Perancangan Rencana Keberlangsungan Bisnis dalam Manajemen Risiko Layanan Teknologi Informasi

http://dx.doi.org/10.28932/jutisi.v9i3.6539

Riwayat Artikel
Received: 19 Mei 2023 | *Final Revision*: 01 Desember 2023 | *Accepted*: 04 Desember 2023

Handoko[✉ #1], Elly[*2]

[#*]*Sistem Informasi, Universitas Mikroskil*
Jl. M.H Thamrin No.140, Medan, 20212, Indonesia
[1]handoko.wu@mikroskil.ac.id
[2]elly@mikroskil.ac.id
[✉]Corresponding author: handoko.wu@mikroskil.ac.id

Abstrak — **Universitas Mikroskil merupakan salah satu Perguruan Tinggi di Kota Medan yang mengimplementasikan teknologi informasi pada proses bisnisnya seperti pelayanan akademik bagi dosen, mahasiswa, dan tenaga kependidikan, administrasi dan penyimpanan data mahasiswa, dosen, tenaga kependidikan, dan sebagainya, proses keuangan, proses perkuliahan, pembimbingan akademik, penjadwalan perkuliahan, presensi kehadiran mahasiswa, pengisian kartu rencana studi, pengumuman jadwal, pengumuman ujian, pengumuman nilai, admisi, pengelolaan perpustakaan dan sebagainya. Penyelesaian masalah saat ini dilakukan case by case yang dirasakan kurang efisien, kurang konsisten, kurang skalabel dalam menangani kondisi yang tidak terduga yang muncul. Melihat banyaknya penanganan proses pada Universitas Mikroskil dibutuhkan suatu rencana penanggulangan bencana yang dapat digunakan level manajerial untuk mengantisipasi terjadinya hal-hal yang tidak diinginkan seperti hilangnya data-data atau dokumen penting, adanya virus pada komputer atau server, dan sebagainya. Tujuan penelitian ini adalah menganalisis dan mengkaji risiko dan dampak risiko pada Universitas Mikroskil. Selanjutnya dilakukan penyusunan perencanaan keberlangsungan bisnis berdasarkan analisis risiko dan dampak bisnis untuk mengatasi teknologi informasi yang terkendala akibat risiko bencana yang terjadi. Penilaian risiko pada dua ancaman alam memiliki kritikalitas Vital. Penilaian risiko pada tiga ancaman manusia memiliki 1 kritikalitas Critical-Mission, 1 kritikalitas Vital, dan 1 kritikalitas Minor. Penilaian risiko pada tiga ancaman infrastruktur memiliki 1 kritikalitas Critical-Mission, dan 2 kritikalitas Vital. Penilaian risiko pada tiga ancaman sistem TI memiliki 2 kritikalitas Critical-Mission, dan 1 kritikalitas Vital. Dari 8 kegiatan operasional terdapat 5 layanan Critical-Mission, 2 layanan Vital, 1 layanan Important.**

Kata kunci— **Analisis Dampak Bisnis; Layanan TI; Penilaian Risiko; Rencana Keberlangsungan Bisnis.**

Designing a Business Continuity Plan in Risk Management of Information Technology Services

Abstract — ***Universitas Mikroskil is one of the universities in Medan City that implements information technology in its business processes such as academic services for lecturers, students, education staff, administration and student data storage, lecturers, education staff,, and so on, financial processes, lecture processes, academic guidance, lecture scheduling, student attendance attendance, study plan card filling, schedule announcements, exam announcements, grade announcements, admissions, library management and so on. Problem solving is currently done case by case which is felt to be less efficient, less consistent, less scalable in***

handling unexpected conditions that arise. Seeing the many processes handled at Mikroskil University, a disaster management plan is needed that can be used at the managerial level to anticipate the occurrence of unwanted things such as loss of important data or documents, viruses on computers or servers, and so on. The aim of this study is to analyze and assess the risks and impacts of risks at Universitas Mikroskil. Next, a business continuity plan is prepared based on an analysis of business risks and impacts to overcome information technology that is constrained by the disaster risk that occurs. Risk assessment on two natural threats has Vital criticality. The risk assessment on the three human threats has 1 Critical-Mission criticality, 1 Vital criticality, and 1 Minor criticality. The risk assessment on three infrastructure threats has 1 Critical-Mission criticality, and 2 Vital criticality. Risk assessment on three IT system threats has 2 Critical-Mission criticality, and 1 Vital criticality. From 8 operational activities, there are 5 Critical-Mission services, 2 Vital services, 1 Important service.

Keywords— ***Business Impact Analysis; Business Continuity Plan; IT Service, Risk Assessment.***

I. PENDAHULUAN

Dalam perjalanan sebuah bisnis, pelaku bisnis umumnya selalu akan menghadapi tantangan dan kendala baik kendala yang minor maupun mayor. Tantangan ini umumnya berupa situasi yang muncul tanpa dikehendaki oleh pelaku bisnis dan biasanya bersifat tidak pasti serta menimbulkan kerugian bagi bisnis. Risiko dapat dikatakan sebagai terjadinya suatu peristiwa yang dapat mempengaruhi tujuan pencapaian organisasi. Risiko ini tidak dapat dipisahkan dari suatu bisnis, tidak terlepas dari bidang bisnis apapun yang dijalankan. Risiko ini dapat muncul dalam berbagai bentuk gangguan baik dari eksternal bisnis (seperti bencana, *malware*, dan sebagainya) maupun ancaman dari internal bisnis sendiri (seperti kesalahan manusia, gangguan utilitas, dan sebagainya). Gangguan ini semakin meningkat dengan semakin banyaknya perusahaan yang mengimplementasikan teknologi informasi dan semakin terhubung dengan jaringan eksternal. Kerugian besar dan bahkan kebangkrutan dapat terjadi dalam suatu organisasi bisnis jika tidak ada perencanaan untuk menghadapinya. Terlepas dari seberapa kompleks TI yang sudah diimplementasikan pada organisasi bisnis, organisasi bisnis membutuhkan rencana untuk menghadapi gangguan yang mempengaruhi bisnis mereka [1].

Dengan menyadari adanya ancaman kerugian yang dapat terjadi tanpa diduga, pelaku bisnis tentu harus memiliki persiapan dalam menghadapi risiko tersebut yang dikenal dengan manajemen risiko. Persiapan tersebut guna untuk memastikan bisnis dapat tetap berjalan meskipun terjadi kendala tersebut. Proses manajemen risiko sendiri memiliki konsep yang berbeda ketika diimplementasikan di proses bisnis pada perusahaan yang berbeda [2]. Oleh karena itu, diperlukan suatu perencanaan untuk memastikan kegiatan operasional suatu organisasi tetap berjalan meskipun terjadi gangguan. Salah satu upaya yang dilakukan adalah membuat *business continuity plan* (BCP) yang sesuai sebagai bagian dari *Business Continuity Management* (BCM) [1]. Untuk menjaga pertumbuhan aktivitas bisnis di pasar mana pun, *Business Continuity Management* merupakan konsep penting yang harus diikuti oleh perusahaan [3]. Instrumen penting untuk kelangsungan hidup organisasi bisnis adalah pembentukan sistem manajemen kesinambungan bisnis yang memungkinkan mereka mengelola risiko, menemukan peluang, dan mengamankan kelangsungannya [4].

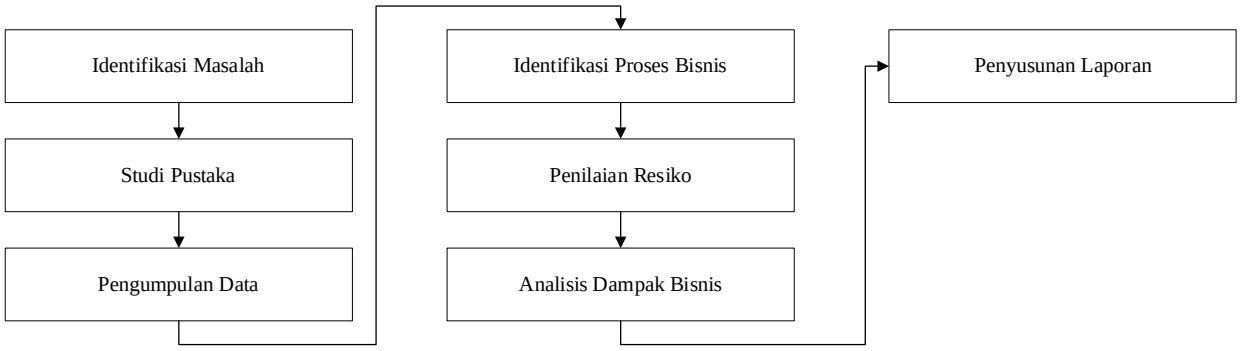
Perguruan Tinggi sebagai salah satu bisnis di bidang pendidikan juga tidak dapat terlepas dari risiko ini. Pada proses bisnis Perguruan Tinggi saat ini mayoritas sudah mengimplementasikan teknologi informasi. Hal ini membuat aset dan sumber daya perusahaan berpotensi rentan terhadap risiko, misalnya, karena serangan *cyber* [5]. Universitas Mikroskil merupakan salah satu Perguruan Tinggi di Kota Medan juga sudah mengimplementasikan teknologi informasi pada proses bisnisnya. Pemanfaatan teknologi informasi ini mencakup pelayanan akademik bagi mahasiswa maupun tenaga kependidikan, administrasi dan penyimpanan data mahasiswa, dosen, tenaga kependidikan, karyawan, dan sebagainya, proses keuangan, proses perkuliahan baik perkuliahan tatap muka/luring maupun perkuliahan daring, pembimbingan akademik, penjadwalan perkuliahan, presensi kehadiran mahasiswa, pengisian kartu rencana studi, pengumuman jadwal, pengumuman ujian, pengumuman nilai, admisi, pengelolaan perpustakaan dan sebagainya. Melihat banyaknya proses pada Universitas Mikroskil yang sudah mengimplementasikan teknologi informasi, tentu akan terhambat apabila teknologi yang diimplementasikan tersebut tidak dapat beroperasi sebagaimana yang direncanakan. Saat ini penanganan risiko hanya dilakukan sesuai dengan prosedur operasi standar yang biasanya dilaksanakan bagian pengelola teknologi informasi. Jika terjadi hal di luar dugaan, maka pihak pengelola teknologi informasi akan mencari masalah apa yang menjadi dan kemudian baru menyelesaikannya. Penyelesaian masalah dilakukan *case by case*. Meskipun pendekatan *case by case* hingga saat ini menjadi pilihan alternatif yang baik, pendekatan ini sebenarnya kurang efisien, kurang konsisten, kurang skalabel maupun berpotensi mengalami *human error* dan biaya yang tinggi dalam menangani kondisi tidak terduga yang muncul. Oleh karena itu Universitas Mikroskil membutuhkan suatu rencana penanggulangan bencana yang dapat digunakan oleh level manajerial untuk mengantisipasi terjadinya hal-hal yang tidak diinginkan seperti hilangnya data-data atau dokumen penting, adanya virus pada komputer atau *server*, dan sebagainya.

Terdapat beberapa penelitian terdahulu yang sudah dilakukan untuk menyusun perencanaan keberlangsungan bisnis, seperti yang dilakukan pada penelitian [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], masing-masing penelitian melakukan analisis dan kajian risiko terhadap proses bisnis tertentu dan pada beberapa penelitian, memiliki penjelasan atau literatur yang dilakukan mengenai implementasi BCP pada perusahaan berskala kecil, menengah dan besar.

Adapun tujuan dari penelitian ini adalah menganalisis dan mengkaji risiko dan dampak risiko tersebut terhadap layanan TI pada Perguruan Tinggi yaitu Universitas Mikroskil. Kemudian akan dilakukan penyusunan perencanaan keberlangsungan bisnis berdasarkan analisis risiko dan dampak bisnis yang sudah dilakukan untuk mengatasi teknologi informasi yang terkendala akibat risiko bencana yang terjadi.

II. METODOLOGI PENELITIAN

Lokasi penelitian adalah Universitas Mikroskil Medan. Penelitian ini menggunakan metode kualitatif yang bertujuan untuk mendeskripsikan dan menganalisis aktivitas sosial yang terjadi [15], [16], [17]. Metodologi penelitian yang digunakan berdasar pada diagram kemajuan perencanaan proyek keberlangsungan bisnis dan pemulihan bencana [2]. Penelitian ini dilakukan dengan beberapa tahapan yang saling berkaitan satu dengan lainnya seperti yang terlihat pada Gambar 1 :



Gambar 1. Tahapan Penelitian

Berikut penjelasan tahapan pada penelitian ini:

1. Identifikasi Masalah
   Tahapan pertama dalam penelitian ini adalah identifikasi masalah. Pada tahapan ini dilakukan penggambaran tentang permasalahan yang dialami oleh perusahaan.
2. Studi Pustaka
   Pada tahapan ini, dilakukan tinjauan penelitian terdahulu dan teori pustaka yang relevan untuk menyelesaikan permasalahan yang ditemukan pada tahapan pertama.
3. Pengumpulan Data
   Pada tahapan ini, dilakukan pengamatan lingkungan organisasi untuk memperoleh data yang dibutuhkan. Beberapa teknik yang direncanakan akan digunakan antara lain wawancara, observasi dan pengamatan, serta dokumentasi untuk menganalisis dokumen-dokumen yang berhubungan dengan proses bisnis dan penerapan teknologi informasi beserta rencana pemulihan bencana pada Universitas Mikroskil.
4. Identifikasi Proses Bisnis
   Pada tahapan ini, dilakukan identifikasi dan melakukan analisis terhadap proses bisnis pada Universitas Mikroskil, lalu menentukan proses bisnis yang akan dievaluasi.
5. Penilaian Risiko
   Pada tahapan ini, akan dilakukan identifikasi gangguan, risiko, atau bencana yang dapat terjadi sesuai dengan proses bisnis yang dievaluasi. Tahapan ini menjadi kunci perencanaan pemulihan bencana. Tahapan ini mencakup beberapa sub tahapan yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko.
6. Analisis Dampak Bisnis
   Selanjutnya akan dilakukan analisis dampak bisnis dari bencana dan gangguan yang terjadi dan memahami dampak yang terjadi karena adanya gangguan tersebut. Pada tahapan ini akan dilakukan evaluasi proses utama dan Teknologi Informasi yang diimplementasikan pada proses itu. Pada tahapan ini juga ditentukan waktu pemulihan, prioritas, beserta sumber daya dan ketergantungannya.
7. Penyusunan Laporan
   Tahapan terakhir adalah menyusun laporan *Business Continuity Plan*.

III. HASIL DAN PEMBAHASAN

A. Penilaian Risiko

Pada penelitian ini dilakukan tiga penilaian risiko, yang mencakup penilaian ancaman (*threat assessment*), penilaian kerentanan (*vulnerability assessment*), dan penilaian dampak (*impact assessment*). Penilaian risiko melibatkan pihak pengelola teknologi informasi, mahasiswa, dan dosen. Penilaian risiko juga dilakukan dengan metode wawancara pada pihak pengelola teknologi informasi terkait dengan nilai risiko, kuesioner pada mahasiswa dan dosen untuk evaluasi kemungkinan terjadi serta kerentanan dan dampaknya. Penilaian risiko (*risk assessment*) menggunakan pendekatan kualitatif. Pada pendekatan kualitatif, ketiga penilaian *vulnerability assessment*, *likelihood assessment*, dan *impact assessment* menggunakan skala penilaian yang terlihat pada Tabel 1 [2]:

TABEL 1
SKALA PENILAIAN

Value	***Likelihood***	***Vulnerability* or *Impact***
6	*Constant*	*Extremely high*
5	*Very frequently*	*Very high*
4	*Frequently*	*High*
3	*Infrequently*	*Low*
2	*Very infrequently*	*Very low*
1	*Never*	*Extremely low*

1. Ancaman Alam (*Natural Threat*)

Terdapat beberapa ancaman alam (*natural threat*) yang dapat berdampak pada proses bisnis Universitas Mikroskil, seperti hujan yang lebat dan berkepanjangan, gempa bumi dengan skala besar, erupsi gunung berapi, asap kebakaran hutan dan lain sebagainya. Ancaman-ancaman tersebut dapat mengganggu proses bisnis dan masing-masing memiliki jangka waktu pemulihan yang berbeda-beda. Penilaian risiko untuk ancaman tersebut diuraikan pada Tabel 2:

TABEL 2
PENILAIAN RISIKO *NATURAL THREAT*

Natural Threat 1		***Natural Threat 2***	
Threat Name	Hujan lebat dan panjang	*Threat Name*	Gempa bumi dengan skala besar
Threat Source	*External*	*Threat Source*	*External*
Vulnerability Rating	*4 (high)*	*Vulnerability Rating*	*4 (high)*
Likelihood Rating	*4 (frequency)*	*Likelihood Rating*	*2 (very infrequently)*
Impact Rating	*4 (high)*	*Impact Rating*	*4 (high)*
Overall Risk Rating	*4 (high)*	*Overall Risk Rating*	*3 (low)*
Criticality	*Vital*	*Criticality*	*Vital*

Berdasarkan Tabel 2, *Existing Control* yang dapat dilakukan berupa:

a) *Natural Threat* 1
   1) Pemasangan *router* pada setiap lantai agar koneksi internet tetap dapat terjangkau.
   2) Memberikan toleransi waktu keterlambatan perkuliahan bagi dosen dan mahasiswa.
   3) Membuat kebijakan bagi dosen dan mahasiswa agar menyampaikan informasi kepada pihak kampus apabila terjebak hujan yang mengakibatkan tidak dapat tiba di kampus secara tepat waktu untuk mengikuti perkuliahan.
   4) Mempersiapkan dan memastikan genset dapat digunakan, dikarenakan jika terjadi hujan deras umumnya akan diikuti dengan pemadaman listrik.

b) *Natural Threat* 2
   1) Mempersiapkan perencanaan penanggulangan gempa bumi bersama dengan para *stakeholder* dengan berbagai variasi skala gempa bumi baik dari yang kecil hingga yang besar.
   2) Melakukan latihan simulasi penyelamatan diri bagi dosen, mahasiswa maupun tenaga kependidikan.
   3) Melakukan kajian mengenai kondisi bangunan secara berkala.
   4) Memastikan *server* penyimpanan berada di lokasi yang aman dari gempa.
   5) Memiliki asuransi untuk gedung, peralatan teknologi informasi, dan elektronik.

2. Ancaman Manusia (*Human Threat*)

Terdapat beberapa ancaman manusia (*human threat*) yang dapat berdampak pada proses bisnis Universitas Mikroskil, seperti kebakaran, pencurian atau perusakan barang elektronik, dan ketidaktahuan pengguna *front-end*. Ancaman-ancaman

tersebut dapat mengganggu proses bisnis dan masing-masing memiliki jangka waktu pemulihan yang berbeda-beda. Penilaian risiko untuk ancaman tersebut diuraikan pada Tabel 3:

TABEL 3
PENILAIAN RISIKO *HUMAN THREAT*

Human Threat 1		***Human Threat 2***		***Human Threat 3***	
Threat Name	Kebakaran	*Threat Name*	Pencurian atau Perusakan Barang Elektronik	*Threat Name*	Ketidaktahuan pengguna *front-end*
Threat Source	*Internal*	*Threat Source*	*Internal* dan *External*	*Threat Source*	*External*
Vulnerability Rating	*6 (extremely high)*	*Vulnerability Rating*	*5 (very high)*	*Vulnerability Rating*	*3 (low)*
Likelihood Rating	*2 (very infrequently)*	*Likelihood Rating*	*3 (infrequently)*	*Likelihood Rating*	*5 (very frequently)*
Impact Rating	*6 (extremely high)*	*Impact Rating*	*5 (very high)*	*Impact Rating*	*3 (low)*
Overall Risk Rating	*5 (very high)*	*Overall Risk Rating*	*4 (high)*	*Overall Risk Rating*	*4 (high)*
Criticality	*Critical-Mission*	*Criticality*	*Vital*	*Criticality*	*Minor*

Berdasarkan Tabel 3, *Existing Control* yang dapat dilakukan berupa:

a) *Human Threat* 1
   1) Membuat perencanaan penanggulangan kebakaran bersama dengan para *stakeholder* baik menganalisis lokasi kebakaran yang dapat terjadi, mengidentifikasi orang yang terdampak dari bencana kebakaran, serta menganalisis cara untuk mengurangi atau menghindari risiko.
   2) Me-*review* dan memperbaharui penilaian risiko kebakaran setiap periode, minimal 1 tahun sekali.
   3) Mempersiapkan rute dan jalan keluar darurat.
   4) Memasang alat pendeteksi asap dan bel peringatan terjadinya kebakaran.
   5) Mempersiapkan alat pemadam kebakaran dan dipasang pada setiap gedung dan lantai.
   6) Memastikan alat pendeteksi, bel peringatan, dan alat pemadam kebakaran dapat berfungsi dengan baik.
   7) Membuat peta evakuasi yang jelas dan pada setiap tingkat gedung.
   8) Membangun ruangan khusus penahan api khususnya untuk ruangan *server* karena *server* sangat rentan dengan api maupun air.
   9) Memiliki asuransi gedung, perlengkapan, dan peralatan.
   10) Membekali dosen, mahaiswa dan tenaga kependidikan agar dapat mempersiapkan diri jika terjadi kebakaran.
   11) Mematikan aliran listrik ketika terjadi kebakaran.

b) *Human Threat* 2
   1) Memastikan semua kamera CCTV baik yang berada di dalam maupun luar gedung dapat berfungsi dan terdapat tenaga sekuritas yang melakukan pengawasan.
   2) Memastikan tenaga sekuritas bertugas pada titik posko yang sudah ditentukan.
   3) Khusus untuk perpustakaan, memastikan tidak ada yang masuk ke dalam ruangan perpustakaan tanpa melakukan *tapping* ke mesin scan yang ada, dan meletakkan barang bawaan pada tempat yang telah disediakan bagi mahasiswa, dosen maupun tenaga kependidikan. Ketika hendak meninggalkan perpustakaan, maka perlu dilakukan pemeriksaan sesuai dengan prosedur yang ada.
   4) Pada area parkir, pihak keamanan harus memastikan bahwa semua orang yang hendak keluar dari area parkir dengan membawa kereta harus menunjukkan STNK kendaraan tersebut dan memastikan seluruh CCTV di area parkir berfungsi dengan baik.

c) *Human Threat* 3
   1) Terdapat prosedur *hardcopy* yang dapat dibaca oleh pengguna untuk mengikuti langkah-langkah atau ketentuan atau aturan yang berlaku.
   2) Terdapat *customer service* yang dapat dihubungi untuk mengajukan pertanyaan atau didatangi secara langsung.

3. Ancaman Infrastruktur (*Infrastructure Threat*)

Ancaman infrastruktur merupakan masalah eksternal yang besar, sulit dikendalikan, dicegah, disebutkan, atau diselesaikan. Terdapat tiga ancaman infrastruktur pada Universitas Mikroskil, yaitu ancaman padamnya listrik, ancaman komunikasi, dan ancaman gangguan transportasi umum. Ketiga hal tersebut dapat mengganggu proses bisnis Universitas Mikroskil. Penilaian risiko untuk ancaman tersebut diuraikan pada Tabel 4:

TABEL 4
PENILAIAN RISIKO *INFRASTRUCTURE THREAT*

Infrastructure Threat 1		***Infrastructure Threat 2***		***Infrastructure Threat 3***	
Threat Name	Padamnya listrik	*Threat Name*	Masalah Komunikasi	*Threat Name*	Gangguan Transportasi Umum
Threat Source	Pemadaman listrik oleh pihak PLN karena faktor tertentu	*Threat Source*	*External*	*Threat Source*	*External*
Vulnerability Rating	*4 (frequently)*	*Vulnerability Rating*	*3 (infrequently)*	*Vulnerability Rating*	*4 (frequently)*
Likelihood Rating	*4 (frequently)*	*Likelihood Rating*	*3 (infrequently)*	*Likelihood Rating*	*4 (frequently)*
Impact Rating	*6 (extremely high)*	*Impact Rating*	*5 (very high)*	*Impact Rating*	*5 (very high)*
Overall Risk Rating	*5 (very high)*	*Overall Risk Rating*	*4 (high)*	*Overall Risk Rating*	*4 (high)*
Criticality	*Critical-Mission*	*Criticality*	*Vital*	*Criticality*	*Vital*

Berdasarkan Tabel 4, *Existing Control* yang dapat dilakukan berupa:

a) *Infrastructure Threat* 1
   1) Terdapat dua buah genset untuk mengantisipasi pemadaman aliran listrik sehingga proses perkuliahan tidak terganggu. Ketersediaan bahan bakar dan genset ini perlu dilakukan pemeriksaan secara berkala.
   2) Pemasangan *sekring* (pemutus arus) sehingga saat terjadi korsleting tidak akan mengakibatkan korsleting lainnya lagi.
   3) Melakukan pemeriksaan secara berkala pada setiap instalasi, stop kontak maupun kabel penghantar listrik. Bila terdapat kerusakan, perlu segera dilakukan perbaikan.
   4) Melakukan investasi *Uninterrupted Power Supplies* (UPS) untuk menyediakan cadangan listrik bagi komputer tenaga kependidikan dan untuk menghindari kerusakan data maupun komputer yang ditimbulkan oleh pemadaman listrik secara tiba-tiba.

b) *Infrastructure Threat* 2
   1) Melakukan koordinasi dengan *service provider* telepon yang digunakan oleh pihak kampus, apabila ditemukan masalah pada perangkat telepon.
   2) Memastikan layanan *WiFi* dapat berjalan dengan baik.

c) *Infrastructure Threat* 3
   1) Memberikan waktu toleransi keterlambatan.
   2) Membuat peraturan yang mengakomodir dosen, mahasiswa, dan tenaga kependidikan agar memberikan pemberitahuan ke pihak kampus agar tidak ketinggalan perkuliahan.

4. Ancaman Sistem TI (*IT-Specific Threat*)

Pada ancaman spesifik TI, Universitas Mikroskil memiliki ancaman terhadap ancaman *cyber* (*cyber threat*), kegagalan sistem atau peralatan, kehilangan data. Penilaian risiko untuk ancaman tersebut diuraikan pada Tabel 5:

TABEL 5
PENILAIAN RISIKO *IT-SPECIFIC THREAT*

IT-Specific Threat 1		***IT-Specific Threat 2***		***IT-Specific Threat 3***	
Threat Name	Serangan *Cyber*	*Threat Name*	Kehilangan Data	*Threat Name*	Kerusakan perangkat keras
Threat Source	*External*	*Threat Source*	*Internal dan external*	*Threat Source*	*Internal dan external*
Vulnerability Rating	*6 (extremely high)*	*Vulnerability Rating*	*6 (extremely high)*	*Vulnerability Rating*	*5 (very high)*
Likelihood Rating	*4 (frequently)*	*Likelihood Rating*	*2 (very infrequently)*	*Likelihood Rating*	*4 (frequently)*
Impact Rating	*6 (extremely high)*	*Impact Rating*	*6 (extremely high)*	*Impact Rating*	*5 (very high)*
Overall Risk Rating	*5 (very high)*	*Overall Risk Rating*	*5 (very high)*	*Overall Risk Rating*	*5 (very high)*
Criticality	*Critical-Mission*	*Criticality*	*Critical-Mission*	*Criticality*	*Vital*

Berdasarkan Tabel 5, *Existing Control* yang dapat dilakukan berupa:

a) *IT-Specific Threat* 1
   1) Melakukan pembaruan *patch* pada sistem keamanan komputer untuk menutupi celah-celah keamanan yang bisa saja muncul pada sistem operasi komputer atau *server* yang digunakan.
   2) Menggunakan *firewall* untuk tidak meneruskan paket data yang tidak diketahui dengan jelas asalnya.
   3) Menggunakan *software* keamanan jaringan komputer yang terpercaya pada sistem komputer atau *server*.
   4) Melakukan pembaruan dan pemeriksaan secara berkala pada *server* komputer untuk menghindari *server* dijadikan *zombie* untuk melakukan *Remote Controlled Attack*.
b) *IT-Specific Threat* 1
   1) Melakukan autentikasi untuk mengontrol akses data sehingga orang yang tidak berkepentingan tidak dapat sembarangan mengakses data tersebut.
   2) Melakukan kegiatan *audit trail* untuk memastikan segala kegiatan yang dilakukan terekam dan terdokumentasi.
   3) Melakukan enkripsi untuk melindungi data yang dikirim dalam bentuk pesan.
   4) Secara konsisten menegakkan semua kebijakan dan prosedur, pengamanan fisik, dan keamanan data.
c) *IT-Specific Threat* 1
   1) Memiliki asuransi perangkat keras.
   2) Melakukan pemeliharaan pada setiap perangkat keras dan pengujian yang berkala.
   3) Memberikan aturan sanksi bagi karyawan yang dengan ceroboh menjatuhkan perangkat keras.
   4) Mendokumentasi kerusakan barang untuk menilai kualitas dari perangkat keras yang ada.
   5) Menyediakan perangkat keras cadangan untuk persiapan bila terjadi kerusakan mendadak sehingga memiliki pengganti ketika dibutuhkan.

B. Analisis Dampak Bisnis

Pada tahapan analisis dampak bisnis ini dilakukan analisis proses mana dalam bisnis yang vital bagi operasional Universitas Mikroskil yang sedang berlangsung serta untuk memahami dampak gangguan proses ini terhadap bisnis. Tujuan utama pada tahapan ini adalah untuk mengkorelasikan komponen sistem spesifik terhadap layanan yang diberikan, yang kemudian digunakan untuk mengkarakterisasi konsekuensi dari gangguan ke komponen sistem.

Tingkat kepentingan suatu fungsi bisnis dalam organisasi dapat dikategorikan menjadi beberapa tingkat sebagai berikut [2]:

1. *Critical-Mission*: proses bisnis ini memiliki dampak paling besar pada operasional Universitas Mikroskil dan memiliki prioritas untuk dipulihkan terlebih dahulu jika terjadi gangguan.
2. *Important:* proses dan fungsi bisnis *Important* tidak akan menghentikan bisnis dari beroperasi dalam jangka waktu dekat, tetapi dapat memberikan dampak jangka panjang jika proses dan fungsi bisnis hilang atau dinonaktifkan.
3. Vital: beberapa fungsi bisnis mungkin dapat berada diantara *Critical-Mission* dan *Important*, jadi dapat digunakan kategori tengah yang diberi label Vital atau *Essential*.
4. Minor: proses dan fungsi bisnis Minor merupakan proses yang telah dikembangkan dari waktu ke waktu untuk menangani masalah atau fungsi kecil yang berulang.

TABEL 6
ANALISIS DAMPAK BISNIS UNIVERSITAS MIKROSKIL

Business Function	***Business Process***	***Functions***	***Criticality***
Operasional	Pembimbingan Akademik	*Critical-Functions*	*Critical-Mission*
	Penjadwalan Perkuliahan	*Critical-Functions*	*Critical-Mission*
	Pengumuman Jadwal dan Ujian	*Essential-Functions*	Vital
	Pengumuman Nilai	*Essential-Functions*	Vital
	Presensi	*Critical-Functions*	*Critical-Mission*
	Admisi dan Pendaftaran Ulang	*Critical-Functions*	*Critical-Mission*
	Administrasi Akademik	*Critical-Functions*	*Critical-Mission*
	Pengelolaan Peminjaman Perpustakaan	*Necessary-Functions*	*Important*

Analisis terhadap dampak bisnis pada Tabel 6 dapat dirincikan sebagai berikut:

1. Pembimbingan Akademik: Pembimbingan Akademik merupakan salah satu proses bisnis yang penting dalam perkuliahan dan termasuk kedalam proses bisnis *Critical-Mission*, dalam pelaksanaan pembimbingan akademik mahasiswa diarahkan oleh dosen pembimbing akademik mulai dari pengisian Kartu Rencana Studi yang kemudian akan disetujui oleh dosen

pembimbing akademik sebagai syarat untuk mengikuti perkuliahan di semester yang akan dimulai. Jika proses bisnis ini tidak tersedia maka akan mengganggu kegiatan perkuliahan mahasiswa.

2. Penjadwalan Perkuliahan: Penjadwalan Perkuliahan merupakan salah satu proses bisnis yang penting dalam perkuliahan dan termasuk kedalam proses bisnis *Critical-Mission*. Penjadwalan Perkuliahan disusun oleh Sekretariat Fakultas sebelum jadwal kuliah di-*update* ke Portal Akademik. Proses bisnis penjadwalan perkuliahan berhubungan erat dengan pengisian KRS pada saat pembimbingan akademik, jadwal kuliah harus tersedia terlebih dahulu setelah itu pengisian KRS baru dapat dilakukan oleh mahasiswa dan juga pemberian persetujuan KRS oleh dosen pembimbing akademik.
3. Pengumuman Jadwal dan ujian: proses bisnis juga termasuk dalam proses bisnis yang penting dalam perkuliahan, dan tergolong dalam kategori Vital. Pengumuman jadwal dan ujian disusun oleh Sekretariat Fakultas dan diinformasikan pada dosen dan mahasiswa menjelang jadwal pelaksanaan ujian tengah semester dan ujian akhir semester, pengumuman akan dikirim melalui email ke masing-masing email mahasiswa dan akan diumumkan di Portal Akademik Mikroskil.
4. Pengumuman nilai: pengumuman nilai juga termasuk dalam proses bisnis yang penting dalam perkuliahan, dan tergolong kedalam Vital. Pengumuman nilai diproses oleh Bagian Administrasi Akademik, setelah pelaksanaan ujian selesai, dosen akan mengoreksi hasil ujian mahasiswanya dan setelah selesai nilai akan diserahkan untuk di-*update* ke Portal Akademik.
5. Presensi: proses presensi menjadi salah satu proses yang paling penting dalam mendukung operasi bisnis utama di Universitas Mikroskil, proses presensi tergolong dalam kategori *Critical-Mission*. Presensi di Universitas Mikroskil dilakukan dengan menggunakan *Mi-Card* yang ditempelkan pada mesin yang sudah terpasang di semua kelas. Status kehadiran dosen dan mahasiswa akan di-*update* pada sistem absensi yang dikelola oleh Sekretariat Fakultas, data yang sudah diproses kemudian akan di-*upload* ke Portal Akademik.
6. Admisi dan Pendaftaran Ulang: Admisi dan pendaftaran ulang adalah kegiatan yang harus dilakukan oleh calon mahasiswa setelah dinyatakan lulus dalam ujian saringan masuk, pendaftaran ulang dapat dilakukan oleh mahasiswa melalui situs Bagian Pemasaran. Proses ini tergolong dalam kategori *Critical-Mission*.
7. Administrasi Akademik: Administrasi akademik merupakan fungsi bisnis yang bertujuan untuk memenuhi kebutuhan akademik mulai dari Administrasi Wisuda, Surat Izin Kegiatan Akademik untuk Perusahaan, Surat Keterangan Riset ke Perusahaan, Surat Keterangan Aktif Kuliah, Pindah Waktu Kuliah, Penundaan Kegiatan Akademik (PKA)/Cuti, Koreksi Nilai, Ujian Khusus, Tugas Akhir, Ujian Akhir, Upload Tugas Akhir dan Jurnal, Ujian Susulan, Upload Dokumen, Pengunduran Diri, Pemrosesan Surat Sakit/Izin, dan lain sebagainya. Semua kegiatan yang ada pada proses bisnis administrasi akademik mendukung perkuliahan mahasiswa sehingga administrasi akademik masuk kedalam golongan *Critical-Mission*.
8. Pengelolaan Peminjaman Perpustakaan: Pengelolaan peminjaman perpustakaan merupakan proses bisnis yang penting yang berifat mendukung kegiatan perkuliahan, mahasiswa dan dosen dapat meminjam buku yang dibutuhkan sebagai bahan referensi dalam meningkatkan wawasan mata kuliah yang bersangkutan, pengelolaan pinjaman perpustakaan termasuk dalam kategori *Important*.

Kegiatan analisis dampak bisnis pada Tabel 6 dapat dilanjutkan ke proses pengembangan strategi mitigasi untuk merencanakan penerimaan risiko dari sisi perguruan tinggi terkait risiko yang dapat diterima. Status mitigasi ini dapat digunakan nantinya untuk melakukan pengembangan rencana keberlangsungan bisnis atau pemulihan bencana jangka panjang, menengah, dan pendek bagi organisasi setingkat perguruan tinggi.

IV. SIMPULAN

Kegiatan penilaian risiko yang dilakukan memaparkan hasil prioritas risiko dengan tingkat kritikalitas sebagai berikut di mana penilaian pada ancaman alam, antara lain: hujan lebat dan panjang dengan nilai risiko 4 kritikalitas Vital, gempa bumi dengan skala besar dengan nilai risiko 3 kritikalitas Vital. Dilanjutkan dengan ancaman manusia, antara lain: kebakaran dengan nilai risiko 5 kritikalitas *Critical-Mission*, pencurian atau perusakan barang elektronik dengan nilai risiko 4 kritikalitas Vital, ketidaktahuan pengguna *front-end* dengan nilai risiko 4 kritikalitas Minor. Selanjutnya ancaman infrastruktur antara lain: padamnya listrik dengan nilai risiko 5 kritikalitas *Critical-Mission*, masalah komunikasi dengan nilai risiko 4 kritikalitas Vital, gangguan transportasi umum dengan nilai risiko 4 kritikalitas Vital. Terakhir ancaman sistem TI antara lain: serangan *cyber* dengan nilai risiko 5 kritikalitas *Critical-Mission*, kehilangan data dengan nilai risiko 5 kritikalitas *Critical-Mission*, dan kerusakan perangkat keras dengan nilai risiko 5 kritikalitas Vital. Dari 8 kegiatan operasional terdapat 5 layanan dengan kritikalitas *Critical-Mission*, 2 layanan Vital, 1 layanan *Important*.

DAFTAR PUSTAKA

[1] S. V. Fani and A. P. Subriadi, "Business continuity plan: Examining of multi-usable framework," Manchester, United Kingdom, 2019.

[2] Susan Snedaker and Chris Rima, Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd ed., Watham, USA: Elsevier, 2014.

[3] A. Abu and R. Al-Ahliyya, "Impact of Strategic Agility on Business Continuity Management (BCM): The Moderating Role of Entrepreneurial Alertne *Journal of Management Information and Decision Sciences*, vol. 25, no. 4, pp. 1-9, 2022.

[4] G. Chatzistelios, E. P. Kechagias, S. P. Gayialis, G. A. Papadopoulos and N. E. Spyridonakos, "Business Continuity During the COVID-19 Pande Era: Surviving and Improving the Quality Process Management System," *WSEAS Transactions on Environment and Development*, vol. 18, pp. 617-6 2022.

[5] K. T. Kosmowski, E. Piesik, J. Piesik and M. Śliwiński, "Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Busir Continuity Management," *Energies (Basel)*, vol. 15, no. 10, pp. 1-21, 2022.

[6] Sandy Febriyanto, Adi Utarini and Ni Luh Putu Eka Andayani, "Strategi Business Continuity Plan Untuk Keberlangsungan RS Mata 'DR. YAP'," *Jur Manajemen Pelayanan Kesehatan*, vol. 25, no. 2, pp. 1-9, 2022.

[7] K. D. Chandra, "Penerapan Business Continuity Pada Bank Central Asia," *Bina Ekonomi*, vol. 21, no. 1, pp. 13-24, 2017.

[8] Muhaemin, "Mengembangkan Business Continuity Planning (BCP) Dengan Pendekatan Kuantitatif Studi Kasus: SIAK –DITJEN ADMIND KEMENDAGRI," *Jurnal Sistem Informasi, Teknologi Informatika dan Komputer*, vol. 9, no. 1, pp. 1-11, 2018.

[9] W. H. Sasongko and T. Sukwika, "Penerapan Business Continuity Management Pada Masa Pandemi COVID-19 Di PT Brantas Abipraya," *Jur Distribusi*, vol. 9, no. 2, pp. 193-206, 2021.

[10] G. B. Santoso and D. Gitarini, "Perancangan Business Continuity Plan Studi Kasus Printgila," *Jurnal Penelitian dan Karya Ilmiah Lemlit*, vol. 2, nc pp. 21-28, 2017.

[11] S. Rahmawati, A. Okfitasari and S. Wulandari, "Perencanaan Keberlangsungan Bisnis di Masa Pandemi," *MABHA JURNAL*, vol. 3, no. 1, pp. 19 2022.

[12] J. S. Dayrit, "Business Continuity Management of Dental Clinics in Pampanga: An Action Research," *PREO Journal of Business and Management*, 3, no. 1, pp. 49-63, 2022.

[13] Mochammad Ikmal Amirullah and Apol Pribadi Subriadi, "Evaluasi Kerangka Kerja Perencanaan Keberlangsungan Bisnis pada PT. Lotte Chemical T Nusantara," *Jurnal SISFO*, vol. 8, no. 2, pp. 87-98, 2019.

[14] D. N. Amalia, "Penyusunan Perencanaan Keberlangsungan Bisnis Pada PT. XYZ," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 5, nc pp. 719-727, 2022.

[15] A. Kosieradzka, J. Smagowicz and C. Szwed, "Ensuring the business continuity of production companies in conditions of COVID-19 pandemic in Pol – Applied measures analysis," *International Journal of Disaster Risk Reduction*, vol. 72, pp. 1-23, 2022.

[16] Mahua Mukherjee , Ranit Chatterjee, Bhagat Kumar Khanna, Preet Pal Singh Dhillon, Atul Kumar , Sukhreet Bajwa, Amit Prakash and Rajib Sh "Ecosystem-centric business continuity planning (eco-centric BCP): A post COVID19 new normal," *Progress in Disaster Science*, vol. 7, pp. 1-5, 2C

[17] Donna Lyn G. Labangon, Simon V. De Leon, Roana Marie L. Flores, Mennie Ruth A. Viray and May L. Cajes, "Staying Ahead of the Curve: Mitiga Disruptions Through Business Continuity Planning in the Academic Library Setting," *Qualitative and Quantitative Methods in Libraries*, vol. 11, nc pp. 161-191, 2022.