISO 31000 mengintegrasikan sebuah manajemen risiko bergantung pada pemahaman tentang struktur dan konteks Universitas Bina Darma Palembang. Struktur berbeda tergantung pada tujuan, sasaran, dan kompleksitas dari Universitas Bina Darma Palembang. Risiko dikelola di setiap bagian dari struktur Universitas Bina Darma Palembang.

Langkah kedua, memahami organisasi dan konteksnya Untuk saat ini DSTI akan menerapkan ISO 27001 untuk suatu standar sistem manajemen keamanan informasi (*information security management system*). Berdasarkan ISO 31000 ketika merancang kerangka kerja untuk mengelola risiko, Universitas Bina Darma Palembang harus memeriksa dan memahami konteks eksternal dan internalnya, mengartikulasikan komitmen manajemen risiko.

Latar belakang tujuan DSTI menerapkan ISO 27001 yaitu untuk melindungi, memelihara kerahasiaan, integritas, ketersediaan informasi, serta mampu mengelola dan mengendalikan risiko keamanan informasi pada perguruan tinggi. Menugaskan peran organisasi, otoritas, tanggung jawab, dan akuntabilitas, direktur DSTI memastikan bahwa otoritas, tanggung jawab, akuntabilitas untuk peran terkait sehubungan dengan manajemen risiko ditugaskan dan dikomunikasikan di semua tingkatan organisasi, serta harus menekankan bahwa manajemen risiko adalah tanggung jawab inti.

Mengalokasikan sumber daya, banyak cara yang dilakukan pihak DSTI untuk menanggulangi terjadi nya risiko, tim yang ada sangat berpengaruh dalam kejadian dan tim berdiskusi untuk melalukan tahapan selanjutnya agar tidak terjadi lagi serangan, dilihat dari kejadiaan yang ada. Didalam sisi ISO 31000 Direktur DSTI memastikan alokasi sumber daya yang tepat untuk tim dalam manajemen risiko, yang dapat mencakup, tetapi tidak terbatas pada orang, keterampilan, pengalaman dan kompetensi, proses, metode, dan alat organisasi. DSTI harus mempertimbangkan kemampuan yang dimiliki seperti staff yang sudah berkompetensi untuk menaggulangi risiko dan kendala dalam mengatasi risiko yang ada pada Universitas Bina Darma Palembang.

Membangun komunikasi dan konsultasi, didalam penerapan yang akan dilakukan pihak DSTI secara langsung di buat oleh pihak DSTI dan pihak DSTI mengajukan permohonan kepada pihak perguruan tinggi. Dalam melakukak pendekatan guna dapat membangun komunikasi dan konsultasi yang baik, Universitas Bina Darma Palembang harus menetapkan pendekatan yang disetujui agar mendukung kerangka kerja dan memfasilitasi penerapan manajemen risiko yang efektif..
Langkah ketiga, pelaksanaan / implementasi, untuk saat ini ISO yang yang di rencanakan masih dalam tahap perancangan, untuk keseluruhan tahapannya sudah di laksanakan hanya saja untuk tahap sertifikasinya belum terlaksana, dan menurut ISO 31000 Universitas Bina Darma Palembang harus mengimplementasikan kerangka kerja manajemen risiko dengan mengembangkan rencana yang sesuai termasuk waktu dan sumber daya, mengidentifikasi di mana, kapan dan bagaimana berbagai jenis keputusan dibuat di seluruh Universitas Bina Darma Palembang dan memastikan bahwa pengaturan Universitas Bina Darma Palembang untuk mengelola risiko dipahami dengan jelas dan dipraktikkan.

Langkah ke empat evaluasi, sejauh dalam penerapan ISO yang ada untuk saat ini masih terkendala biaya karena biaya sertifikasi sangat mahal, tetapi untuk saat ini semua kegiatan sudah mengarah ke ISO 27001 dan pada saat penerapan ini pihak DSTI harusnya selalu mengevaluasi disetiap manajemen penerapan yang ada. Menurut ISO 31000 Untuk mengevaluasi efektivitas kerangka kerja manajemen risiko. Universitas Bina Darma Palembang harus secara berkala mengukur kinerja kerangka kerja manajemen risiko terhadap tujuannya,implementasi rencana, indikator, dan perilaku yang diharapkan menentukan apakah tetap cocok untuk mendukung pencapaian tujuan Universitas Bina Darma Palembang.

Langkah kelima perbaikan / peningkatan, menyesuaikan kondisi untuk menanggulagi terjadinya risiko dengan menerapakan ISO 27001 pihak DSTI harus terus memantau dan mengadaptasi kerangka kerja manajemen risiko untuk mengatasi perubahan eksternal dan internal. Dengan demikian, Universitas Bina Darma Palembang dapat meningkatkan nilainya. Terus meningkatkan penerapan ISO 27001, DSTI harus terus meningkatkan kesesuaian, kecukupan, dan efektivitas kerangka kerja manajemen risiko dan cara proses manajemen risiko terintegrasi. Ketika celah yang relevan atau peluang peningkatan diidentifikasi, organisasi harus mengembangkan rencana dan menugaskan mereka yang bertanggung jawab untuk implementasi. Setelah di implementasikan, perbaikan ini harus berkontribusi pada peningkatan manajemen risiko.

Dari beberapa penjabaran sebelumnya bahwa DSTI saat ini baru akan menerapkan ISO 27001 untuk suatu standar sistem manajemen keamanan informasi (*information security management system*). ISO 27001 sudah dalam tahap perancangan secara keseluruhan sudah diterapkan tetapi untuk sertifikasi yang saat ini belum di lakukan.

B. Hasil Identifikasi Risiko

Proses identifikasi risiko dilakukan dengan menggunakan checklist dan wawancara. Adapun hasil dari identifikasi risiko ini diklasifikasikan ke dalam 3 ruang lingkup risiko yang diteliti, yaitu :

Tabel 2. *Distribusi jawaban informan dalam identifikasi Risiko*

No	Risiko Proses	Ya	Tidak
1	Pelayanan pengguna sistem (P1)	11	0
2	Perangkapan tugas (P2)	4	7
3	Prosedur kerja DSTI (SOP) (P3)	11	0
4	Data *corrupt* (P4)	11	0
5	Kegagalan *backup / generate* data (P5)	11	0
6	Kegagalan proses pemeliharaan dan *continue development* (P6)	11	0
7	*Web service* mati tiba-tiba (P7)	11	0
8	*Hacking* terhadap jaringan (P8)	11	0
9	Serangan virus (P9)	11	0
	Risiko SDM		
10	Kompetensi dan keahlian (SDM1)	1	10
11	Integritas (SDM2)	1	10
12	Perputaran kerja (SDM3)	0	11
13	Budaya organisasi (SDM4)	2	9
14	Konflik kepentingan (SDM5)	0	11
15	Perekrutan karyawan (SDM6)	0	11
	Risiko Insidental		
16	Listrik (I1)	11	0
17	Kebakaran (I2)	11	0
18	Gempa bumi (I3)	11	0
19	Banjir (I4)	11	0
20	Pencurian atau teror (I5)	11	0

Sumber: Data Primer Diolah, 2019.

Data pada tabel 2 pada risiko proses bahwa hampir semua risiko proses diidentifikasi atau diketahui oleh informan. Disetiap jenis risiko ada beberapa pendapat informan yang tidak berpengaruh kepada risiko, seperti Risiko jenis ke-2 perangkapan tugas, hal ini tidak berpengaruh kepada risiko karena setiap staff sudah memiliki tugas masing-masing.

Pada risiko SDM dari beberapa risiko cenderung tidak terlalu mempengaruhi dalam terjadinya risiko karena sebagian besar hal tersebut sudah di atasi oleh pihak DSTI.

Pada risiko Insidental dari beberapa risiko hal tersebut bisa saja terjadi karena dapat mempengaruhi risiko yang terjadi seperti listrik berhenti saat ada kegiatan (padam), terkadang dapat menyebabkan kebakaran karena aliran listrik yang bermasalah atau karena kelalaian karyawan atau pengguna sistem sehingga menyebabkan kebakaran, peristiwa alam juga dapat mempengaruhi risiko seperti gempa bumi dan banjir hal ini mengharuskan suatu instansi untuk melakukan back up data, hal lain juga dapat terjadi seperti pencurian atau terror dari pihak luar, pihak luar mengancam untuk mencuri aset perguruan tinggi.

Dari hasil identifikasi peneliti memahami potensi risiko yang terjadi, risiko dapat terjadi akibat interaksi antara sistem yang digunakan dengan pengguna, dimana masing-masing pihak memiliki kepentingan yang berbeda-beda. Hal ini akan menghasilkan daftar potensi risiko dan peluang.

C. Hasil Analisis Risiko

Risiko yang telah di identifikasi selanjutnya akan dianalisis dalam dua kriteria, yakni kriteria probabilitas (seberapa sering risiko tersebut akan timbul) dan kriteria dampak (seberapa besar konsekuensi yang akan ditimbulkan jika risiko tersebut terjadi). Tabel 3 dan 4 menyajikan jenis risiko yang telah diidentifikasi, probabilitas dan dampak dari masing-masing jenis risiko, serta jumlah informan yang melakukan analisis risiko.

Tabel 3. *Analisis Probabilitas*

No	Risiko Proses	Probabilitas	Level Risiko
1	Pelayanan pengguna sistem (P1)	3	Sedang
2	Perangkapan tugas (P2)	1	Rendah
3	Prosedur kerja DSTI (SOP) (P3)	3	Sedang
4	Data *corrupt* (P4)	3	Sedang
5	Kegagalan *backup / generate* data (P5)	3	Sedang
6	Kegagalan proses pemeliharaan dan *continue development* (P6)	2	Rendah
7	*Web service* mati tiba-tiba (P7)	3	Sedang
8	*Hacking* terhadap jaringan (P8)	4	Tinggi
9	Serangan virus (P9)	3	Sedang
	Rata-rata	3	Sedang
	Risiko SDM		
10	Kompetensi dan keahlian (SDM1)	1	Rendah
11	Integritas (SDM2)	1	Rendah
12	Perputaran kerja (SDM3)	1	Rendah
13	Budaya organisasi (SDM4)	1	Rendah
14	Konflik kepentingan (SDM5)	2	Rendah
15	Perekrutan karyawan (SDM6)	1	Rendah
	Rata-rata	1	Rendah
	Risiko Insidental		
16	Listrik (I1)	3	Sedang
17	Kebakaran (I2)	4	Tinggi
18	Gempa bumi (I3)	3	Sedang
19	Banjir (I4)	3	Sedang
20	Pencurian atau teror (I5)	4	Tinggi
	Rata-rata	3	Sedang

Sumber: Data Primer Diolah, 2019.

Disetiap macam-macam risiko yang ada pada risiko probabilitas bahwa dari beberapa jenis risiko yang terjadi bahwa kemungkinan risiko yang ada bisa saja terjadi, tetapi bisa juga tidak terjadinya risiko karena jika ada kelalaian dalam bekerja dapat meninmbulkan risiko yang sebenarnya jika tidak lalai dan memonitoring secara berkala maka tidak akan terjadi risiko.

Dari hasil probobabilitas risiko yang ada untuk pengendalian risiko yang memiliki ancaman cukup tinggi, penanganan risiko dapat melalui pemantauan

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

khusus dan spesifik atau dapat melalui prosedur yang tanggap yang telah di tetapkan sehingga risiko dapat segera diatasi dan tidak menimbulkan risiko yang baru. Berikut ini adalah analisis dampak risiko yang terjadi :

Tabel 4. *Analisis Dampak Risiko*

No	Risiko Proses	Dampak	Level Risiko
1	Pelayanan pengguna sistem (P1)	3	Sedang
2	Perangkapan tugas (P2)	1	Rendah
3	Prosedur kerja DSTI (SOP) (P3)	3	Sedang
4	Data *corrupt* (P4)	3	Sedang
5	Kegagalan *backup / generate* data (P5)	3	Sedang
6	Kegagalan proses pemeliharaan dan *continue development* (P6)	3	Sedang
7	*Web service* mati tiba-tiba (P7)	2	Rendah
8	*Hacking* terhadap jaringan (P8)	2	Rendah
9	Serangan virus (P9)	2	Rendah
	Rata-rata	3	Sedang
	Risiko SDM		
10	Kompetensi dan keahlian (SDM1)	1	Rendah
11	Integritas (SDM2)	1	Rendah
12	Perputaran kerja (SDM3)	1	Rendah
13	Budaya organisasi (SDM4)	1	Rendah
14	Konflik kepentingan (SDM5)	1	Rendah
15	Perekrutan karyawan (SDM6)	1	Rendah
	Rata-rata	1	Rendah
	Risiko Insidental		
16	Listrik (I1)	3	Sedang
17	Kebakaran (I2)	3	Sedang
18	Gempa bumi (I3)	3	Sedang
19	Banjir (I4)	3	Sedang
20	Pencurian atau teror (I5)	3	Sedang
	Rata-rata	3	Sedang

Sumber: Data Primer Diolah, 2019.

Pada tabel 4 dampak kemungkinan terjadinya risiko dalam level masih dalam tingkat wajar dengan tindakan perbaikan dilakukan sesuai periode waktu yang direncanakan dan masih perlu dilakukan perbaikan karena risiko yang terjadi masih dapat di toleransi.

Dari hasil analisis dampak, risiko yang timbul karena listrik berhenti beroperasi (paham), aliran listrik yang bermasalah atau karena kelalaian pengguna sistem sehingga menyebabkan kebarakan. Risiko yang timbul karena peristiwa alam seperti gempa bumi dan banjir, risiko yang timbul karena adanya ancaman dari luar untuk mencuri asset perusahan. Berdasarkan studi literatur (N. Djauhari, 2014) untuk daerah Palembang masih aman dari gempa bumi namun kewaspadaan akan terjadi bencana harus selalu ditingkatkan. Dan untuk terjadi nya banjir untuk wilayah Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111 berdasarkan studi literatur dan pengamatan tidak berpotensi banjir walaupun terjadi hujan yang besar karena dilihat dari kondisi fisik gedung sudah tinggi dan aman dari banjir.

D. Evaluasi Risiko

Proses evaluasi akan membantu mementukan risiko-risiko mana yang memerlukan atas risiko yang ada. Proses evaluasi risiko ini dilakukan dengan menggunakan metode evaluasi kualitatif, yakni dengan menggunakan matriks kemungkinan dan dampak (probability impact matrix). Matriks ini membantu menunjukan risiko-risiko operasional mana saja yang masuk dalam zona merah (risiko tinggi), zona kuning (risiko menengah), dan zona hijau (risiko rendah) yang selanjutnya akan diberikan treatment oleh para Informan, berikut ini adalah hasil evaluasi dari jenis-jenis risiko.

Gambar 2. *Matriks level risiko proses*

Gambar 3. *Matriks level risiko SDM*

Gambar 4. *Matriks level risiko insidental*

Masukan bagi para informan untuk mengambil keputusan dalam menangani risiko-risiko operasional yang diteliti, yakni:

1. Zona merah (Risiko Tinggi)

Perhatian dan dukungan dari manajemen puncak diperlukan. Rencana, tindakan, dan akuntabilitas perlakuan risiko harus jelas dan terukur. Pelaksanaannya pun harus segera.

2. Zona kuning (Risiko Sedang)

Penanganan melalui pemantauan khusus dan spesifik atau melalui prosedur tanggap yang telah ditetapkan. Akuntabilitas biasanya terletak pada manajemen operasional dan harus ditetapkan secara jelas.

3. Zona hijau (Risiko Rendah)

Penanganan cukup dengan prosedur rutin dan tidak perlu menggunakan sumber daya yang spesifik.

E. Perlakuan Risiko

Sebuah proses yang berulang, mulai dari asesmen terhadap sebuah perlakuan risiko sampai memperkirakan

apakah tingkat risiko yang tersisa dapat diterima atau tidak bila perlakuan tersebut diterapkan. Ada 4 jenis perlakuan risiko yaitu berbagi, menghindari, mengurangi, dan menerima risiko, pada tabel 5 menjelaskan hasil dari perlakuan risiko.

Tabel 5. *Perlakuan Risiko*

No	Risiko Proses	Perlakuan Risiko
1	Pelayanan pengguna sistem	Mitigasi : 1. Mengadakan briefing setiap 1 minggu sekali atau lebih. 2. Mengadakan evaluasi bulanan. 3. Menggunakan pendekatan personal kepada staff. 4. Memantau kinerja staff
2	Perangkapan tugas	Berbagi: 1. Bekerja Bersama tim. 2. Menanggung risiko Bersama-sama. 3. Diskusi tentang langkah yang akan di ambil untuk memperbaiki risiko. 4. Risiko perangkapan tugas tidak akan menimbulkan dampak yang signifikan.
3	Prosedur kerja DSTI (SOP)	Mitigasi: 1. Mengadakan evaluasi 2. Memberikan motivasi, nasehat, teguran, atau sanksi kepada karyawan yang melanggar SOP. 3. Membagikan sejumlah checklist kepada staff (*checklist* berisi pekerjaan-pekerjaan yang harus diselesaikan oleh masing-masing staff)
4	Data *corrupt*	Mitigasi: 1. Menjalankan program deteksi virus 2. Mengisolasi asal masalah dan memperbaikinya. 3. Pencadangan data di tempat lain.
5	Kegagalan *backup / generate* data	Mitigasi : 1. Menerapkan konsep replikasi 2. Menerapkan konsep backup
6	Kegagalan proses pemeliharaan dan *continue development*	Berbagi: 1. Menyelesaikan masalah dengan berdiskusi Bersama tim untuk menyelesaikan kegagalan.
7	*Web service* mati tiba-tiba	Berbagi: 1. Bekerja Bersama tim. 2. Menanggung risiko Bersama-sama. *3. Update*
8	*Hacking* terhadap jaringan	Berbagi: 1. Berdiskusi Bersama tim 2. Merekrut pihak yang berkopeten di bidang hacking terhadap jaringan.
9	Serangan virus	Berbagi: 1. Berdiskusi Bersama tim 2. *Update* sistem
	Risiko SDM	
10	Kompetensi dan keahlian	Mitigasi: 1. Mengadakan traning kepada staff 2. Melakukan rolling staff 3. Memperketat sistem perekrutan staff 4. Melakukan pelatihan.
11	Integritas	Berbagi: 1. Melakukan evaluasi dengan berdiskusi minimal 1 minggu sekali. 2. Memasang cctv di ruangan kerja.
12	Perputaran kerja	Mitigasi: 1. Mengadakan evaluasi bulanan. 2. Menjaga relasi antar staff, pimpinan.
13	Budaya organisasi	Mitigasi: 1. Mengadakan evaluasi secara rutin 2. Memperketat sistem perekrutan staff.
14	Konflik kepentingan	Mitigasi: 1. Melakukan negoisasi dengan staff yang bersangkutan
15	Perekrutan karyawan	Mitigasi : 1. Menerapkan desain kerja yang fleksibel.
	Risiko Insidental	
1	Listrik	Mitigasi: 1. Menyediakan genset 2. Meng update informasi pemadaman listrik melalui media sosial.
2	Kebakaran	Mitigasi: 1. Menyediakan APAR (Alat Pemadam Api Ringam) 2. Melakukan pengecekan secara rutin terhadap alat-alat yang terhubung langsung dengan api dan aliran listrik.
3	Gempa bumi	Mitigasi: Berkomunikasi dengan rekan yang bekerja di BASARNAS (Badan SAR Nasional)
4	Banjir	Mitigasi: Membuat resapan air di

		sekitar lokasi institusi.
5	Pencurian atau teror	Mittigasi: 1. Memasangan CCTV 2. Menjalin relasi sosial dengan masyarakat. Cara ini dapat membantu untuk mengantisipasi risiko pencurian atau teror melalui aktivitas ronda malam yang rutin dilakukan oleh masyarakat.

Sumber: Data Primer Diolah, 2019.

Berdasarkan data yang disajikan pada tabel 5 dapat diketahui bahwa secara keseluruhan risiko-risiko operasional yang diteliti ditangani oleh informan dengan 2 opsi perlakuan risiko, yaitu: opsi berbagi, dan mitigasi.

Tabel 6. *Distribusi jumlah perlakuan risiko*

No	Perlakuan Risiko	Risiko Operasional			Jumlah (%)
		P	S	I	
1	Berbagi	5	1	-	6 (30%)
2	Mitigasi	4	5	5	14(70%)
	Jumlah	9	6	5	

Sumber: Data primer diolah, 2019.

Dari kedua opsi perlakuan pada tabel 6 dapat diketahui bahwa opsi mitigasi merupakan opsi perlakuan risiko yang memiliki jumlah pernyataan terbanyak, yakni sebanyak 14 pernyataan (70%). Opsi tersebut dinilai manajemen mengelola risiko dengan membuat prosedur dan pengawasan internal, pelatihan atau sosialiasi internal.

Selanjutnya, sebanyak 6 pernyataan (30%) dijawab oleh infrorman dengan jawaban berbagi, opsi tersebut dipilih karena para informan saat ini belum menemukan opsi perlakuan risiko yang paling tepat, opsi tersebut diyakini Akan memberikan manfaat yang akan menyeimbangi bahkan pihak manajemen dapat mengelola risiko lain dengan bersekutu dengan pihak lain melalui joint venture dan joint financing dalam rangka menanggung risiko bersama-sama.

3. Kesimpulan

Dari penelitian ini dapat dinyatakan bahwa, setelah dilakukan analisis risiko diketahui bahwa kecil kemungkinan terjadi. Secara keseluruhan risiko yang terjadi yaitu berada pada skala 2 dan berdasarkan matriks level masih berada pada zona hijau yang artinya penanganan risiko cukup dengan prosedur rutin saja, tidak perlu menggunakan sumber daya yang spesifik.

Kondisi ini dapat ditindak lanjuti bahwa seharusnya suatu perguruan tinggi perlu mengadopsi standar atau ISO untuk menangani risiko-risiko yang terjadi, karena sesuai dengan kemajuan teknologi yang ada yaitu era pendidikan 4.0 maka suatu perguruan tinggi wajib menerapkan standar manajemen IT yang ada agar tidak mengalami kesulitan dalam menangani risiko yang terjadi.

Daftar Pustaka

B. S. Institution. 2018. *International Organization for Standardization / IEC 31000.* Switzerland.

J. Lam. 2014. *Enterprise risk management: form incentives to controls, second ed.* United States Of America: John Wiley & Sons, Inc., Hoboken, new jersey.

A. M. Sucud, M. Bizoi and F. G. Filip. 2010. *Audit for Information Systems Security.* Information Economica: 43-48.

M. H. Arief and Suprapto. 2018. *Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang.* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer :101-110.

D. Ramdani. 2018. *Peta dan tata kelola TIK institusi pemerintah.*Yogyakarta: Diandra Kreatif.

N. Djauhari. 2014. *Pengantar mitigasi bencana geologi*. Yogyakarta: Deepublish.

M. Gehrmann. 2018. *Combining ITIL, COBIT andISO/IEC 27002 for structuringcomprehensive informationtechnology for management inorganizations.* Navus – Revista de Gestão e Tecnologia, Frianópolis: 66-77.

Sugiyono. 2016. *Metode penelitian kuantitatif dan kualitatif dan R & D.* Bandung: Alfabeta.

B. Wijayantini. 2012. *Model pendekatan manajemen risiko*. JEAM: 57-64.

Hery. *Manajemen bisnis terintegrasi*, Jakarta: PT. Gramedia Widiasarana Indonesia.