Perancangan *Contingency Planning Disaster Recovery* Unit Teknologi Informasi Perguruan Tinggi menggunakan NIST SP800-34

Design of Contingency Planning Disaster Recovery for Higher Education Information Technology Units using NIST SP800-34

Wahyu Adi Prabowo[1], Rima Dias Ramadhani[2]
[1,2] Fakultas Informatika, Jurusan Informatika, Institut Teknologi Telkom Purwokerto
E-mail: [1]wahyuadi@ittelkom-pwt..ac.id, [2]rima@ ittelkom-pwt.ac.id

Abstrak

Pembangunan institusi pendidikan selama ini telah bertumbuh pesat sesuai dengan kebutuhan masyarakat dan menjadikan sebuah insitusi yang semakin komplek dengan kebutuhan fungsi operasional sistem layanan informasinya. Untuk menjalankan fungsinya, institusi pendidikan didukung oleh infrastruktur sistem layanan teknologi informasi yang sangat kompleks. Dalam penyelenggaraan fungsi operasional layanan tersebut, perguruan tinggi membutuhkan peran sistem teknologi informasi yang handal dalam keberlangsungan kegiatan kerjanya. Semua komponen teknologi informasi merupakan komponen yang rentan terhadap gangguan baik itu dari internal maupun eksternal, untuk itu dalam penyelenggaraan institusi pendidikan, perguruan tinggi dalam hal ini wajib memiliki rencana untuk menanggulangi segala gangguan maupun bencana. Dalam hal ini penanganan penanggulangan ganguan dan bencana memuat beberapa prosedur dan mekanisme tersendiri dalam pengamanan datanya. Disaster Recovery Plan (DRP) merupakan langkah tepat dalam membangun penanganan gangguan dan bencana terhadap infrastruktur sistem layanan teknologi informasi yang ada di perguruan tinggi. Penerapan untuk membangun penanganan bencana ini mengacu pada NIST SP 800-34 Rev.1 yang didalamnya terdapat beberapa tahapan penilaian resiko, menganalisa dampak bisnis, mengidentifikasi pencegahannya dan pengembangan strategi mitigasi. Hasil akhir dari penelitian ini adalah rancangan dokumen DRP berdasarkan NIST SP 800-34 Rev.1 yang disesuaikan dengan kondisi di perguruan tinggi

Kata kunci: Disaster Recovery Plan, NIST SP 800-34 Rev 1, Business Continuity Plan

Abstract

The development of educational institutions so far has been growing rapidly by following the needs of the community and making an institution that has increasingly complex needs of its operational functions. To carry out its functions, educational institutions are supported by a very complex information technology infrastructure. In carrying out these operational functions, Higher-educational institution requires the role of reliable information technology continuity of its work activities. All its information technology infrastructure is components that are vulnerable to disturbances both from internal and external, for that case the implementation of educational institutions are required to have a plan to deal with all disruptions and disasters. In this case, the handling of disaster management contains several procedures and separate mechanisms in securing the data. Disaster Recovery Plan (DRP) is the right step for building disaster management of the existing information technology infrastructure at Higher-educational institution. This methodology for developing disaster management refers to NIST SP 800-34 Rev.1, which includes several stages of risk assessment, analyzing business impacts, identifying prevention and developing mitigation strategies. The final result of this study is the DRP document design based on NIST SP 800-34 Rev.1 which is adapted to the conditions at the Higher-educational institution.

Keywords: Disaster Recovery Plan, NIST SP 800-34 Rev 1, Business Continuity Plan

1. PENDAHULUAN

Resiko merupakan paparan terhadap kemungkinan-kemungkinan kerugian atau keuntungan ekonomi maupun keuangan, kerusakan fisik atau kerusakan material, dan keterlambatan penanganan sebagai konsekuensi dari ketidakpastian yang terkait dengan melakukan suatu tindak lanjut yang pasti [1]. Selama 2 dekade terakhir ini, manajemen resiko telah menjadi terkenal akarena telah menjadi fungsi yang terorganisir [2]. Ketika dijalankan, fungsi resiko ini telah mempertimbangkan sejumlah besar kemungkinan-kemungkinan ancaman terhadap bisnis. Tidak hanya dibisnis saja tetapi dengan adanya fungsi resiko ini akan dapat memantau spektrum yang lebih besar dari ancaman-ancaman ke dalam organisasi itu sendiri, fungsi resiko ini perlu untuk diintegrasikan ke dalam seluruh organisasi. Munculnya strategi manajemen resiko dapat menyebabkan manajemen resiko secara otomatis telah tertanam di setiap proses perencanaan strategis di suatu institusi. Kemungkinan-kemungkinan resiko yang telah diciptakan melalui strategi yang baik, akan dapat diantisipasi dan ditindak lanjuti sesuai dengan rencana yang telah di buat dan dapat mengurangi dampak dari resiko tersebut [3]. Setiap organisasi pasti ada berbagai jenis resiko dan organisasi harus mengembangkan budaya manajemen resiko. Semua resiko tersebut harus diidentifikasi, dinilai dan dikelola dengan baik. Pendekatan ini tentunya dapat memberikan kepada organisasi sebuah kemampuan untuk memahami jumlah dari resiko yang di dapat dan dapat memahami kebergantungan antar resiko-resiko tersebut [4].

Banyak penelitian yang menerapkan metode manajemen resiko teknologi informasi di berbagai bidang, seperti penelitian yang dilakukan oleh Hanafi & Ernastuti dengan memakai ISO 31000:2018 pada perusahaan pertamina, Hanafi menemukan bahwa dengan dengan memakai ISO 31000:2018 didapatkan 3 jenis variable resiko yakni resiko dari alam/lingkungan, resiko dari kesalahan manusia dan resiko dari sistem dan infrastruktur [5]. Prilly et all menganalisa manajemen resiko teknologi informasi dengan menggunakan COBIT 5 pada perusahaan. Prilly merekomendasikan bahwa untuk menerapkan manajemen risiko harus dibentuk sebuah manajemen khusus dalam pengelolaan resiko sehingga manajemen resiko dapat dikontrol dengan baik, membuat sebuah dokumen yang spesifik tentang resiko beserta skenario TI dalam mengatasi resiko [6]. Evaluasi yang dilakukan oleh Damar & Achmad pada kantor arsip daerah kota Samarinda untuk manajemen resiko teknologi Informasi dengan menggunakan The Risk IT Framework mengatakan bahwa dalam melakukan evaluasi manajemen resiko teknologi informasi harus dilakukan secara terus menerus dan terjadwal sehingga risiko dapat dimonitor dengan baik [7]. Pada penelitian tersebut dapat dilihat bahwa manajemen resiko sangat penting untuk diimplementasikan disuatu institusi, salah satunya adalah institusi pendidikan.

Institusi pendidikan merupakan organisasi yang kompleks dari masa ke masa, dari segi proses bisnis, jabatan struktural dan jabatan organisasi hingga ukuran jumlah sumber daya baik itu sumber daya manusia dan sumber daya teknologi informasi yang ada di dalamnya. Perubahan yang kompleks ini diikuti juga dengan perubahan kondisi teknologi informasi yang dihadapi dalam usaha untuk mewujudkan visi misi institusi. Perubahan yang kompleks ini tidak terlepas dari pengelolaan manajemen resiko yang telah menjadi salah satu aktivitas paling dimonitoring di saat ini. Setiap institusi pendidikan harus memiliki kebijakan manajemen resiko yang komprehensif agar dapat dihadapi dengan tepat dari setiap resiko yang telah dicatat. Tantangan-tantangan dalam pengelolaan manajemen resiko ini semakin ketat dikarenakan institusi pendidikan merupakan sentralisasi pengelolaan pendidikan yang tidak terlepas dari penggunaan sumber daya teknologi Informasi. Salah satu contoh resiko yang dihadapi oleh institusi pendidikan adalah masalah keamanan yaitu kerentanan sistem informasi di lingkungan belajar virtual (yang mengarah kepada keaslian data, manipulasi dan pencurian informasi). Yang lain adalah kerentanan dari perluasan infrastruktur fisik pendidikan tinggi (masalah pencurian, kondisi Kesehatan dan keselamatan yang semakin kompleks, kebakaran) [8].

Penelitian yang dilakukan oleh Deni et all dalam menerapkan manajemen resiko pada perguruan tinggi dengan metode *octave allegro* menyatakan bahwa dengan adanya penilaian resiko dapat memberikan sebuah gambaran mengenai kemungkinan adanya sebuah ancaman pada asset kritikal dan dengan dapat dengan cepat mengambil langkah-langkah yang tepat dalam

pencegahannya [9] . Menurut Susanti et all bahwa area yang paling terdampak dari resiko pada perguruan tinggi adalah reputasi universitas, kepercayaan pengguna dan biaya operasional [10]. Maka dari itu dalam meningkatkan investasi Teknologi Informasi (TI), Institut Teknologi Telkom Purwokerto (ITTP) selalu berupaya untuk melakukan evaluasi terhadap resiko-resiko layanan TI yang akan dihadapi. Peranan layanan TI telah membawa dampak yang signifikan bagi perkembangan institusi terutama adalah untuk mendukung kegiatan proses bisnis yang semakin besar tiap tahunnya. Faktor-faktor ancaman resiko yang akan dihadapi oleh institusi pun akan semakin besar kedepannya. Ancaman ini pun akan bervariasi sesuai dengan keadaan, seperti rusaknya peralatan TI, hilang maupun tidak berfungsinya operasional alat TI (*Hardware*). Tidak hanya *hardware*, tetapi juga ancaman-ancaman resiko infrastruktur TI yang berupa sistem dan data menjadi hal penting untuk menjadi perhatian bagi top manajemen, karena infrastruktur sistem dan data menjadi pondasi penting untuk keberlangsungan proses bisnis perguruan tinggi Institut Teknologi Telkom Purwokerto. Adanya ancaman risiko tersebut akan mengakibatkan dampak kerugian yang besar bagi institusi. Dengan mempertimbangkan ruang lingkup manajemen resiko IT, ITTP semakin sadar akan resiko-resiko yang akan terjadi kedepannya. Diharapkan dengan adanya perancangaan contingency planning DRP ini dapat membantu ITTP dalam menanggulangi resiko dari alam maupun dari manusia itu sendiri.

Tidak hanyak bencana alam, tetapi gangguan dari manusia menjadi faktor penting dalam merancang DRP. Menurut Abdul Kadir, ancaman yang menjadi perhatian didalam sistem informasi dibagi menjadi 2, yaitu ancaman aktif dan ancaman pasif. Ancaman aktif merupakan kejahatan yang terjadi yang diakibatkan oleh kecurangan dan kejahatan terhadap komputer, sedangkan ancaman pasif mencakup kegagalan sistem, kesalahan manusia dan bencana alam [11].

Disaster Recovery Planning (DRP) diperlukan untuk meminimalkan dampak risiko yang terjadi terhadap ancaman bencana yang mengancam infrastruktur layanan IT. Menurut Undang-undang Republik Indonesia Nomor 24 tahun 2007 tentang penanggulangan bencana, DRP adalah serangkaian kegiatan yang dilakukan untuk mengatasi bencana melalui pengorganisasian serta melalui langkah yang tepat guna dan berdayaguna. DRP juga salah satu langkah untuk mengurangi dampak ancaman risiko yang ditimbulkan dari bencana yang telah terjadi sehingga proses bisnis masih tetap dapat berjalan. Menurut Susan Snedaker, DRP merupakan sebuah metodologi yang digunakan untuk membuat dan memvalidasi sebuah rencana untuk memonitor operasi bisnis yang berkesinambungan sebelum, selama dan setelah bencana atau peristiwa terjadi. *Disaster recovery* merupakan bagian dari *business continuity*, dan berkaitan langsung dengan dampak yang dihasilkan dari suatu bencana maupun peristiwa yang terjadi. Pemulihan pemadaman server, pelanggaran keamanan maupun bencana alam seperti angin topan, gempa, banjir, tanah longsor merupakan termasuk kategori ancaman [12].

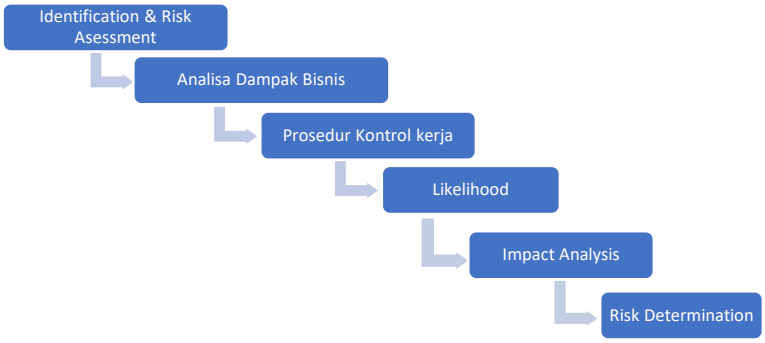
Menurut Susan Snedaker *disaster recovery* biasanya memiliki beberapa langkah dalam tahap perencanaan, meskipun langkah-langkah itu tidak menggambarkan yang akan terjadi ke depannya tetapi *disaster recovery* dapat menghentikan efek dari dampak bencana agar secepat mungkin diatasi. Langkah ini mungkin saja dengan mematikan sebuah sistem yang telah disusupi, mengevaluasi sistem mana yang terkena dampak banjir maupun gempa bumi dan menentukan cara terbaik utuk melanjutkan proses bisnis yang akan di jalankan [13].

Pentingnya untuk membuat *Disaster Recovery Planing* dengan menggunakan NIST sp800-34 menjadi konsentrasi penulis untuk mengatasi permasalahan manajemen resiko di Institut Teknologi Telkom Purwokerto dari ancaman resiko terhadap layanan sistem informasi yang mungkin akan mengganggu proses bisnis pendidikan di ITTP terjadi kedepannya dan mengembalikan fungsi-fungsi sistem dalam keadaan semula.

2. METODE PENELITIAN

Dalam melakukan proses implementasi perancangan DRP, Penulis membutuhkan data sekunder yang dikumpulkan dari unit IT *Support* ITTP, data DRP ini diperlukan data-data kualitatif yang berupa data aset Sistem Informasi dan infrastruktur Teknologi Informasi yang nantinya akan digunakan untuk penilaian terhadap resiko dan analisa dampak bisnis, dan data

kuantitatif digunakan untuk menentukan RTO (*Recovery Time Objective*) dan RPO (*Recovery Point Objective*) yang merupakan data dari hasil wawancara dengan unit Sistem Informasi yang berada di ITTP .Untuk melengkapi analisa *Risk Assessment* yang akan dilakukan, secara umum penelitian ini akan dibagi beberapa tahapan. Perancangan DRP ini menerapkan kerangka kerja dari NIST SP 800-34 yang memuat prosedur *Identification* & *Risk Assessment*, Analisa Dampak Bisnis, Prosedur Kontrol, *Likelihood, Impact Analysis & Risk Determination*, yang dapat dilihat pada gambar 1.



Gambar 1. Metode Penelitian

a. Risk Asessment

Pengolahan hasil data dari *Diaster Recovery Plan* diawali dengan menentukan aset-aset kritikal dengan menggunakan analisa *value chain*. Penentuan aset kritikal ini dikerjakan dengan maksud untuk mengidentifikasi sumber daya dan kemampuan layanan TI yang ada di Institut Teknologi Telkom Purwokerto dalam berbagai kegiatan bisnisnya.

b. Identifikasi Resiko

Langkah ini dilakukan untuk mengidentifikasi adanya sebuah resiko terhadap sistem TI. Resiko ini dapat datang dan menjadi kelemahan dari sebuah sistem TI, kelemahan ini dapat disebabkan dari beberapa faktor yaitu faktor alam, manusia dan lingkungan. Sangat penting sekali bagi para top level manajemen teknologi informasi untuk memahami resiko dan respon apa yang akan dilakukan kedepannya terhadap resiko-resiko yang di hadapi kedepannya.

c. Kontrol Sistem

Langkah ini bertujuan untuk mendokumentasikan seluruh daftar kontrol keamanan yang dilakukan guna untuk mengontrol sistem layanan TI yang sedang berjalan. Kontrol ini harus sesuai dengan kebijakan dari standar institusi yang bersangkutan karena berkaitan dengan standar audit TI. Analisa ini juga bertujuan untuk mengevaluasi apakah standar yang sudah dilakukan dapat berjalan dengan perencanaan yang sudah dibuat

d. Identifikasi Kemungkinan (Likelihood)

Pada langkah berikutnya, peneliti melakukan penetapan peringkat untuk suatu kemungkinan resiko yang akan terjadi untuk suatu system layanan teknologi Informasi yang terdiri atas nilai tinggi (*high*), sedang (*moderate*), dan rendah (*low*). Resiko-resiko ini akan diidentifikasi didalam tabel, dan penilaian bersifat subjektif berdasarkan kemungkinan (*likelihood*) kerentanan terhadap *threat* atau *vulnerability* yang akan terjadi dan kemungkinan akan menjadi ancaman kedepannya

e. Identifikasi Impact Analysis

Langkah ini bertujuan untuk menetapkan peringkat terhadap dampak resiko dengan nilai tinggi ,sedang, dan rendah terhadap resiko yang telah teridentifikasi. Peringkat ini ditentukan berdasarkan tingkat dampak terparah yang dihasilkan dari resiko yang telah di identifikasi. Langkah ini juga bertujuan untuk mengidentifikasi besar dampak yang terjadi terhadap gangguan operasional layanan TI terhadap organisasi, sistem dan fungsi mana yang terganggu bagi

keberlangsungan operasional bisnis. Analisa ini dilakukan untuk membuat keputusan yang penting bagaimana untuk membuat strategi terbaik dalam pemulihan bencana yang terjadi.

f. Risk Determination

Tujuan dari langkah ini adalah untuk menghitung tingkat resiko secara keseluruhan dengan nilai tinggi, sedang dan rendah untuk setiap resiko yang telah diidentifikasi. Dalam hal ini untuk menentukan tingkat resiko didasarkan pada kemungkinan-kemungkinan resiko yang terjadi dan dampaknya terhadap organisasi.

3. HASIL DAN PEMBAHASAN

a. Risk Asessment

Tujuan dari sebuah analisis resiko TI adalah untuk mengidentifikasi dan menilai resiko yang dihadapi terhadap teknologi informasi/sistem informasi, agar dapat dipilih pengamanan yang tepat untuk menghadapi segala resiko yang akan dihadapi nanti [14]. Tahapan ini untuk mengidentifikasi potensi-potensi sumberdaya yang ada di ITTP sehingga resiko-resiko terhadap proses bisnis dan sistem dapat diidentifikasi secara menyeluruh melalui *value chain analysis.* Barney merekomendasikan bahwa *value-chain analysis* merupakan suatu metode untuk mengidentifikasi sumber daya dan kemampuan dengan potensi yang maksimal untuk menciptakan keunggulan yang kompetitif [15]. Dalam memudahkan penjabaran proses bisnis ITTP, digunakan *porter's value-chain analysis* seperti digambarkan pada gambar 2.

Gambar 2. *Value-chain analysis*

Dari hasil analisa *value chain* tersebut didapatkan ada 2 bagian aktivitas yang mempunyai peranan penting dalam proses bisnis ITTP. Bagian aktivitas yang pertama (*primary activity*) terdapat beberapa aktivitas, yaitu kegiatan Penerimaan Mahasiswa Baru (PMB), e-Learning, perkuliahan praktikum dan laboratorium, perpustakaan, kegiatan kemahasiswaan, yudisium, wisuda, *Career Development Center*, dan Alumni Tracer. Bagian aktivitas yang kedua (*secondary activities*) terdapat beberapa aktivitas, yaitu perencanaan kurikulum, pengadaan, sarana dan prasarana (logistik), kepegawaian, keuangan, pengawasan internal dan penjaminan mutu. Berdasarkan *value-chain* diatas lalu peneliti melakukan identifikasi aset SI/TI yang ada di ITTP, analisa tersebut diambil berdasarkan analisa perangkat lunak (*software*) dan perangkat keras (*hardware*), analisis jaringan serta kondisi sistem yang berjalan di lingkungan ITTP.

Dalam mengidentifikasi perangkat keras dan jaringan peneliti melakukan survey ke unit sisfo (Sistem Informasi) untuk mendapatkan data-data perangkat keras dan pendukungnya yang telah digunakan di ITTP. Data tersebut dapat dilihat pada tabel 1.

Tabel 1.. Daftar Perangkat Pendukung Sistem Informasi

No	Perangkat Pendukung	Jumlah
1	Bandwith	100Mbps
2	Router Mikrotik	2 unit
3	Access Point	30 unit
4	Ruang data center	3 ruang
5	Ruang Server (router)	2 ruang
6	Ruang Server CCTV	1 Ruang

Dokumen rencana strategis ITTP menjelaskan bahwa ITTP telah memanfaatkan infrastruktur teknologi informasi yang mendukung kegiatan proses bisnisnya dalam hal pendidikan dan kegiatan administratif untuk memberikan pelayanan terbaik bagi para *stakeholder* baik secara langsung maupun tidak langsung. Data-data terkait dengan sistem informasi di identifikasi dapat dilihat pada tabel 2.

Tabel 2. Daftar Sistem Informasi

No	Sistem Informasi	Fungsional
1	Sistem Informasi Akademik: i-Gracias	Sistem yang dibangun untuk keperluan pengelolaan data-data akademik dengan penerapan TI
2	PMB Online	Sistem Penerimaan mahasiswa baru secara online
3	e-learning	Sistem yang membantu mahasiswa dalam kuliah secara online
4	Sistem Informasi Perpustakaan	Sistem untuk memudahkan pelayanan perpustakaan bagi mahasiswa dan petugas perpustakaan
5	E-journal	Sistem portal jurnal online
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	Sistem Aplikasi keuangan tentang pelaporan keuangan dari ITTP kepada Yayasan Telkom
7	Website official ittelkom.ac.id	Informasi tentang Institut Teknologi Telkom Purwokerto
8	Blog dosen, mahasiswa, staff, UKM	Blog yang diperuntukkan kepada dosen, mahasiswa, staff ITTP dan UKM
9	Aplikasi Memo online	Informasi memo kepada seluruh staff manajemen ITTP
10	Aplikasi Nomor surat kesekretariatan	Sistem yang berisi tentang penomoran terhadap surat-surat resmi yang akan disahkan oleh manajemen ITTP

b. Identifikasi Resiko

Pada tahapan ini, identifikasi resiko dilakukan untuk mengetahui proses kritikal yang dapat mempengaruhi proses bisnis di ITTP. Lallmahamood membahas bahwa ada beberapa resiko yang akan dihadapi terhadap teknologi Informasi, seperti penghapusan file-file penting, *hacker* yang merusak sistem antarmuka web, sabotase sebuah sistem, virus yang dapat menghapus data seluruh organisasi dan badai yang dapat mengancam infrastruktur fisik teknologi informasi [16]. Selain itu masih ada kerentanan yang mengancam Infrastruktur TI, menurut Brar et al, ada banyak jenis bencana alam seperti gempa bumi, banjir, angin topan dan bencana yang diakbitkan dari manusianya sendiri seperti perang, ledakan bom, kebocoran bahan kimia, dll atau kecelakaan yang mengakibatkan kebakaran dahsyat maupun pesawat yang menabrak pusat data yang dapat menghancurkan blok-blok data penting [17]. Brar et al juga mengatakan bahwa bencana yang paling berbahaya adalah bencana yang diakibatkan dari kesengajaan, contohnya adalah karyawan ataupun mantan karyawan yang tidak puas terhadap perusahaan sehingga dapat membalas dendam dengan cara mencemari data perusahaan dengan virus sehingga dapat melumpuhkan kinerja perusahaan maupun mencuri data dengan sembunyi-sembunyi [17]. Kategori ini merupakan kategori dari spionase atau pengrusakan yang disebabkan oleh *hacker*. Resiko resiko yang disebutkan oleh Lallmahamood dan Brarr merupakan resiko bencana yang disebabkan oleh bencana alam maupun manusia, dan semua kategori yang telah disebutkan tersebut merupakan bencana yang sama, yang dapat menghancurkan sistem dan infrastruktur teknologi informasi. Tabel identifikasi resiko IT dapat dilihat pada tabel 3.

Tabel 3. Identifikasi Resiko

No	Asset	Threat	Vulnerability
1	Sistem Informasi Akademik: i-Gracias	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
2	PMB Online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
3	e-learning	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
4	Sistem Informasi Perpustakaan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
5	E-journal	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
7	Website official ittelkom.ac.id	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
8	Blog dosen, mahasiswa, staff, UKM	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
9	Aplikasi Memo online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system
10	Aplikasi Nomor surat kesekretariatan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system

c. Kontrol Sistem

Tahapan ini adalah proses untuk mengdokumentasikan seluruh proses kritikal untuk mengontrol keadaan keamanan agar proses bisnis tetap berjalan dengan baik. Kontrol ini lalu dicocokan dengan resiko yang sudah diidentifikasi sebelumnya, yang hasilnya dapat dilihat pada tabel 4.

Tabel 4. Kontrol Sistem

No	Asset	Threat	Kontrol
1	Sistem Informasi Akademik: i-Gracias	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
2	PMB Online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
3	e-learning	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
4	Sistem Informasi Perpustakaan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
5	E-journal	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
7	Website official ittelkom.ac.id	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
8	Blog dosen, mahasiswa, staff, UKM	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
9	Aplikasi Memo online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server
10	Aplikasi Nomor surat kesekretariatan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server

d. Identifikasi Kemungkinan (*Likelihood*)

Tahapan *likelihood* ini merupakan tahapan untuk memeringkatkan asset bisnis yang menjadi asset krusial jika terjadi sebuah bencana. Pemeringkatan ini dilakukan agar jika terjadi bencana, ada hal yang harus dilakukan terhadap sistem agar proses bisnis secepatnya dapat berjalan untuk meminimalkan resiko bisnis yang ada di ITTP. Dari segi perspektif ekonomi dan bisnis [13], DRP fokus terhadap kegiatan yang memiliki efek untuk mengurangi kemungkinan terjadinya bencana daripada berfokus untuk meminimalkan dampak bencana.

Menurut Bryson et al, kehandalan dari DRP adalah untuk mengukur kemungkinan resiko yang akan terjadi terhadap perencanaan strategi agar tercapainya kesinambungan, pemulihan sistem , dan restorasi sistem yang telah ditetapkan sebelumnya [18]. Karena implementasi dari DRP pada dasarnya adalah pemulihan aktivitas layanan dari proyek teknologi dan sistem informasi, yang sangat memungkinkan bahwa aktivitas proyek infrastruktur TI tersebut dapat gagal untuk diaktifkan. Oleh karena itu di perlukan pemetaan kemungkinan jalur-jalur kritis sistem agar pemulihan layanan sistem dapat tercapai, pemulihan ini juga sangat dipengaruhi oleh kejadian-kejadian yang tidak terduga. Identifikasi *likelihood* dapat dilihat pada tabel 5.

Tabel 5. Identifikasi Kemungkinan (Likelihood)

No	Asset	Likelihood
1	Sistem Informasi Akademik: i-Gracias	high
2	PMB Online	high
3	e-learning	moderate
4	Sistem Informasi Perpustakaan	very low
5	E-journal	low
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	very low
7	Website official ittelkom.ac.id	low
8	Blog dosen, mahasiswa, staff, UKM	low
9	Aplikasi Memo online	very low
10	Aplikasi Nomor surat kesekretariatan	low

e. Identifikasi *impact analysis*

Penilaian peringkat resiko khususnya melibatkan identifikasi resiko, analisis resiko dan penentuan prioritas resiko [19]. Hal ini sangat penting karena dapat menentukan penilaian resiko terhadap perubahan-perubahan yang akan terjadi [20]. Dampak resiko ini dilihat dari data RPO, RTO dan MTD yang telah dikumpulkan. Langkah berikutnya dalam menganalisis dampak resiko yang telah di identifikasi maka selanjutnya melakukan analisis terhadap data RPO (*Recovery Point Objective*), RTO (*Recovery Time Objective*, MTD (*Maximum Tolerable Downtime*). Menurut Snedaker, RPO adalah jumlah waktu maksimal atas kehilangan data proses bisnis yang berjalan yang dapat ditoleransi oleh instansi organisasi, RTO adalah waktu yang tersedia dalam memulihkan suatu sistem dan sumber daya dari operasional TI akibat gangguan (*disaster*) yang terjadi, MTD adalah jumlah total waktu maksimal dari kehilangan data yang dapat ditoleransi oleh instansi atau organisasi untuk mengembalikan proses bisnisnya seperti semula akibat terjadinya gangguan. RPO, RTO dan MTD ini menurut snedaker digunakan untuk untuk menentukan waktu yang digunakan untuk memulihkan (*recovery time*) proses bisnis yang diakibatkan oleh gangguan [8]. Identifikasi *Impact analysis* dapat dilihat pada tabel 6.

Tabel 6. Impact Analysis

No	Asset	Impact Level
1	Sistem Informasi Akademik: i-Gracias	high
2	PMB Online	moderate
3	e-learning	moderate
4	Sistem Informasi Perpustakaan	very low
5	E-journal	moderate
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	very low
7	Website official ittelkom.ac.id	moderate
8	Blog dosen, mahasiswa, staff, UKM	moderate
9	Aplikasi Memo online	very low
10	Aplikasi Nomor surat kesekretariatan	low

f. *Risk Determination*

Tahapan ini adalah untuk menentukan tingkatan resiko terhadap kemungkinan dan dampak yang terjadi terhadap organisasi di ITTP. Dalam penentuan ini nilai-nilai yang diberikan masih bersifat subjektif, nilai tersebut berdasarkan nilai kemungkinan (*likelihood*) yang dikombinasikan dengan dampak kejadian. Dalam setiap nilai tingkatan resiko dinyatakan dengan korelasi antara dampak resiko dan kemungkinan yang dihasilkannya. Tabel 7 dibawah ini merupakan penjelasan terhadap *risk determination* di Institut Teknologi Telkom Purwokerto.

Tabel 7. Risk Determination

No	Asset	Likelihood	Impact Level	Matrix Score	Risk Level
1	Sistem Informasi Akademik: i-Gracias	high	high	100	High
2	PMB Online	high	moderate	50	medium
3	e-learning	moderate	moderate	50	Medium
4	Sistem Informasi Perpustakaan	very low	very low	10	Low
5	E-journal	low	moderate	30	low
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	very low	very low	10	low
7	Website official ittelkom-pwt.ac.id	low	moderate	30	low
8	Blog dosen, mahasiswa, staff, UKM	low	moderate	30	low
9	Aplikasi Memo online	very low	very low	10	Low
10	Aplikasi Nomor surat kesekretariatan	low	low	10	low

4. KESIMPULAN DAN SARAN

Dari hasil penelitian yang dilakukan dalam merancang DRP ITTP, didapatkan beberapa kesimpulan sebagai berikut, :

1. Hasil dari analisa *risk assessment* TI yang dilakukan di Institut Teknologi Telkom Purwokerto dengan menggunakan NIST Sp 800-34 dihasilkan beberapa resiko terhadap infrastruktur TI dan Sistem TI yang dapat dijadikan sebuah acuan terhadap penerapan rencana pemulihan sistem jika terjadi suatu bencana.
2. Dari analisa *value chain* terdapat 10 kritikal aset Sistem TI yang terdapat di Institut Teknologi Telkom Purwokerto
3. Hasil *risk determination* menunjukkan pula nilai tingkat resiko dari aset sistem TI yang dapat mengganggu proses bisnis ITTP jika terjadi suatu bencana, yaitu pada *level high* terdapat didalam sistem informasi akademik, pada level *medium* terdapat didalam sistem PMB dan E-Learning, pada level *low* terdapat di dalam sistem informasi perpustakaan, E-

Journal, Sistem Aplikasi pelaporan keuangan dari IT Telkom ke Yayasan (SIMONAL), Website official www.ittelkom-pwt.ac.id, Blog dosen, mahasiswa, staff dan UKM, Aplikasi memo online, aplikasi nomor surat kesekretariatan.

Berdasarkan identifikasi hasil penelitian tentang implementasi perancangan DRP, peneliti menyarankan *Disaster Recovery Planning* (DRP) dapat digabungkan dengan standar manajemen resiko ISO 31000:2018 agar dapat terbentuknya dokumen *Business Continuity Planning* (BCP) yang berkaitan erat dengan *Disaster Recovery Plan* (DRP). Sehingga proses bisnis dapat berjalan sesuai dengan *Standar Operating Procedure* (SOP) yang dimiliki oleh ITTP yang sudah terbentuk berdasarkan dokumen dari DRP dan BCP.

UCAPAN TERIMA KASIH

Penelitian ini didukung oleh LPPM Institut Teknologi Telkom Purwokerto yang telah banyak membantu dan memberikan dukungan terkait dengan bantuan fasilitas penelitian, dan pendanaan internal terkait dengan penelitian ini.

DAFTAR PUSTAKA

[1] C. B. Chapman and D. F. Cooper, "Risk analysis: Testing some prejudices," *Eur. J. Oper. Res.*, vol. 14, no. 3, pp. 238–247, 1983, doi: 10.1016/0377-2217(83)90260-6.

[2] M. Woods, "Linking risk management to strategic controls: A case study of Tesco plc," *Int. J. Risk Assess. Manag.*, vol. 7, no. 8, pp. 1074–1088, 2007, doi: 10.1504/IJRAM.2007.015295.

[3] A. Campbell and M. Jones, "Rethinking business risk," 2007.

[4] H.-P. Berg, "Risk management: procedures, methods and experiences," *Risk Manag.*, vol. 1, no. 17, pp. 79–95, 2010.

[5] H. I. Pribadi, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000 : 2018 Dengan FMEA (Studi Kasus PT Pertamina)," vol. 01, pp. 28–35, 2020, doi: 10.21456/vol10iss1pp28-35.

[6] P. P. Thenu, A. F. Wijaya, C. Rudianto, U. Kristen, and S. Wacana, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 (STUDI KASUS : PT GLOBAL INFOTECH)," vol. 2, no. 1, pp. 1–13, 2020.

[7] D. Nurcahyono and A. Djunaedi, "Evaluasi Pelaksanaan Manajemen Risiko Teknologi Informasi pada K antor Arsip Daerah Kota Samarinda dengan Menggunakan The Risk IT Framework," vol. 2, no. 3, pp. 3–6, 2013.

[8] I. Helsloot and W. Jong, "Risk management in higher education and research in the Netherlands," *J. Contingencies Cris. Manag.*, vol. 14, no. 3, pp. 142–159, 2006, doi: 10.1111/j.1468-5973.2006.00490.x.

[9] Deni Ahmad, "Manajemen Resiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Actave Allegro. Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013.," *Semin. Nas. Apl. Teknol. Inf.*, pp. 37–42, 2013.

[10] Susanti, D. Syamsuar, and Y. N. Kunang, "Manajemen Risiko Penerapan Teknologi Informasi Pada Universitas Bina Darma," no. September, pp. 380–385, 2018.

[11] Abdul Kadir, "Pengenalan Sistem Informasi Edisi Revisi," *Edisi Revisi*. 2014.

[12] S. Snedaker, *Business Continuity & Disaster Recovery for IT Professionals*. Syngress Publishing, Inc, 2007.

[13] S. Snedaker and C. Rima, *Business Continuity and Disaster Recovery Planning for IT Professionals: Second Edition*. 2013.

[14] A. R. Ahlan and Y. Arshad, "Information technology risk management: the case of the International Islamic University Malaysia," *J. Inf. Syst. Res. Innov.*, vol. 1, pp. 58–67, 2012, [Online]. Available: http://irep.iium.edu.my/32107/.

[15] J. B. Barney, *Gaining and sustaining competitive advantage*, vol. 104. 2002.

[16] M. Lallmahamood, "An Examination of Individual's Perceived Security and Privacy of

the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model," *J. Internet Bank. Commer.*, vol. 12, pp. 1–26, 2007.

[17] T. Pal, S. Brar, D. Sharma, and S. S. Khurmi, "Disaster Recovery and Business Continuity Planning for Electronic Banking : A Comparative Study," vol. 5976, pp. 64–71, 2015.

[18] K.-M. Osei-Bryson, H. Millar, A. Joseph, and A. Mobolurin, "Using formal MS/OR modeling to support disaster recovery planning," *Eur. J. Oper. Res.*, vol. 141, pp. 679–688, 2002, doi: 10.1016/S0377-2217(01)00275-2.

[19] B. W. Boehm, "Software risk management: Principles and practices," *Softw. Manag. Seventh Ed.*, pp. 365–374, 2007, doi: 10.1109/9780470049167.ch11.

[20] M. A. Rahman, R. Razali, and D. Singh, "A risk model of requirements change impact analysis," *J. Softw.*, vol. 9, no. 1, pp. 76–81, 2014, doi: 10.4304/jsw.9.1.76-81.