

ANALISIS IT RISK MANAGEMENT PADA PERGURUAN TINGGI MENGUNAKAN ISO 31000 (STUDI KASUS UNIVERSITAS MA CHUNG)

Gregorius Allan ¹⁾, Yudhi Kurniawan ²⁾, Rudy Setiawan ³⁾

1) *Sistem Informasi Universitas Ma Chung, Villa Puncak Tidar N-1 Malang*
email : 321810006@student.machung.ac.id¹⁾, yudhi.kurniawan@machung.ac.id²⁾, rudy.setiawan@machung.ac.id³⁾

Abstrak

Dalam meningkatkan kinerja universitas dalam memberikan jasa dan layanan, Universitas Ma Chung memanfaatkan infrastruktur IT dan sistem informasi yang dapat menunjang keberlangsungan proses bisnisnya. Terdapat kemungkinan risiko yang dapat mengancam keberlangsungan proses bisnis. Universitas Ma Chung masih belum menerapkan standard dalam menangani manajemen risiko IT pada Universitas Ma Chung, hal ini menyebabkan adanya ketidakpastian terutama dalam menyikapi risiko terhadap aset pada Universitas Ma Chung. Dengan menggunakan standar yang telah diadopsi oleh Badan Standardisasi Nasional (BSN) yaitu ISO 31000 yang dapat diimplementasikan untuk organisasi yang dinamis dan fleksibel sehingga, standar ini bisa digunakan untuk melakukan penilaian terhadap risiko dan respon terhadap risiko. Tujuan dari penulisan dokumen tugas akhir ini adalah untuk mengidentifikasi dan menganalisis risiko serta melakukan pengurangan dampak terhadap risiko pada Teknologi Informasi Universitas Ma Chung menjadi mekanisme peningkatan berkelanjutan perusahaan dalam menghadapi risiko. Dibuatnya kebijakan untuk melakukan pemantauan dan meninjau manajemen risiko.

Kata Kunci :

Manajemen risiko, Universitas, Risiko, ISO 31000

Abstract

In improving university performance in providing services and services, Ma Chung University utilizes IT infrastructure and information systems that can support the sustainability of its business processes. There are possible risks that can threaten the sustainability of business processes. Ma Chung University still has not implemented standards in dealing with IT risk management at Ma Chung University, this causes uncertainty, especially in addressing risks to assets at Ma Chung University. By using the standard that has been adopted by the National Standardization Agency (BSN), namely ISO 31000 which can be implemented for dynamic and flexible organizations so that this standard can be used to conduct risk assessments and responses to risks. The purpose of writing this final project document is to identify and analyze risks and to reduce the impact of risks on Information Technology at Ma Chung University as a mechanism for continuous improvement of companies in facing risks. Established a policy to monitor and review risk management.

Keywords :

Risk Management, University, Risk, ISO 31000

1. PENDAHULUAN

Saat ini Teknologi Informasi (IT) pada Universitas Ma Chung dikelola oleh sebuah badan yakni UPT Sistem Informasi Universitas Ma Chung (UPT SI). UPT SI merupakan salah satu bidang yang membantu Universitas Ma Chung dalam mengimplementasikan program dan megaton yang menunjang pembelajaran dan pelayanan.

Dalam meningkatkan kinerja universitas dalam beroperasi, Universitas Ma Chung memanfaatkan infrastruktur IT dan sistem informasi yang dapat menunjang keberlangsungan proses bisnisnya. Terdapat kemungkinan risiko yang dapat mengancam keberlangsungan proses bisnis. Penggunaan asset IT harus diikuti dengan kebijakan dan perlakuan yang tepat

dan sesuai sehingga mampu meminimalisir risiko-risiko yang mungkin terjadi didalam proses bisnisnya.

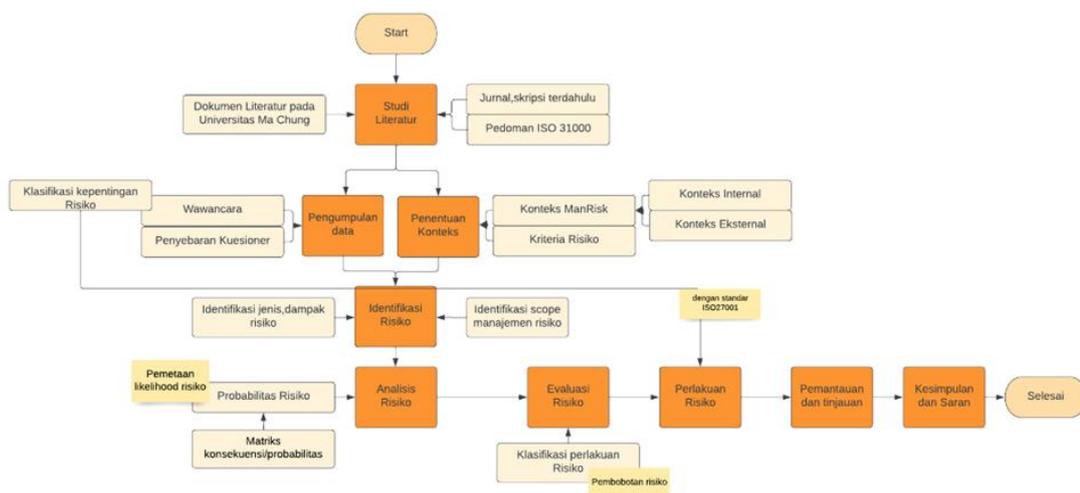
Proses menganalisa serta memperkirakan timbulnya suatu risiko dalam suatu kegiatan disebut sebagai manajemen risiko. Perlunya melakukan suatu tindakan pencegahan untuk memastikan kelangsungan proses bisnis dalam organisasi tetap berjalan dengan meminimalisasi risiko yang akan ataupun sudah terjadi. Dengan adanya manajemen risiko dapat mengetahui risiko apa yang dapat diprioritaskan dalam penanganan bagi pihak Universitas Ma Chung.

Universitas Ma Chung masih belum menerapkan standard dalam menangani manajemen risiko IT pada Universitas Ma Chung, hal ini menyebabkan adanya ketidakpastian terutama dalam menyikapi risiko terhadap aset pada Universitas Ma Chung, dibutuhkan penyikapan terhadap risiko secara tertulis sebagai panduan dan pedoman dalam menyikapi risiko.

Oleh karena itu, penerapan manajemen risiko berkaitan dengan teknologi informasi dalam pelaksanaan proses bisnis di Universitas Ma Chung merupakan hal yang sangat krusial. Dengan menggunakan standar yang telah diadopsi oleh Badan Standarisasi Nasional (BSN) yaitu ISO 31000 yang dapat diimplementasikan untuk organisasi yang dinamis dan fleksibel sehingga, standar ini bisa digunakan untuk melakukan penilaian terhadap risiko dan respon terhadap risiko. Pemetaan yang menyeluruh terhadap risiko-risiko teknologi informasi dapat dijadikan landasan untuk merumuskan kebijakan dalam rangka mencegah kegagalan layanan teknologi informasi dalam proses bisnis di Universitas Ma Chung serta memberikan respon yang digunakan untuk perbaikan pengelolaannya pada masa yang akan datang.

2. METODE / ALGORITMA

Bagian ini memuat penjelasan secara lengkap Pada tahapan ini, akan membahas tentang ahapan yang digunakan untuk Menyusun dokumen manajemen risiko. Ada 8 tahapan utama dalam penyusunan laporan yakni :



Gambar 1 Alur/ Tahapan penelitian

2.1 Studi Literatur

Melakukan pengumpulan literasi *E-book* tentang pengelolaan risiko menggunakan ISO 31000 seperti skripsi yang sudah ada, jurnal, dan karya ilmiah lainyadan melakukan studi banding antara penelitian terdahulu dan penelitian yang akan dilakukan.

2.2 Pengumpulan Data

Melakukan tanya jawab pada pihak yang berwenang di UPT SI, selaku badan yang mengelola IS/TI di Universitas Ma Chung. Terutama *scope* UPT SI dalam mengelola SI/TI di Universitas Ma Chung

2.3 Identifikasi Risiko

Tahapan identifikasi risiko bertujuan untuk mengidentifikasi risiko yang harus dikelola organisasi melalui proses yang sistematis dan terstruktur [1]. Proses identifikasi risiko menghasilkan suatu daftar peristiwa risiko yang dilengkapi informasi pendukung seperti dampak risiko dan jenis risiko yang dikenal dengan nama register risiko (*risk register*), adalah suatu daftar yang memuat risiko-risiko yang dihadapi oleh asset [2].

1) Identifikasi Aset Kritis

Melakukan pengumpulan data pada asset Universitas Ma Chung terutama yang berhubungan dengan IT/IS. Universitas Ma chung merupakan sebuah perguruan tinggi, dimana proses bisnis utama yakni kegiatan akademik/tridharma. Pada area akademik merupakan area *business process core* dari Universitas. Identifikasi aset kritis melibatkan keterkaitan unit kerja yang digunakan oleh bagian keuangan mahasiswa.

2) Identifikasi Risiko dari Aset Kritis

Dari asset kritis yang dipilih, diidentifikasi ancaman risiko yang dapat terjadi dan mengganggu keberlangsungan proses bisnis utama Universitas Ma Chung. Ancaman risiko yang telah diidentifikasi lalu dikelompokkan berdasarkan jenisnya. Berdasarkan jenisnya, ancaman dibedakan menjadi 5, yakni: Risiko Personil, Risiko Infrastruktur, Risiko Sistem Informasi, Risiko Jaringan, dan Risiko *Policy*

3) Identifikasi Dampak Risiko dari Aset Kritis

Setelah melakukan tahapan identifikasi kemungkinan risiko, langkah selanjutnya adalah melakukan identifikasi dampak dari risiko. Proses ini akan mengidentifikasi dampak dan kerugian yang akan dialami oleh Universitas Ma Chung jika kemungkinan risiko yang sudah diidentifikasi sebelumnya terjadi.

2.4 Analisa Risiko

Setelah melakukan pengidentifikasian risiko pada setiap IT/IS, dilakukannya analisa terhadap risiko yang telah diidentifikasi. Risiko akan dianalisis guna mengetahui risiko mana yang dominan terjadi berdasarkan frekuensi terjadinya dan kemudian tingkat kebesaran dampak (*impact*) dari risiko atau tingkat risiko akan dibandingkan menggunakan matriks analisis risiko [3]. Metode analisis yang digunakan dalam adalah menggunakan analisis kualitatif dikarenakan analisis ini cepat dan relatif mudah digunakan untuk menjangkau identifikasi dampak (*impact*) beserta kemungkinan (*likelihood*) yang luas sehingga dapat digunakan sebagai bahan evaluasi penilaian dari risiko[4].

Untuk menentukan prioritas atas tindakan respons yang lebih jauh dengan pengukuran dan pengkombinasikan probabilitas terjadinya risiko beserta dampak dari risiko tersebut. Dibuatlah indikator dampak dan *likelihood* risiko sebagai acuan dalam menganalisa risiko[2].

2.5 Evaluasi Risiko

Pada tahapan evaluasi resiko, data yang telah dinilai dari pengumpulan data pada tahap sebelumnya seperti seringnya terjadi risiko serta dampak yang dihasilkan dari setiap risiko akan diolah. Sehingga pada tahap ini akan menghasilkan peringkat risiko yang terjadi pada IT/IS pada UPT SI Universitas Ma Chung untuk penentuan prioritas dalam menangani dan melakukan mitigasi pada risiko.

Tabel 2 Kriteria risiko

Risiko tinggi (17-20)	Risiko yang berbahaya dan harus ditangani secepatnya
Risiko sedang (12-16)	Risiko yang harus diwaspadai dan membutuhkan penanganan yang berkelanjutan
Risiko Rendah (1-11)	Risiko yang dapat ditangani dengan menggunakan kebijakan dan peraturan tertentu

2.6 Perlakuan Risiko

Pada tahapan evaluasi resiko, risiko yang telah diidentifikasi dalam *risk assessment* akan dimodifikasi, dimana proses ini mencakup upaya dalam memperlakukan risiko. Seperti melakukan pilihan dalam menangani risiko. Perlakuan risiko terdiri dari beberapa jenis [1] yakni: Menghindari Risiko (*Risk Avoidance*), Mitigasi Risiko (*Risk Mitigation*), Penerimaan risiko (*Risk Acceptance*).

Tahap perlakuan risiko ini diberikan saran atas tindakan yang dapat dilakukan atas kemungkinan risiko yang telah dievaluasi, perlakuan risiko yang diberikan berdasarkan *control Objective ISO 27001 standar Information Security Management System (ISMS)* atau disebut sebagai (Sistem Manajemen Keamanan Informasi) tahun 2013 yang menyediakan kerangka kerja untuk pendekatan sensitif untuk pengelolaan sistem keamanan informasi[4].

2.7 Pemantauan dan Tinjauan

Tahapan pemantauan (*monitoring*) meliputi proses pemeriksaan, pengawasan, pengamatan atau penentuan secara kritis dan berkelanjutan terhadap suatu status. Tujuan pemantauan adalah mengidentifikasi perubahan dari tingkat kinerja yang diperlukan atau diharapkan. Tahapan peninjauan (*review*) adalah kegiatan untuk menentukan kesesuaian, kecukupan dan efektivitas dari pokok persoalan dalam mencapai sasaran yang ditetapkan.

2.8 Kesimpulan dan Saran

Tahap ini memberikan hasil akhir dari penelitian yang telah dilaksanakan serta memberikan saran terhadap organisasi terutama dalam menangani risiko kedepannya.

3. HASIL DAN PEMBAHASAN

3.1 Prinsip Manajemen risiko

Terdapat prinsip-prinsip yang memandu atau membentuk karakteristik manajemen risiko yang efisien dan efektif, yang terdiri atas: Terintegrasi, Terstruktur dan Komprehensif, Disesuaikan, Inklusif, Dinamis, Informasi Terbaik yang Tersedia, Faktor Manusia dan Budaya, serta Perbaikan Berkelanjutan.

3.1.1 Menciptakan dan Melindungi Nilai

Poin menciptakan dan melindungi nilai melekat dalam pemenuhan 8 prinsip manajemen risiko.

3.1.2 Integrasi

Semua aktivitas atau kegiatan yang dilakukan oleh tiap bagian dalam organisasi harus dihubungkan dengan manajemen risiko, agar nantinya mendukung terhadap pencapaian tujuan dan peningkatan kinerja serta inovasi. Tahapan manajemen risiko selalu menjadi faktor penting dalam menggapai dan menuju tujuan organisasi.

3.1.3 Struktur dan Komprehensif

Maksud dari terstruktur adalah adanya kejelasan pada penanggung jawab pada organisasi baik pada setiap proses bisnis maupun penanggung jawab keseluruhan. Komprehensif berarti harus mencakup seluruh area organisasi.

3.1.4 Disesuaikan

Maksud dari disesuaikan adalah manajemen risiko harus dibuat sesuai dengan kebutuhan dan sasaran organisasi.

3.1.5 Inklusif

Inklusif seluruh manajemen risiko melibatkan dan mencakupi semua pihak yang berkepentingan. Manajemen risiko dapat berhasil jika semua pemangku kepentingan dalam organisasi aktif terlibat dan bekerja dalam mencapai tujuan. Semua anggota organisasi terlibat dalam manajemen risiko. Setiap orang dalam organisasi adalah pemilik dan pengelola risiko.

3.1.6 Dinamis

Manajemen risiko bersifat dinamis karena selalu tanggap atau responsif terhadap situasi terkini yang dihadapi oleh organisasi, sedangkan situasi itu sendiri selalu berubah sepanjang waktu. Manajemen risiko bersifat berulang, Artinya, Langkah-langkah dalam manajemen risiko bersifat seperti daur (siklus) yang harus dilaksanakan secara terus-menerus.

3.1.7 Informasi Terbaik Tersedia

Informasi terbaik tersedia dimaksudkan pengambilan keputusan dalam manajemen risiko harus dilandasi oleh informasi terbaik yang tersedia. informasi risiko harus disajikan tepat.

3.1.8 Faktor Budaya Dan Manusia

Manajemen risiko dapat dipengaruhi oleh karakteristik manusia. Apabila sebuah aturan yang dibuat sebagai kontrol risiko menyesuaikan karakteristik manusia pemilik risiko, maka aturan tersebut akan lebih mudah diterima dan berdampak besar terhadap perbaikan kinerja dan pencapaian sasaran sebuah organisasi. Sehingga budaya organisasi, budaya lingkungan, dan perilaku anggota organisasi dapat lebih terjaga keselarasannya dalam pengelolaan risiko.

Peningkatan berkelanjutan merupakan prinsip yang meningkatkan keefektifitasan kerja manajemen risiko. Perbaikan yang dilakukan secara konsisten adalah suatu siklus berkesinambungan dengan menerapkan evaluasi dan pendokumentasian.

3.2 Kerangka Kerja



Gambar 2 Kerangka Kerja Manajemen Risiko

Tujuan kerangka kerja adalah membantu organisasi dalam menerapkan konsep manajemen risiko pada kegiatan organisasi dan fungsi kerja yang terkait organisasi. Siklus diawali dengan kepemimpinan dan komitmen dari manajemen puncak. Perintisan itu dilanjutkan dengan integrasi dengan sistem lain di dalam organisasi. Hasil integrasi diwujudkan di dalam desain kerangka kerja manajemen risiko untuk selanjutnya diterapkan dalam implementasi. Terakhir, efektivitas sistem dinilai pada evaluasi dan ditingkatkan pada perbaikan.

3.1.8 Kepemimpinan dan Komitmen

Peran manajemen puncak akan sangat berpengaruh dalam pelaksanaan manajemen risiko. Efektivitas manajemen risiko akan tergantung dari seberapa jauh Direksi mengintegrasikan manajemen risiko ke dalam tata kelola organisasi.

3.1.9 Integrasi

Integrasi manajemen risiko ke dalam organisasi adalah proses yang dinamis dan berulang, serta sebaiknya disesuaikan dengan kebutuhan dan budaya organisasi. Manajemen risiko sebaiknya menjadi bagian dari, dan tidak terpisahkan dari, tujuan, tata kelola, kepemimpinan dan komitmen, strategi, sasaran, dan operasi organisasi. Manajemen risiko yang difokuskan adalah Manajemen risiko terhadap IT/IS, dimana proses, aktivitas, dan fungsi yang dijalankan adalah untuk mendukung ketersediaan asset IT sebagai penunjang proses bisnis. Terutama server, sebagai asset yang paling krusial.

3.1.10 Desain

Dalam proses desain terdapat beberapa penjelasan di dalamnya sebagai berikut:

Pemahaman organisasi dan konteksnya Konteks eksternal bisa berasal dari luar organisasi TI atau dari luar organisasi induk. Sedangkan konteks internal adalah lingkungan internal organisasi teknologi informasi. Beberapa konteks eksternal yang mempengaruhi pengelolaan risiko teknologi informasi diantaranya adalah:

1) Vendor

Universitas Ma Chung menjalin kerjasama *Microsoft Partner* dalam dukungan ketersediaan perangkat lunak dari *Microsoft* dan dalam hal pembelian *software* berlangganan dan sekaligus fasilitas dukungan. Universitas Ma Chung juga menggunakan jasa *Indihome* dan *Astinet* sebagai *provider* internet, layanan dan sekaligus fasilitas dukungan.

Beberapa konteks internal dalam pengelolaan risiko teknologi informasi diantaranya adalah:

1) Struktur Organisasi

Universitas Ma Chung memiliki struktur organisasi yang digunakan untuk memetakan unit yang terlibat dalam proses manajemen risiko berdasarkan peran dan akuntabilitasnya masing-masing.

2) Sasaran Organisasi

Universitas Ma Chung merupakan perguruan tinggi, dimana proses bisnis utama yakni kegiatan akademik/tridharma dimana ini akan berpengaruh pada area fokus dalam melakukan manajemen risiko.

3) Penegasan Komitmen Manajemen Risiko

Manajemen puncak dan badan pengawas, jika memungkinkan, sebaiknya menunjukkan dan menegaskan komitmen berkelanjutan mereka terhadap manajemen risiko melalui kebijakan, pernyataan, atau bentuk lain yang secara jelas menyampaikan sasaran dan komitmen organisasi terhadap manajemen risiko.

a. Penetapan Kewenangan, Tanggung Jawab dan Akuntabilitas Organisasi

Dari dokumen OTK (Organisasi dan Tata Kerja di Lingkungan Universitas Ma Chung) tahun 2020, disebutkan bahwa UPT Sistem Informasi merupakan unsur penunjang yang berfungsi mendukung pelaksanaan kegiatan akademik dan non-akademik yang membutuhkan teknologi informasi untuk memudahkan dan melancarkan aktifitas kerja sehingga menciptakan sumberdaya yang berdaya cipta tinggi yang sesuai dengan perkembangan kebutuhan dan teknologi informasi

b. Alokasi Sumber Daya

Manajemen puncak dan badan pengawas, sesuai penerapan, sebaiknya memastikan alokasi sumber daya manajemen risiko yang memadai. Organisasi sebaiknya mempertimbangkan kapabilitas, dan keterbatasan, sumber daya yang ada.

c. Komunikasi dan Konsultasi

Organisasi sebaiknya menetapkan pendekatan yang disetujui untuk komunikasi dan konsultasi guna mendukung kerangka kerja dan memfasilitasi penerapan efektif manajemen risiko.

Komunikasi melibatkan pembagian informasi dengan audiens yang dituju. Konsultasi juga melibatkan pemberian umpan balik dari partisipan dengan harapan bahwa hal itu dapat berkontribusi dan membentuk keputusan atau aktivitas lain.

3.1.11 Implementasi

Organisasi mengimplementasikan rencana manajemen risiko yang telah ditentukan beserta pengelolaan risiko yang dipahami oleh seluruh pihak dibutuhkan pencatatan dan dokumentasi. Dokumentasi terhadap pemetaan risiko dan perlakuan terhadap risiko yang di dapat pada tahapan *risk assessment*.

3.1.12 Evaluasi

Evaluasi terhadap kerangka kerja dapat dilakukan dengan melakukan pemantauan dan peninjauan. Pemantauan dan peninjauan diperlukan untuk memastikan bahwa implementasi manajemen risiko telah dilaksanakan sesuai dengan perencanaan yang dilakukan. Hasil *monitoring* dan *review* juga dapat digunakan sebagai pertimbangan untuk melakukan perbaikan terhadap proses manajemen risiko kedepannya (berkelanjutan). Organisasi harus menetapkan

mekanisme pemantauan dan peninjauan untuk meningkatkan kualitas dan efektifitas terhadap proses manajemen risiko.

3.1.13 Peningkatan

Peningkatan berkelanjutan merupakan prinsip yang meningkatkan keefektifitasan kerja manajemen risiko. Perbaikan yang dilakukan secara konsisten adalah suatu siklus berkesinambungan dengan menerapkan evaluasi.

3.2 Proses Manajemen Risiko

Proses manajemen risiko menerapkan beberapa kebijakan, prosedur, dan praktik pada tahapan-tahapan komunikasi dan konsultasi, penetapan konteks, penilaian, perlakuan, pemantauan, peninjauan, pencatatan, serta pelaporan risiko.

Kerangka kerja dan proses dari manajemen risiko yang dapat dipergunakan sebagai arsitektur di dalam manajemen risiko sebagai bentuk usaha untuk menjamin penerapan manajemen risiko IT/IS.

3.3.1 Konsultasi dan Komunikasi

Komunikasi dan konsultasi bertujuan untuk membantu pemangku kepentingan terkait memahami risiko, dasar pengambilan keputusan, dan alasan mengapa Tindakan tertentu diperlukan. Tahap konsultasi dan komunikasi dilakukan dengan melakukan wawancara dan penyebaran kuesioner guna membantu mendapatkan informasi terutama dalam pendefinisian, pertimbangan serta penilaian terhadap risiko yang berdasarkan atas persepsi pihak mereka terhadap risiko tersebut.

3.3.2 Lingkup, Konteks, dan Kriteria

Beberapa konteks eksternal yang mempengaruhi pengelolaan risiko teknologi informasi diantaranya adalah:

1) Vendor

Universitas Ma Chung menjalin kerjasama Microsoft Partner dalam dukungan ketersediaan perangkat lunak dari Microsoft dan dalam hal pembelian software berlangganan dan sekaligus fasilitas dukungan. Universitas Ma Chung juga menggunakan jasa Indihome dan Astinet sebagai provider internet, layanan dan sekaligus fasilitas dukungan.

Beberapa konteks internal dalam pengelolaan risiko teknologi informasi diantaranya adalah:

2) Struktur organisasi

Universitas Ma Chung memiliki struktur organisasi yang digunakan untuk memetakan penetapan para pihak yang terlibat dalam proses manajemen risiko berdasarkan peran dan akuntabilitas-nya masing-masing.

3) Sasaran organisasi

Universitas Ma Chung merupakan perguruan tinggi, dimana proses bisnis utama yakni kegiatan akademik/tridharma dimana ini akan berpengaruh pada area fokus dalam melakukan manajemen risiko.

3.3.3 Risk Assessment

1) Identifikasi Risiko

Tabel 1 Identifikasi risiko pada aset server

Jenis Risiko	Risiko	Penyebab risiko
Personil	Kesalahan konfigurasi dan perawatan <i>server</i>	Kelalaian petugas
	Akses tidak diotorisasi	Adanya praktek illegal Adanya celah keamanan pada <i>server</i>
	<i>Cyber attack</i>	Adanya praktek illegal Adanya celah keamanan pada <i>server</i> Lokasi <i>server</i> yang mudah dijangkau
	Kehilangan perangkat	Pencurian perangkat Lokasi perangkat yang mudah dijangkau
Policy	Pelanggaran SOP perawatan	Kelalaian petugas
Infrastruktur	<i>Server</i> usang	Perawatan <i>server</i> yang tidak terjadwal Kualitas <i>server</i> yang tidak memadai
	Hilangnya pasokan listrik	Pemadaman listrik yang tidak terjadwal UPS tidak berfungsi Genset tidak berfungsi
	Memori <i>server</i> penuh	Perawatan <i>server</i> yang tidak terjadwal
	<i>Server</i> terserang virus/ <i>malware</i> , <i>malicious code</i>	Adanya praktek illegal Adanya celah keamanan pada <i>server</i>
	Kerentanan terhadap voltase yang bervariasi	Pemadaman listrik yang tidak terjadwal UPS tidak berfungsi Genset tidak berfungsi

2) Analisa risiko

Tabel 2 Pemetaan *likelihood* dan dampak pada asset kritis

	ID	Sumber Risiko	Risiko	<i>Likely hood</i>	Dampak	Level Dampak
Infrastruktur - Server	S1	Kelalaian petugas	Kesalahan konfigurasi, dan perawatan server	2	<ul style="list-style-type: none"> Menghambat layanan yang diberikan server (operasional) 	2
		Panduan yang tidak memadai				
	S2	Perawatan server yang tidak terjadwal	Server usang	5	<ul style="list-style-type: none"> Menghambat layanan yang diberikan server (operasional) Kehilangan data menyebabkan rusaknya perangkat kerugian finansial dan non-finansial 	4
Kualitas server yang tidak memadai						
S3	Adanya praktek ilegal	Akses tidak diotorisasi	1	<ul style="list-style-type: none"> Menghambat layanan yang diberikan server (operasional) Manipulasi data 	2	

3) Evaluasi Risiko

Pada tahapan evaluasi risiko, risiko yang telah diketahui besaran dampak dan besaran probabilitasnya akan dinilai menggunakan rujukan berupa matriks risiko, terbagi menjadi 3 level risiko dalam matriks tersebut di antaranya *low*, *medium* dan *high*. Nilai dari probabilitas dan dampak yang telah ditemukan pada risiko yang terpapar pada tahapan proses sebelumnya akan dibedakan kembali menyesuaikan matriks risiko.

Seringnya terjadi risiko serta dampak yang dihasilkan dari setiap risiko akan diolah. Sehingga pada tahap ini akan menghasilkan peringkat risiko yang terjadi pada IT/IS pada UPTSI Universitas Ma Chung untuk penentuan prioritas dalam menangani dan melakukan mitigasi pada risiko.

Tabel 3 Pemetaan Risiko pada Aset kritis Universitas Ma Chung

Likelihood	Sangat sering (5)	9	15	18 J7	23 S2	25
	Sering (4)	6 A3 M3	12	16 P3	19	24 P4
	Jarang (3)	4	10 P6	14 S5 J8 P5 A6	17 S15 A5	22 P9
	Sangat jarang (2)	2	7 S1 S12 J6 J9 P7 P11 M1 M5	11 J10 J12 J14 M2 A1	13 S7 S11 J2 J	21 S4 S8 J4 J13 P8 P10
	Tidak pernah (1)	1	3 S3 S9 S13 J5	5 P2 M6 A2	8 S6 M4 A4	20 S10 S14 J1 J11 P1
		(1) Sangat Kecil	(2) Kecil	(3) Cukup	(4) Besar	(5) Sangat besar
Dampak						

3.3.4 Perlakuan Risiko

Tabel 4 Perlakuan Risiko

Sumber Risiko	ID	Risiko	Besaran Risiko	Perlakuan Risiko	
				Bentuk perlakuan risiko	Rekomendasi SOP
Pemadaman listrik tidak terjadwal	P4	Hilangnya pasokan listrik pada Perangkat PC	24	<ul style="list-style-type: none"> Memberikan suplai listrik cadangan berupa UPS dan genset Melakukan peninjauan terhadap ketersediaan suplai listrik cadangan 	<ul style="list-style-type: none"> SOP pengadaan kebutuhan keamanan perangkat PC SOP perawatan dan pemeliharaan kebutuhan keamanan perangkat PC
Konslet					
Perawatan server yang tidak terjadwal	S2	Server usang	23	<ul style="list-style-type: none"> Melakukan peninjauan berkala terhadap performa dan kondisi server Melakukan peremajaan perangkat server Melakukan pembelian/penggantian terhadap server 	<ul style="list-style-type: none"> SOP pengadaan perangkat server SOP perawatan dan pemeliharaan perangkat server
Kualitas server yang tidak memadai					

Sumber Risiko	ID	Risiko	Besaran Risiko	Perlakuan Risiko	
				Bentuk perlakuan risiko	Rekomendasi SOP
Lokasi PC dan perangkat yang mudah dijangkau	P9	Kerusakan fisik pada perangkat PC	22	<ul style="list-style-type: none"> • Penempatan perangkat pada tempat yang aman dan terlindungi dari gangguan • Memberikan perlindungan fisik pada perangkat PC 	<ul style="list-style-type: none"> • SOP penempatan PC • SOP pengadaan kebutuhan keamanan perangkat PC
Serangga					
Infrastruktur yang tidak memadai					

4. KESIMPULAN

Kesimpulan pada penelitian ini adalah pembuatan dokumen manajemen risiko menggunakan standar ISO31000. Manajemen risiko dilakukan pada aset yang dianggap kritis yakni server, Perangkat jaringan, PC dan kelengkapan, *Microsoft family*, dan sistem informasi area akademik

Dari proses identifikasi risiko yang terdapat pada aset kritis di Universitas Ma Chung, diperoleh 52 Risiko. Hasil penilaian dikategorikan dalam tiga level penilaian risiko yaitu risiko tinggi, risiko sedang, dan risiko rendah. Sehingga dapat diuraikan sebagai berikut: (1) Terdapat 17 risiko dalam kategori risiko tinggi, (2) Terdapat 9 risiko dalam kategori risiko sedang, (3) Terdapat 26 risiko dalam kategori risiko rendah, dan (4) Risiko yang memiliki dampak terbesar adalah risiko yang berkaitan dengan listrik dan jaringan.

5. REFERENSI

- [1] Susilo, L.J., 2018. *Manajemen Risiko Berbasis ISO 31000: 2018: Panduan untuk Risk Leaders dan Risk Practitioners*. Gramedia Widiasarana Indonesia.
- [2] Mahardika, K.B., Wijaya, A.F. and Cahyono, A.D., 2019. *Manajemen risiko teknologi informasi menggunakan iso 31000: 2018 (studi kasus: cv. xy)*. Sebatik
- [3] Erlika, Y., Herdiansyah, M.I. and Mirza, A.H., 2020. *Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000*. Jurnal Informatika Global
- [4] Wijaya, V.P.P., 2022. *Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000: 2018*. JATISI (Jurnal Teknik Informatika dan Sistem Informasi)