PENYUSUNAN DOKUMEN *DISASTER RECOVERY PLAN* UNIT IT XYZ MENGGUNAKAN *FRAMEWORK* NIST 800-34

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh:

NUR IRVAN RIZQI
H76219030

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA

2023

LEMBAR KEASLIAN

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini,

Nama : Nur Irvan Rizqi

NIM : H76219030

Program Studi : Sistem Informasi

Angkatan : 2019

Menyatakan bahwa saya tida melakukan plagiat dalam penulisan skripsi saya yang berjudul "**PENYUSUNAN DOKUMEN *DISASTER RECOVERY PLAN* UNIT IT XYZ MENGGUNAKAN *FRAMEWORK* NIST 800-34",** apabila suatu saat nanti terbukti saya melakukan tindakan plagiat maka saya bersedia menerima sanksi yang telah ditetapkan.

Dengan pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 27 Juni 2023

Yang Menyatakan,

(Nur Irvan Rizqi)

NIM. H76219030

LEMBAR PERSETUJUAN PEMBIMBING

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA : NUR IRVAN RIZQI

NIM : H76219030

JUDUL : PENYUSUNAN DOKUMEN *DISASTER RECOVERY PLAN* UNIT IT XYZ MENGGUNAKAN *FRAMEWORK* NIST 800-34

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 22 Juni 2023

Dosen Pembimbing 1	Dosen Pembimbing 2
Muhammad Andik Izzuddin, M.T	Prasasti Karunia Farista A, M.Kom, M.IM
NIP. 198403072014031001	NIP. 202111013

LEMBAR PENGESAHAN TIM PENGUJI SKRIPSI

PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi Nur Irvan Rizqi ini telah dipertahankan
di depan tim penguji skripsi
di Surabaya, 5 Juli 2023

Mengesahkan,

Dewan Penguji

Penguji I

Faris Mushlihul Amin, M.Kom
NIP 198808132014031001

Penguji II

Andhy Permadi, M.Kom
NIP 198110142014031002

Penguji III

Muhammad Anwik Izzuddin, M.T
NIP. 198403072014031001

Penguji IV

Prasasti Karunia Fursta A, M.Kom, M.IM
NIP. 202111013

Mengetahui,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr. Ahmad Saepul Hamdani, M.Pd
NIP.196507312000031002

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama	: Nur Irvan Rizqi
NIM	: H76219030
Fakultas/Jurusan	: Sains dan Teknologi / Sistem Informasi
E-mail address	: h76219030@uinsby.ac.id

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
■ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul : PENYUSUNAN DOKUMEN DISASTER RECOVERY PLAN UNIT IT XYZ MENGGUNAKAN FRAMEWORK NIST 800-34

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 14 Juli 2023
Penulis

(NUR IRVAN RIZQI)
nama terang dan tanda tangan

ABSTRACT

PENYUSUNAN DOKUMEN DISASTER RECOVERY PLAN UNIT IT XYZ MENGGUNAKAN FRAMEWORK NIST 800 34

Oleh:
Nur Irvan Rizqi

Unit IT XYZ merupakan instansi milik perguruan tinggi yang melayani tentang *Information Comunication and Technology (*ICT) dan bertugas menjalankan semua tentang teknologi informasi dan pengolahan data yang dibutuhkan di perguruan tinggi sehingga menjadi informasi yang tepat bagi mahasiswa dan dosen. Di dalam menjalankan proses operasionalnya terdapat beberapa ancaman atau bencana yang mengganggu pada layanan dan asset IT di Unit IT. Disaster Recovery Plan merupakan sebuah solusi bagi instansi ini untuk mencegah dan meminimalisir agar terus menjalankan proses operasionalnya.

Adapun tujuan dari penelitian ini adalah mengidentifikasi beberapa bencana yang terjadi serta merancang dokumen DRP dengan menggunakan framework NIST 800-34 sebagai alternatif pedoman ketika terjadi serangan sistem baik bencana alam sampai gangguan IT, DRP juga sebagai pedoman dalam memperbaiki kualitas sistem. Penyusunan DRP pada Unit IT XYZ melalui beberapa tahapan dimulai dari Risk Assesment dengan mengidentifikasi dan analisis resiko menggunakan metode QRA (*Quantitive Risk Analysis*), Melakukan analisa dampak bisnis dan melakukan Strategy Recovery sesuai pedoman *framework National Insitute Standart Of* Technology (NIST 800 34).

Hasil dari penelitian ini terdapat analisis yang diperoleh dari metode QRA bahwasanya jenis aset server yang mempunyai kerugian finansial tertinggi dengan nominal Rp.95.202.000. Serta jenis ancaman yang memiliki kerugian tertinggi sehingga mendapatkan pengendalian adalah gempa bumi dengan nominal Rp. 68.110.400 dan pada layanan IT terdapat 15 ancaman yang didapatkan setelah melakukan analisis risiko menggunakan QRA, ancaman tersebut dapat mengganggu layanan IT serta keberlangsungan proses operasionalnya hasil akhirnya pada penelitian ini yaitu dokumen DRP yang telah disesuaikan dengan kondisi internal di Unit IT XYZ.

Kata kunci: Disaster Recovery Plan, Strategi pemulihan, Metode Analisis kuantitatif Risiko, Framework NIST 800 34.

.

ABSTRACT

PREPARATION OF THE XYZ IT UNIT DISASTER RECOVERY PLAN DOCUMENTS USING THE NIST FRAMEWORK 800 34

By:
Nur Irvan Rizqi

The XYZ IT Unit is an institution belonging to a tertiary institution that serves Information Communication and Technology (ICT) and is tasked with carrying out all information technology and data processing needed in tertiary institutions so that it becomes the right information for students and lecturers. In carrying out its operational processes, there are several threats or disasters that disrupt IT services and assets in the IT Unit. The Disaster Recovery Plan is a solution for this agency to prevent and minimize it from continuing to carry out its operational processes.

The purpose of this study is to identify several disasters that occur and design DRP documents using the NIST 800-34 framework as an alternative guideline when a system attack occurs, both natural disasters and IT disruptions, DRP is also a guide in improving system quality. The preparation of DRP in the XYZ IT Unit went through several stages starting from Risk Assessment by identifying and analyzing risks using the QRA (Quantitive Risk Analysis) method, Conducting business impact analysis and carrying out Recovery Strategy in accordance with the framework guidelines of the National Institute Standard Of Technology (NIST 800 34).

The results of this study are the analysis obtained from the QRA method that the type of server asset has the highest financial loss with a nominal value of Rp. 95,202,000. As well as the type of threat that has the highest loss so that it gets control is an earthquake with a nominal value of Rp. 68,110,400 and in IT services there are 15 threats that are obtained after conducting a risk analysis using QRA, these threats can disrupt IT services and the continuity of the operational process. The end result in this study is DRP documents that have been adapted to internal conditions in XYZ IT Unit

Keywords: *Disaster Recovery Plan, Strategy Recovery, Metode Quantitativer Risk Analysis, Framework NIST 800 34*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam mengembangkan sebuah nilai suatu usaha, sebuah instansi wajib memiliki sumber daya yang esensial terutama dalam bidang teknologi informasi, dikarenakan teknologi informasi merupakan aset penting bagi perusahaan, maka daripada itu seluruh jajaran *stake holder* sampai *staff* perlu untuk merawat sebuah aset *information system* dengan serius dikarenakan menjadi tuntutan bagi perusahaan (Budiarto, 2017). Pada saat ini sangat banyak perusahaan yang bertumpu pada *information system* untuk menjalankan proses operasional atau bisnisnya termasuk sektor pengolahan data dan informasi yang ada di lingkup perguruan tinggi.

Unit IT adalah salah satu instansi milik perguruan tinggi XYZ yang melayani tentang *ICT (Information, Communications, and Technology)* dan bertugas menjalankan semua tentang teknologi informasi dan pengolahan data yang dibutuhkan di perguruan tinggi sehingga menjadi informasi yang tepat bagi mahasiswa dan dosen. Kegiatan sering dilakukan di Unit IT yakni menggunakan asset TI baik itu fisik maupun non fisik untuk mendukung pekerjaannya, Dalam proses kegiatan tersebut dapat terjadi suatu bencana tidak terduga yang dapat mengganggu proses operasional di Unit IT, Jika proses operasional terganggu maka akan berdampak pada layanan perguruan tinggi XYZ. Implementasi teknologi sistem informasi dikatakan berhasil apabila dapat melindungi asset IT dari suatu bencana atau gangguan dimana itu merupakan aset terpenting bagi instansi, Beragam cara atau upaya untuk mengurangi kerentanan tiada hentinya dilaksanakan, baik dalam hal teknis sampai efektifitas pengguna (Isa, 2018).

Salah satu upaya tersebut adalah mengeluarkan peraturan mengenai keamanan manajemen sistem informasi pada pasal 1 ayat 5 tahun 2016 yang berbunyi keamanan manajemen sistem informasi merupakan ketetapan untuk pelaksana sistem informasi dalam menerapkan pengamanan informasi berupa landasan dasar dari risiko yang dikeluarkan oleh kementerian komunikasi dan informatika. Selanjutnya pada ayat 6 yang berbunyi keamanan informasi dan data merupakan terjaminnya kerahasiaan, ketersediaan serta keutuhan. Berlandaskan peraturan tersebut maka menjadi hal wajib bagi instansi termasuk perguruan tinggi

untuk menerapkan manajemen risiko dan keamanan pada aset informasi. Dari beberapa serangan yang telah terjadi baik masalah *human cause* ataupun bencana alam, Unit IT belum mempunyai strategi atau dokumentasi tentang penanganan dan prosedur untuk menanggulangi dampak dari kerusakan. Sehingga perlu adanya sebuah dokumen mekanisme untuk mengurangi kerugian dari sebuah bencana (Daud, 2016). Di antara perencanaan untuk mengatasi permasalahan jika suatu sistem yang terdapat di Unit IT mengalami suatu keadaan kritis saat terjadinya bencana baik akibat *human cause* ataupun bencana alam yaitu dengan membuat dokumen *Disaster Recovery Plan* (DRP).

DRP merupakan dokumen yang digunakan kepada sistem yang telah mengalami serangan sehingga sistem itu menjadi sangat kritis. Pada saat ini di beberapa institusi perusahaan maupun perguruan tinggi belum menerapkan DRP mengingat pentingnya menjaga aset informasi dan data yang sifatnya sangat penting dan krusial. Adanya DRP pada instansi merupakan bentuk antisipasi dalam mengurangi keterlambatan dalam proses operasioanal layanan IT yang mengalami kerusakan atau kehilangan akibat bencana yang terjadi. DRP juga membantu proses pengambilan keputusan secara individual selama terjadi bencana . Dengan urgensi dan manfaat yang dimiliki DRP bagi instansi maka penyusunan DRP pada penelitian ini mengacu kepada kerangka kerja *(Framework)* NIST *(National Institute Of Standards and Technology)* 800-34 yang memuat acuan dalam merancang sebuah rencana dalam mengatasi bencanab . Rencana dalam menangani bencana diawali dengan mengelompokkan aset kritis paling mempengaruhi proses bisnisdi suatu instansi (Prabowo & Saputri, 2020). Kerangka kerja NIST 800-34 berfungsi sebagai petunjuk, pedoman pertimbangan dan rekomendasi dalam merancang suatu rencana kontigensi pada IT/IS. Rencana Kontingensi adalah tindakan sementara dalam memulihkan aset IT/IS yang saat itu dalam keadaan darurat. Peneliti menggunakan *Framework* NIST dikarenakan kerangka kerja yang tepat dalam memberikan pedoman serta dapat digunakan untuk instansi atau perusahaan dengan skala kecil sampai menengah serta dapat digunakan dalam menyusun DRP yang terdiri dari *Risk Assesment, Business Impact Analysis*, *Recovery Strategy* serta dokumentasinya (Agung, 2019). Tahapan dalam menyusun dokumen *DRP* yaitu dengan mengidentifikasi dan menganalisis penilaian risiko

menggunakan *Quantitative risk analys* (QRA) dengan tujuan mendapatkan beberapa jenis risiko yang mengancam pada Unit XYZ. lalu tahapan berikutnya adalah menentukan prioritas pemulihan dengan memerlukan *Business Impact Analysis* (BIA). Beberapa jenis risiko yang sudah di identifikasi sebelumnya serta prioritas pemulihan dapat membantu dalam pencegahan serta perencanaan kontingensi.

Berdasarkan penelitian terdahulu yang membahas terkait perancangan DRP dalam menggunakan Framework NIST 800-34 yang diteliti oleh (Isa, 2020) dimana dalam penelitian ini menghasilkan Business Impact Analysis yang ditinjau dari dampak *(impact)* yang dimiliki SIAK UMMI dari segi ancamannya pada fase ini menghasilkan beberapa sistem yang mempunyai dampak terbesar yakni pada sistem keuangan dengan presentasi 99% dan sistem yang mempunyai dampak terendah yakni pada sistem pedoman akademik dengan nilai presentasi 62% dan hasil penelitian didapatkan dokumen DRP yang berisi 9 *strategy recovery* untuk menghadapi ancaman yang terjadi di SIAK UMMI. Penelitian lain terkait perancangan DRP yakni diteliti oleh (Prabowo & Ramadhani, 2021)), penelitian ini disusun berdasarkan *framework* NIST 800-34 dengan beberapa tahapan didalamnya dari mulai identifikasi dan menilai risiko sampai pembuatan strategi kontingensi. Adapun perbedaan dengan penelitian kali ini yaitu mengidentifikasi dan menilai sebuah risiko menggunakan metode QRA serta menghasilkan dokumen *DRP* yang berisikan pedoman tahapan pemulihan serta tindakan yang dilakukan jika terjadi suatu bencana pada Unit IT perguruan tinggi XYZ. Dokumen ini telah disesuaikan dengan keadaan internal objek penelitiannya.

Dari latar belakang diatas menunjukkan adanya permasalahan yang ada di Unit XYZ dengan membutuhkan perancangan dokumen untuk digunakan ketika telah terjadi serangan sistem baik itu dari *human cause* atau bencana alam juga sebagai pedoman dalam memperbaiki kualitas sistem yang telah disesuaikan dengan kondisi internal di Unit XYZ. Untuk itu perlu adanya perancangan dokumen DRP menggunakan framework NIST 800-34 dengan mengacu beberapa tahapan didalamnya. Dengan demikian peneliti ingin mengangkat judul "**PENYUSUNAN DOKUMEN *DISASTER RECOVERY PLAN* UNIT IT XYZ MENGGUNAKAN *FRAMEWORK* NIST 800-34".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka disusun rumusan masalah dalam penelitian ini adalah " bagaimana cara mengidentifikasi aset dan risiko menggunakan metode QRA dan cara merancang dokumen DRP pada Unit XYZ menggunakan *Framework* NIST 800-34" ?.

1.3 Batasan Masalah

Demi penelitian ini dapat berjalan dengan melakukan ruang lingkup yang tidak melebar sesuai dengan cakupan permasalahan. Maka dibuat batasan masalah sebagai berikut :

1. Objek penelitian yang digunakan yaitu Unit XYZ yang menangani tentang teknologi sistem informasi diperguruan tinggi.
2. Pada aspek analisis risiko menggunakan metode *Quantitative risk analysis.*
3. Perancangan dokumen DRP pada Unit XYZ menggunakan Framework NIST 800-34 dengan beberapa tahapan didalamnya

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian yakni mengidentifikasi beberapa bencana atau ancaman menggunakan metode QRA serta merancang dokumen DRP *Disaster Recovery Plan* dengan menggunakan framework NIST 800-34 sebagai alternatif pedoman ketika telah terjadi serangan sistem baik itu dari *human cause* atau bencana alam juga sebagai pedoman dalam memperbaiki kualitas sistem yang telah disesuaikan dengan kondisi internal di Unit XYZ.

1.5 Manfaat Penelitian

1. Bagi akademik

a. Dapat dijadikan sumber referensi untuk penelitian

b. Dapat dijadikan pedoman dalam merancang dokumen *Disaster Recovery Plan* (DRP) menggunakan *Framework* NIST 800-34.

2. Bagi Unit IT Perguruan Tinggi XYZ

a. Dapat dijadikan pedoman untuk memperbaiki dan mengimplementasikan demi mencapai tujuan organisasi.

b. Dapat meningkatkan kepercayaan terhadap pengguna.

BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Penelitian Terdahulu

Untuk dapat memperoleh hasil penelitian yang tepat dalam pengerjaaan serta mendapatkan wawasan yang luas maka akan dilakukan tinjauan penelitian terdahulu yang telah disesuaikan dengan tema penelitian. Penelitian terdahulu dijadikan sumber referensi oleh penulis pada saat dilakukan penelitian. Dengan itu maka akan memperbanyak teori yang dikaji. Berikut jurnal yang akan dijadikan sumber referensi oleh peneliti yang dijabarkan pada tabel 2.1:

Table 2. 1 Penelitian Terdahulu

Judul	Hasil dan Metode	Korelasi dan Perbedaan Penelitian
Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi (Indra Griha Tofik Isa, 2020).	Penelitian ini menghasilkan Business Impact Analysis yang ditinjau dari dampak *(impact)* yang dimiliki SIAK UMMI. hasil penelitian didapatkan dokumen DRP yang berisi 9 *strategi recovery* untuk menghadapi ancaman yang terjadi di SIAK UMMI. Framework yang dipakai pada penelitian ini berpacu pada NIST 800-34	Pada penelitian ini sama menggunakan Framework NIST 800-34. Pada penelitian sekarang menggunakan objek Unit Teknologi Informasi dan melakukan sebuah proses penilaian menggunakan *Quantitative Risk Analys* (QRA).
Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301 (Ito Setiawan, dkk. 2019)	Penelitian ini tentang perancangan business continuity plan dan Disaster Recovery Plan dengan menjaga proses operasional bisnis agar investasi dapat terus berjalan jika layanan IT/IS mengalami gangguan akibat bencana yang, Metode yang digunakan dalam penelitian ini menggunakan ISO 22301. Hasil penelitian ini adalah sebuah perancangan business continuity plan dan Disaster Recovery Plan yang berlandaskan dengan	Pada penelitian ini sama-sama membuat dokumen disaster recovery plan. Perbedaan penelitian terletak pada framework yang digunakan pada penelitian sekarang menggunakan objek Unit Teknologi Informasi dan menggunakan framework NIST 800-34 fokus pada penelitian sekarang adalah menyusun dan mengacu pada aspek atau tahapan yang ada didalam NIST

	kerangka kerja yang dipakai dengan hasil clause 4 : context of the organization,clause 5 : leadership, clause 6 : planning, clause 7 : support	800-34 dan sampai terbuatnya dokumen DRP
Analisis Rancangan Disaster Recovery Plan Pada Industri Pertambangan Studi Kasus PT. Vale Indonesia,TBK (M. Noor Fuad, dkk. 2021).	Tujuan dari penelitian ini yakni menganalisis dan menerapkan hasil dari disaster recovery plan pada industri pertambangan. Metode yang digunakan adalah sistem snap mirror dan teknologi dari Netapp untuk menerapkan sistem backup data pada 2 server. Hasil penelitian ini menunjukkan pengiriman data antar server dibutuhkan waktu 118.7503041 per jam dengan bandwith sebanyak 22.51857618 mb	Pada penelitian ini membahas tentang dokumen disaster recovery plan. Penelitian ini membahas tentang analisis dan menerapkan sebuah recovery plan menggunakan teknologi dari netapp untuk menyimpan suatu data. Pada penelitian sekarang menggunakan objek Unit Teknologi Informasi dan menggunakan kerangka kerja NIST 800-34 dan fokus pada penelitian ini adalah pembuatan dokumen DRP
Structural and Operational Factors and Participation in Sustainable Disaster Recovery Programs: The Case of Bangladesh (Emadul Islam dan Haris Abd Wahab. 2020)	Penelitian menghasilkan rekomendasi untuk penguatan lokal dan nasional serta strategi untuk partisipasi bottom-up dalam program pemulihan bencana.. Selain itu, faktor yang berhubungan dengan jenis partisipasi masyarakat jatuh bervariasi sepanjang struktural, operasional, masyarakat, dan domain peserta. Temuan studi berpendapat bahwa untuk mempromosikan partisipasi bottom-up, Kolaborasi dan integrasi antar program pemulihan diperlukan untuk memperbaiki kebijakan yang ada atau mengadopsi kebijakan baru.	Pada penelitian ini sama-sama membuat dokumen disaster recovery plan. Pada penelitian sekarang menggunakan objek Unit Teknologi Informasi dan menggunakan kerangka kerja NIST 800-34 dan berfokus pada aspek penilaian dan sampai terbuatnya dokumen DRP
Rancangan Dokumen Disaster Recovery Plan Pada IT/IS Di Dinas XYZ (Zanuar Rifai, dkk. 2018)	Penelitian ini menghasilkan pedoman dokumen DRP untuk diimplementasikan ke Dinas XYZ dengan mengacu pada framework yakni NIST 800-34 dengan	Pada penelitian ini sama-sama menyusun dokumen Disaster Recovery Plan. Perbedaan penelitian ini menggunakan objek Unit Teknologi Informasi dan

	menggunakan pendekatan kualitatif.	melakukan sebuah proses penilaian menggunakan *Quantitative Risk Analys* (QRA)
Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode Quantitative dan Qualitative Risk Analysis	Pada penelitian ini menggunakan dua metode yakni Quantitative Risk Analys serta menggunakan Framework NIST 800 30 dengan hasil penelitian yang didapatkan Penyajian seluruh hasil analisis risiko dapat memberikan hasil rekomendasi risiko yang akan dikomunikasikan bersama manajemen IT kampus. Untuk kemudian dapat membantu pihak kampus dalam membuat sebuah keputusan yang memuat tentang kebijakan, prosedur, anggaran, operasi sistem, dan manajemen perubahan	Pada penelitian ini sama sama menggunakan metode QRA dalam menentukan ancaman. penelitian ini menyusun sebuah dokumen DRP dengan beberapa tahapan

Jika dibandingkan dengan penelitian terdahulu yang menggunakan beberapa Kerangka kerja seperti ISO 22301, metode sistem snap mirror teknologi dari Netapp dan Framework NIST 800-34 dengan beberapa tahapan untuk pembuatan DRP. Dari penelitian tersebut menghasilkan langkah-langkah untuk membuat DRP dengan berujuk dari beberapa framework yang digunakan salah satunya adalah NIST 800 -34. Namun dari penelitian mengenai framework NIST 800-34 belum ada penelitian yang melakukan identifikasi dan penilaian risiko menggunakan *Quantitative Risk Analyst* (QRA) guna memperoleh jenis risiko dengan potensi paling mengalami dampak kerugian pada aset IT yang ada di Unit XYZ. Lalu langkah berikutnya adalah memastikan aset IT yang paling mengancam untuk dipulihkan terlebih dahulu dengan menggunakan *Business Impact Analysis* (BIA), dengan adanya analisis ini maka pola risiko dalam prioritas layanan untuk pemulihan menghasilkan rencana. Selanjutnya rencana ini akan disempurnakan dengan beberapa tahapan yakni tahap rekonstruksi, aktivasi dan pemulihan.

2.2 Landasan Teori

2.2.1 Pengertian Bencana

Bencana merupakan suatu ancaman yang tidak mungkin bisa diprediksi bilamana akan terjadi, baik bencana alam maupun non alam. Pemicu bencana ini beragam seperti halnya bencana alam yang disebabkan oleh faktor alam seperti tsunami, banjir, longsor, dst. Bencana non alam seperti ancaman yang bersumber dari alat yang digunakan atau bersumber dari faktor manusia. Risiko dari bencana yang disebabkan akan berdampak kerugian pada keberlangsungan proses bisnis dengan level dampak yang berbeda pula, baik berlangsung cepat atau lama (Nasution, 2020). Berikut ini akan menjelaskan bencana sesuai dengan penyebab yang terjadi:

Table 2. 2 Jenis Bencana

Bencana	Penyebab Yang Terjadi
Natural (alami)	Bencana yang disebabkan oleh reaksi alam seperti tsunami, banjir, angin,dst.
Human (Manusia)	Bencana yang disebabkan oleh manusia, seperti serangan hacker, pembajakan, dst.
Environment (Lingkungan)	Bencana yang disebabkan oleh faktor lingkungan yang terlibat, seperti jaringan rusak, sistem mengalami error, kesalahan alat yang digunakan.

2.2.2 Serangan Pada IT/IS

Menurut Lestari (2018) di dalam bukunya yang berjudul *Komunikasi Bencana Aspek Penting Pengurangan Resiko Bencana* mendeskripsikan bahwa gangguan atau serangan yang disebabkan dari bencana Teknologi Informasi merupakan semua peristiwa yang disebabkan oleh kelalaian pada pengoperasian, kecerobohan atau kesengajaan manusia dalam pemakaian teknologi yang bisa akibatkan kerusakan pada komponen penting, kebocoran data, Dll. Penerapan TI/IS pada sebuah instansi pada sekarang ini merupakan aspek yang sangat penting dikarenakan dapat membantu pekerjaan setiap pengguna. Di Dalam penggunaanya IT/IS dapat mengakibatkan terjadinya suatu bencana atau resiko. Resiko yang di

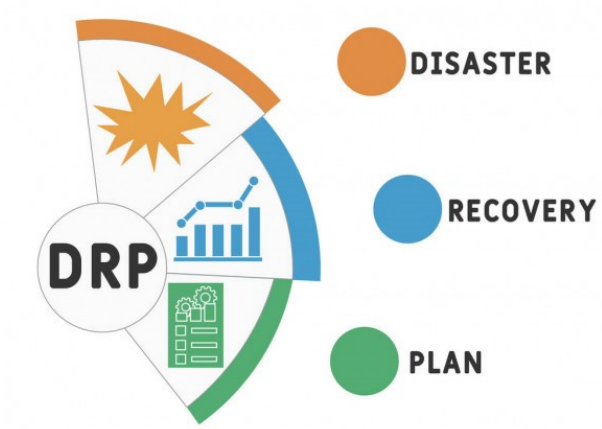
maksud merupakan aset IT. bencana yang timbul dari IT akan berakibatkan berhentinya suatu operasional proses bisnis

2.2.3 Manajemen Keamanan Informasi

Menurut Bahrudin & Firmansyah (2018) manajemen keamanan informasi merupakan suatu prinsip untuk mengatur segala sesuatu yang berhubungan dengan pengelolaan aset informasi secara efektif dengan tujuan menjamin keamanan aset yang dimiliki. Sistem informasi adalah suatu aset yang berharga bagi instansi. Aset IS/IT dapat berupa data, layanan, dokumen dan informasi. Manajemen keamanan informasi merupakan bagian dari prinsip manajemen risiko yang mana bertujuan untuk mengidentifikasi, merawat serta mengurangi risiko yang ada pada aset IT.

Keamanan informasi merupakan usaha dalam melindungi aset IT dari segala ancaman baik itu serangan sampai bencana, secara tidak langusng keamanan informasi ikut memastikan proses keberlangsungan bisnis sampai mengoptimalkan laba atas investasi selain itu manajemen keamanan informasi turut menjaga proses operasional bisnis instansi agar tetap berjalan saat terjadinya suatu bencana atau serangan pada sistem keamanan. Fase pada manajemen keamanan informasi yang harus dijalankan yakni mengidentifikasi ancaman apa saja yang mungkin berdampak pada sumber daya lalu mengidenfikasi risiko yang disebabkan oleh ancaman tersebut setelah diidentifikasi langkah selanjutnya adalah menentukan kebijakan keamanan informasi yang akan digunakan fase terakhir yakni mengimplementasikan semua kebijakan untuk meminimalisir semua risiko yang akan terjadi.

2.2.4 *Disaster Recovery Plan (DRP)*



Gambar 2. 1 Pengertian *Disaster Recovery Plan*

(Sumber : *Ehacking.net*)

Menurut Disaster Recovery Plan merupakan solusi untuk melindungi aset data dan infrastruktur yang dikelola dengan tujuan proses operasional berjalan dengan selayaknya (Wicaksono, 2008). DRP adalah sebuah rencana yang berpusat pada IT/IS yang dibuat agar bisa memulihkan operasi sistem, aset IT, aplikasi, Fasilitas komputer saat keadaan kritis (Swanson et al., 2010).

DRP merupakan suatu dokumen yang menjelaskan tentang segala tindakan dan tahapan yang perlu dilakukan oleh setiap *stakeholder* sampai *Staff* guna melindungi aset IT yang paling berharga(Daud, 2016). DRP disusun sesuai kebijakan dan prosedur untuk mempersiapkan pemulihan serta melindungi layanan yang bermasalah setelah terjadinya suatu bencana (Snedaker, 2013). DRP merupakan suatu bentuk dari *Business Continuity* yang merupakan kegiatan yang dilaksanakan suatu instansi dalam menjamin sebuah fungsi dari sebuah bisnis yang kritis tetap ada bagi pelaku bisnis itu sendiri (Santoso & Dirgantara, 2017).

NIST (*National Institute Of Standards and Technology*) memaparkan bahwa rencana kontingensi dibagi beberapa macam. Salah satu diantaranya adalah DRP (*Disaster Recovery Plan*) yang berisikan tentang bagaimana tanggapan *Stakeholder* serta persiapan apa saja yang dilakukan ketika bencana terjadi. Didalam proses penyusunan DRP ada beberapa tahapan yang harus dilakukan yakni dimulai dari

sebuah analisis, plan serta penyusunan DRP sendiri. Beberapa kejadian yang terjadi dari suatu bencana yang dapat merusak semua peralatan dan aset IT lainya akan menimbulkan berhentinya suatu proses bisnis yang dijalankan. Jika kegiatan proses bisnis terus berhenti maka akan mengakibatkan kerugian yang sangat besar. Dampak jika terjadi kerusakan pada aset IT beragam tergantung sebuah instansi memerlukan Teknologi informasi yang diterapkan.

2.2.5 *Framework NIST 800 34*

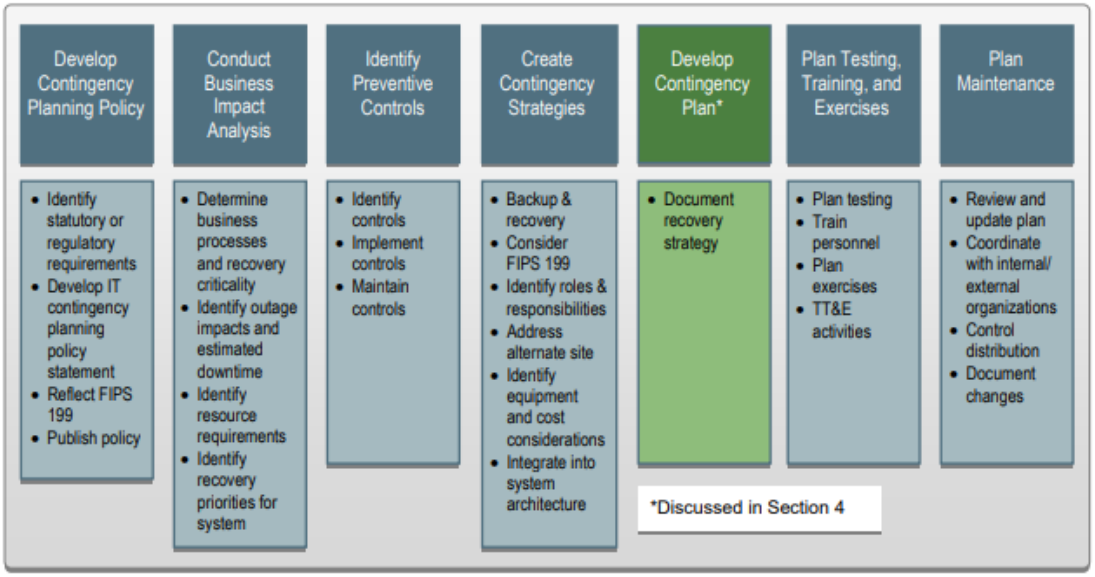
Framework NIST 800 34 yang dirilis oleh *National Institute Of Standards and Technology* merupakan *framework* yang berisikan pedoman dalam merancang dokumen DRP*(Disaster Recovery Plan*) atau *contingency plan.* Fokus framework ini yaitu pada penyusunan kontingensi berisikan tahapan tahapan yang dilakukan terlebih dahulu ketika saat terjadinya bencana, Tindakan awal seperti memindahkan layanan operasional ke lokasi alternatif atau dilakukan secara manual dengan membuat rencana kontijensi. Pada Framework NIST 800 34 memuat beberapa prosedur yang wajib dilaksanakan jika akan merancang dokumen DRP. Prosedur tersebut diantaranya adalah *Business Impact Analysisis* (BIA) dan *Business Continuity Plan* (BCP) Aspek beberapa tahapan dalam *Framework* NIST 800-34 sampai menghasilkan dokumen DRP dapat dilihat pada gambar 2.2:

Gambar 2. 2 Framework NIST 800-34

(Sumber : NIST 800 -34 *Framework*)

Langkah atau tahapan ini merupakan elemen penting untuk menyusun rencana kontingensi sistem informasi yang menyeluruh ke semua aspek. Didalam

mengembangkan sebuah perencanaan kontinjensi serta menjalankan BIA langkah yang tepat adalah menyelesaikannya terlebih dahulu sebelum dikategorikan sesuai kebutuhan internal. Pengembangan rencana merupakan aspek penting dari perencanaan kontingensi sistem informasi. semua organisasi yang ada kaitanya dengan sistem informasi harus mempunyai rencana kontingensi yang merupakan suatu tindakan yang bersifat sementara untuk memulihkan suatu aset atau infrastruktur sistem informasi yang pada saat itu dalam keadaan darurat. Berikut merupakan ilustrasi proses perencanaan kontingensi yang akan dijelaskan pada gambar 2.3:



Gambar 2. 3 Ilustrasi Proses rencana kontingensi

(Sumber : NIST 800 -34 Framework)

2.2.6 *Business Impact Analysis*

Aspek Business Impact Analysis (BIA) pada perencanaan kontingensi pada implementasinya digunakan untuk mengevaluasi proses krusial yang ada pada komponen aset IT serta untuk menentukan waktu pemulihan, prioritas pemulihan, Resource dengan ketergantungannya(Muhaemin, 2018). Tujuan utama dari aspek Aspek *Business Impact Analysis* (BIA) yakni untuk mengidentifikasi dampak jika layanan pada aset IT tidak serta menggunakan hasil dari BIA guna untuk menentukan prioritas pada pemulihan Aset IT.

Business Impact Analysis (BIA) berwenang melihat dampak yang terjadi pada aset sistem informasi dalam mendukung keberlangsungan proses bisnisnya. Yang mana ada 3 tahapan utama dalam pelaksanaan BIA yakni

a) Menentukan Proses bisnis yang akan dianalisis
b) Mengidentifikasi Resource IT
c) Mengindetifikasi level tingkatan untuk pemulihan atau Resource utama dalam pemulihan TI

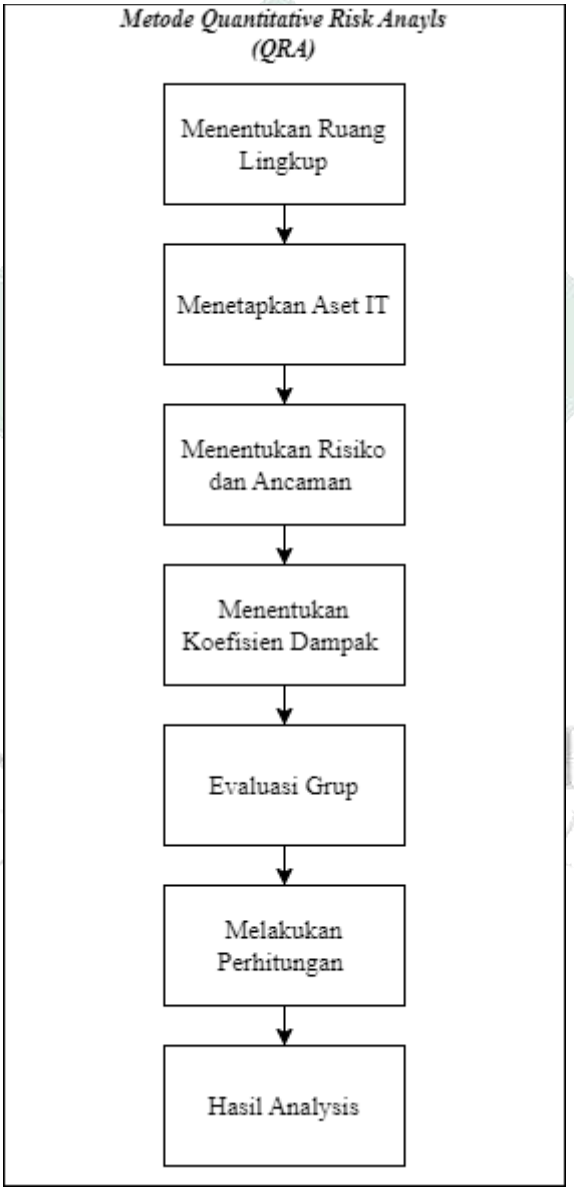
Hasil dari *Business Impact Analysis* (BIA) sendiri di implementasikan oleh suatu instansi untuk mengukur suatu dampak dari kerusakan pada area bisnis disuatu instansi dan menentukan kebutuhan pada operasional bisnis dan menentukan prioritas utama terhadap sistem yang penting dan fungsioanal bisnis yang segera di pulihkan jika bencana terjadi (Rubil, 2012).

2.2.7 *Risk Assesment*

Risk assessment masuk kedalam aspek atau tahapan dari penerapan manajemen risiko. Manajemen risiko sendiri merupakan ancaman yang mungkin dapat mengancam sensibilitas pada suatu aset yang berakibatkan rusak sampai kerugian pada suatu instansi. Tujuan manajemen risiko adalah mengidentifikasi resiko apa terjadi dan bagaimana dampak terhadap proses bisnis serta memberikan beberapa strategi yang akan meminimalisir resiko yang terjadi. Fungsi dari *Risk Assessment* sendiri adalah mengetahui sejauh mana tingkatan resiko yang dapat mengancam aset penting dalam membentuk sebuah strategi *Business Continuity Management* (BCM) *Risk Assessment* bertujuan guna melihat representasi dari dampak yang terjadi oleh instansi jika benar ancaman itu terjadi yang berakibat kegagalan atau berhentinya suatu proses bisnis (Isa, 2020). Risk Analysis merupakan tahapan pemahaman dari sebuah risiko serta menetapkan level risiko jika dapat terjadi. Didalam melakukan tahapan ini ada hal yang perlu di tinjau kembali yakni dalam hal sumber penyebab dan level keseriusan (*Saverity)* sebuah instansi dapat melakukan pengelompokan suatu bencana dari sebuah waktu salah satu metode yang dilakuakan dalam risk asessment, yakni:

2.2.8 *Metode Quantitative Risk Analys (QRA)*

Analisis risiko kuantitatif bertujuan untuk menetapkan sasaran independen nilai moneter untuk komponen penilaian risiko dan melihat dampak dari potensi kerugian dari bisnis yang mana dijadikan acuan dalam melakukan analisa dampak bisnis. menurut (Meritt, 2000) menjelaskan mengenai alur untuk QRA penjelasan alur sebagai berikut:



Gambar 2. 4 Tahapan Metode *Quantitative Risk Analys*

(*Sumber* : J.W. Merrit 2000)

A. Menentukan ruang lingkup, dalam tahapan ini perlu memperhatikan 2 hal yakni menentukan objek yang akan di evaluasi dan pengumpulan data.
B. Menetapkan Aset IT. Menentukan segala harga dari setiap aset dengan disesuaikan tipe dan model yang akan dianalisis dari aset yang dimiliki
C. Menentukan risiko dan ancaman. Membuat dan mengidentifikasi prioritas sumber ancaman
D. Menentukan koefisien dampak. Menganalisis kerentanan suatu aset terhadap risiko.
E. Evaluasi grup. Membahas ancaman apa saja yang paling impact pada aset IT
F. Melakukan Perhitungan. Menghitung dampak dari kejadian yang menyebababkan kerugian dengan menggunakan *Single Loss Expectancy* (SLE) dan *Annualized Loss Expectancy* (ALE)
G. Hasil Analisis. Hasil tersebut nantinya akan dibuat strategy recovery.

2.3 Integrasi Keilmuan

Penyusunan Dokumen *Disaster Recovery Plan* (DRP) berdasarkan Framework NIST 800 34 pada Unit IT yang terdapat di perguruan tinggi XYZ. Tujuan dilakukan penelitian ini adalah menyusun dokumen DRP yang berguna sebagai alternatif pedoman ketika terjadinya suatu bencana baik itu yang disebabkan dari *Human Cause* atau bencana alam seperti banjir, tsunami, longsor, dst. Berdasarkan kalimat yang telah disampaikan beliau Dr. Sanuri, S.Ag., M.Fil.I. selaku Ketua Prodi program Doktoral Ilmu al Qur'an dan tafsir di Universitas Islam Negeri Sunan Ampel Surabaya melalui wawancara yang diilaksanakan pada tanggal 2 Februari 2023 bahwasanya menurut pandangan islam mengenai penyusunan dokumen DRP sebagai alternatif pedoman ketika terjadinya suatu bencana dengan tujuan menolong atau membantu semua yang rusak karena bencana agar pulih kembali dengan ini ada kaitannya dengan ayat Al Qur'an yang berbunyi:

وتَعَاوَنُوْا عَلَى الْبِرِّ وَالتَّقْوٰىۖ وَلَا تَعَاوَنُوْا عَلَى الْاِثْمِ وَالْعُدْوَانِۚ وَاتَّقُوا اللّٰهَۗ اِنَّ اللّٰهَ شَدِيْدُ الْعِقَابِ

Artinya:

“ Saling tolong menolonglah kamu dalam hal melaksanakan kebajikan dan taqwa. Dan janganlah kamu saling tolong menolong dalam hal perbuatan dosa dan permusuhan. Bertaqwalah kepada Allah SWT. Sesungguhnya Siksaan Allah SWT sangat pedih “.(Q.S Al Maidah Ayat 2)

Manusia merupakan makhluk sosial yang tidak dapat memenuhi kebutuhannya sendiri dan pasti akan bergantung dengan orang lain. Maka dengan itu terciptalah peran atau sikap saling tolong menolong agar bertujuan meringankan kesulitan yang dialami oleh manusia. Sebagaimana yang dilakukanya penelitian ini yakni bertujuan untuk menyusun dokumen DRP guna untuk memulihkan suatu objek tertentu jika terjadi bencana.

Pada konteks tolong menolong dalam hal Taqwa dapat diartikan berupa orang yang menyesedekahkan waktunya dalam keadaan lapang maupun sempit. Dengan konteks tersebut ada kaitannya juga dengan ayat al qur’an yang berbunyi :

ٱلَّذِينَ يُنفِقُونَ فِى ٱلسَّرَّآءِ وَٱلضَّرَّآءِ وَٱلْكَٰظِمِينَ ٱلْغَيْظَ وَٱلْعَافِينَ عَنِ ٱلنَّاسِ ۗ وَٱللَّهُ يُحِبُّ ٱلْمُحْسِنِينَ

Artinya : Orang yang menafkahkan atau mensedekahkan harta atau waktunya, baik dalam keadaan lapang maupun sempit dan orang yang menahan amarahnya dan memaafkan kesalahan orang lain. Sesungguhnya Allah SWT sangat menyukai orang yang berbuat kebajikan. (Q.S Ali imran Ayat 134)

Dalam Orientasi Ayat tersebut ketaqwaan seseorang diukur dalam kesholehan sosial masyarakat. Sebagaimana yang dilakukan penelitian kali ini Tim yang mensenggangkan waktunya untuk menyusun dokumen DRP guna membantu sosial masyarakat terkhusus Unit IT XYZ dalam memulihkan jika terjadi suatu bencana yang tentunya masuk kedalam prinsip sosial manusia, barang siapa yang menyelamatkan satu manusia sama dengan menyelamatkan manusia sedunia.

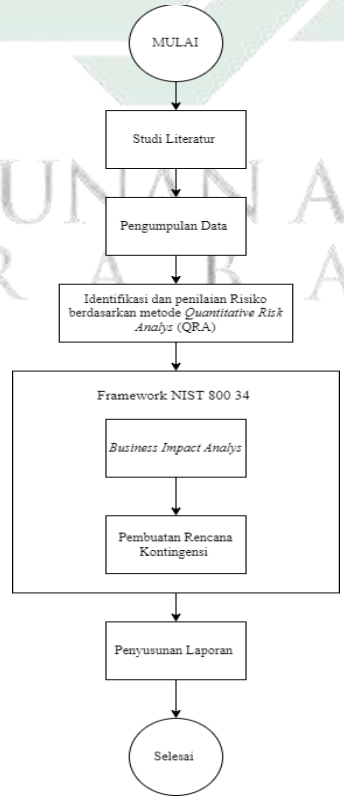
BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Pada penelitian ini menggunakan metode *quantitative* dan *qualitative risk analys*, sebagaimana disampaikan oleh (Muslim, 2018) bahwasanya penggunaan metode *quantitative risk analysis* adalah sebuah cara dalam menganalisis risiko dengan nilai atau angka untuk meningkatkan efektivitas dan probabilitas sedangkan penggunaan metode *qualitative risk analys* yaitu menggunakan *framework* NIST 800-34, pedoman ini dapat digunakan untuk menghasilkan dokumen di unit IT XYZ. Penelitian ini menerapkan dua metode dengan harapan menemukan hasil analisis risiko dengan tepat..

3.2 Tahapan Penelitian

Tahapan penelitian berupa diagram alur atau kerangka penelitian. Tahapan penelitian dibuat berdasarkan tinjauan teori yang sudah dijelaskan. Penjelasan alur penelitian dijelaskan pada Gambar 3.1:



Gambar 3. 1 : Tahapan Penelitian

3.2.1 Studi Literatur

Pada tahapan Studi Literatur Menurut (Fitrah, 2018) dalam melakukan studi literatur peneliti harus memperhatikan konsep penelitian dengan baik, karena hasil dari studi literatur dapat menghasilkan nilai dengan memperoleh ide yang mendukung dalam penelitian serta memperoleh banyak informasi tentang hasil dan metode yang mempunyai korelasi dengan penelitian yang dilaksanakan.Pada tahapan ini. Peneliti akan mencari beberapa sumber referensi baik itu berupa buku, dokumen, jurnal dan artikel yang nantinya akan dikaji ulang sesuai dengan permasalahan dan topik penelitian.

3.2.2 Identifikasi dan Analisis Risiko Berdasarkan *Quantitative Risk Analys* (QRA)

Pada tahapan ini merupakan langkah dalam menentukan potensi risiko yang akan terjadi dan mengancam beberapa aset IT di Unit XZY. Pada proses identifikasi risiko dapat diilihat dari ancaman *(Threat)* dan kelemahan *(vulnerability)* pada aset IT dan layanan pendukungnya. Selain melakukan identifikasi perlu untuk menganalisis sebuah risiko.

Risk anaylsis juga dilakukan sebagai parameter untuk menilai suatu tingkat resiko yang akan terjadi di Unit XYZ. Risiko tersebut akan dianalisis serta dinilai menggunakan parameter tingkat seberapa bahaya yang disebabkan dari bencana yang terjadi. *QRA* pada saat ini banyak dipakai dalam mengukur risiko pada Aset IT. Berikut tahapan yang metode QRA :

3.2.2.1. Menentukan Ruang Lingkup

A. Menentukan Objek Penilitian

Menentukan objek secara tepat untuk dilakukan analysis risiko. Dalam penelitian ini objek yang digunakan adalah Unit IT Perguruan Tinggi XYZ. Dengan alasan Unit IT ini belum adanya suatu analisis risiko untuk membuat *strategi recovery.*

B. Pengumpulan Data

Pada tahapan ini peneliti melakukan beberapa tahapan dari metode atau cara untuk mengumpulkan data antara lain pengamatan secara langsung atau observasi pada objek yang di teliti yakni Unit XYZ dengan melakukan tahapan wawancara terhadap Tim atau Staff IT yang ada di Unit XYZ. Pengumpulan Data yang

digunakan untuk penelitian diperoleh dari unit IT yang ada pada perguruan tinggi dikawasan kabupaten bojonegoro, Nama perguruan tinggi bersifat rahasia dikarenakan pada penelitian ini difokuskan pada pembahasan ancaman dan risiko IT terhadap asset di perguruan tinggi itu sendiri, Data yang diperoleh nantinya merupakan data yang reliabel dan dapat dihitung hasilnya, sumber data yang diperoleh melalui proses wawancara dengan kepala unit IT serta beberapa sumber dokumen seperti buku inventaris asset IT

Pada tahapan observasi Menurut (Sari et al., 2022) observasi merupakan teknik dalam pengumpulan data yang memiliki identitas yang berbeda dengan teknik pengumpulan data yang lain seperti kuisoner atau wawancara. Observasi digunakan apabila penelitian yang dilaksanakan berhubungan langsung dengan manusia, proses bisnis, segala gejala alam dan apabila responden yang akan dilakukan penelitian tidak telalu banyak. Pada tahapan observasi peneliti melakukan pengamatan secara langsung bagaimana pengguna menggunakan sistem atau aset IT yang ada di Unit XYZ dan standart operasioanal apa saja yang dilakukan dalam menggunakan sistem data. Serta bagaimana pengguna ini melakukan tindakan jika terjadi suatu serangan atau bencana. Hasil dari tahapan ini nantinya akan dijadikan acuan juga untuk tahapan analisis.

Pada tahapan wawancara. Peneliti melaksanakan wawancara langsung dengan staff atau pihak yang berkepentingan langsung dengan aset IT yang dimiliki oleh Unit XYZ. Dalam wawancara kali ini peneliti tentunya akan mengajukan beberapa pertanyaaan contoh seperti bagaiamana berjalannya proses sistem IT pada Unit XYZ dan Apakah pernah ada upaya yang pernah dilakukan jika terjadi suatu bencana baik itu diakibatkan oleh *human cause* atau bencana alam dan tindakan seperti apa yang diambil dalam meminimalisir jika terjadi suatu bencana tersebut. Selanjutnya dari hasil data yang diperoleh akan digunakan proses analisis menggunakan metode QRA.

3.2.2.2. Menetapkan Aset

Penetapan aset harus dilakukan dengan tujuan untuk mengetahui aset IT beserta nominal harga. Jumlah aset yang digunakan dalam metode ini adalah aset yang terbaru yakni pada periode 2021-2023. Penetapan aset ini dilakukan dengan menentukan harga yang disesuaiakan dengan tipe dan model aset IT. Penentuan

harga kali ini didapatkan dari laporan pengadaan barang aset atau layanan IT pada periode 2021-2023 yang ada di Unit IT Perguruan Tinggi XYZ.

3.2.2.3. Menentukan Risiko dan ancaman

Menentukan risiko dan ancaman bertujuan untuk menentukan prioritas utama sehingga dapat mengetahui dampak dari terjadinya bencana yang mengakibatkan aset atau layanan IT rusak atau hilang. Penentuan risiko berdasarkan kategori yang dikemukakan oleh (Meritt, 2000) yang membuat 15 kategori ancaman antara lain:

Table 3. 1 Kategori Ancaman Menurut (Meritt 2000)

No	Ancaman	Penjelasan
1	Kehilangan daya	Jika kehilangan daya pada sistem informasi yang digunakan akan berdampak pada gangguan pada fungsi aset atau layanan IT
2	Kehilangan Komunikasi	Jika kehilangan komunikasi maka ancamannya yakni tidak bisa mentransfer sistem ke sistem lainnya
3	Kehilangan integritas data	Jika integritas data hilang maka akan mengancam suatu keabsahan data sehingga akan berdampak kerugian besar bagi Instansi.
4	Kesalahan tidak sengaja	Penyalahgunaan asset TI tidak adanya niatan jahat, akan tetapi kesalahan dalam penggunaan system sehingga mengakibatkan kerugian bagin instansi
5	Virus Computer	Akan mengancam penyerangan virus pada komputer yang digunakan
6	Penyalahgunaan hak akses	Ancaman yang dilakukan oleh karyawan terhadap penyalahgunaan akses
7	Bencana alam	Ancaman ini terjadi karena tidak terduga yakni seperti banjir,petir,angin yang dapat merusak aset IT
8	Usaha orang luar untuk mengakses sistem	Ancaman yang dilakukan oleh pihak selain karyawan untuk masuk kedalam sistem
9	Pencurian dan penghancuran aset dan layanan IT	Dilakukan oleh pengguna yang tidak mempunyai akses
10	Penghancuran data	Ancaman dapat merusak informasi atau daya yang dimiliki oleh perusahaan
11	Penyalahgunaan hak akses oleh pengguna lain	Ancaman dari pengguna lain dapat menyebabkan sistem dapat disalah gunakan
12	Pihak luar yang berhasil mengakses sistem	Ancaman dari orang luar meliputi pengguna yang tidak sah yang berhasil masuk sistem atau yang disebut hacker

13	Penghentian proses tanpa bencana	Ancaman informasi ketika saat system atau layanan tidak tersedia untuk digunakan tetapi bukan disebabkan oleh bencana.
14	Kebakaran	Dapat terjadi dimanapun kapanpun
15	Gempa Bumi	Bencana alam yang dapat merusak banyak aset IT

3.2.2.4. Menentukan koefisien dampak

Didalam menentukan koefisiensi dampak maka dibutuhkan tahapan identifikasi yang mana aset IT mempunyai beberapa kerentanan pada risiko atau tidak. Penentuan kali ini dilakukan pemilihan dampak dari pada Aset IT berdasarkan tingkat ancaman *(Threat)* dan kelemahan *(vulnerability)* pada aset IT dan layanan pendukungnya. Analisa kerentanan pada aset IT dilaksanakan agar mengetahui prioritas potensi kehilangan atau kerusakan pada aset IT yang disebut *exposure factor* dengan melihat nilai persentase akibat ancaman terhadap aset IT yang menyebabkan kehilangan atau kerusakan. Penentuan koefisien dampak kali ini berdasarkan wawancara yang diperoleh dari hasil wawancara dengan pihak berkepentingan dalam aset IT.

Menurut (Meritt, 2000) penentuan koefisien dampak untuk mengetahui tingkat kerentanan pada aset IT. Merrit membuat nilai koefisien dampak agar mengetahui *exposure factor* yang akan dijelaskan pada tabel 3.2 :

Table 3. 2 Koefisien Dampak

Nilai	Penjelasan
0	Aset IT tahan akan kerusakan yang diakibatkan oleh ancaman
0,3	Tid ak ada kerusakan yang disebabkan oleh ancaman akan tetapi ada kemungkinan membutuhkan penggantian total
0,5	Kemungkinan tidak mengalami kerusakan terhadap aset IT
0,7	Aset IT yang mengalami kerusakan akan membutuhkan penggantian
1	Hasil yang bisa diidentifikasi perlu penggantian secara total pada aset IT.

3.2.2.5. Evaluasi kelompok

Pada tahapan kali ini dilakukan dengan mengulas ancaman *(threat),* koefisien dampak serta jenis aset IT yang sudah diidentifikasi beserta harga, risiko

dan dampak dari risiko tersebut. Kelompok pada tahapan ini terdiri dari orang yang berkepentingan pada aset IT serta layanannya.

3.2.2.6. Perhitungan

Pada tahapan perhitungan dengan melakukan analisis dampak yakni perhitungan terkait dampak dari kejadian gangguan keamanan berupa *Single Loss Expectancy* (SLE) dan *Annualized loss Expectancy* (ALE). Dalam menentukan *Annualized Rate of Occurrence* (ARO) yakni Perkiraan frekuensi ancaman akan terjadi dalam satu tahun dan dicirikan setiap tahun sebagai contoh : Ancaman yang terjadi sekali dalam 10 tahun memiliki ARO 0,1 dan ancaman yang terjadi 10 kali dalam setahun memiliki ARO 10.

1) *Single Loss Expectancy* (SLE) = Aset Value × Exposure Factor (EF)
   Sebagai contoh : SLE = Rp. 40.233.200 × 0,3 = Rp.12.069.960
   Keterangan:
   a. SLE = Nilai moneter yang akan hilang pada satu kali kejadian serangan keamanan aset IT.
   b.Nilai aset : Total harga dari item aset IT
   c. *Exposure Factor* (EF) = Factor dengan melihat nilai persentase akibat ancaman terhadap aset IT yang menyebabkan kehilangan atau kerusakan. Nilai EF didapatkan dari hasil wawancara dengan menyesuaikan tabel yang disusun oleh J.W. Merrit.
2) *Annualized Loss Expectancy* (ALE) = SLE ×ARO
   Sebagai contoh , ALE = Rp. 12.069.960 × 0,3 = Rp.3.620.988
   Keterangan :
   a. ALE = nilai moneter yang hilang dikarenakan terjadin gangguan terhadap Aset IT pada jangka waktu satu tahun
   b. SLE = nilai moneter yang akan hilang pada suatu kali kejadian serangan keamanan aset IT.
   c. *Annualized Rate of Occurance* (ARO) = Frekuensi perkiraan ancaman yang terjadi dalam satu tahun dan dicirikan setiap tahun sebagai contoh ancaman yang telah terjadi satu kali dalam 10 tahun mempunyai nilai ARO 0,1 sedangkan ancaman yang telah terjadi dalam waktu 10 kali

dalam setahun mempunyai nilai ARO 10. Penentuan nilai ARO didapatkan dari hasil wawancara dengan informan yang berkompenten di bidang IT di Unit IT perguruan tinggi XYZ.

3.2.2.7. Hasil Analysis

Tahapan ini merupakan fase analisis yang bertujuan guna menentukan aset IT dan risiko yang berdampak pada kerugian. Pada tahapan ini menggunakan 2 metode yakni *analysis across asset* dan analysis risk asset. *analysis across asset* menerapkan dengan menjumlahkan nilai dampak masing-masing aset IT. Pada *analysis risk* asset diterapkan dengan menjumlahkan nilai dampak masing masing risiko. Selanjutnya, Peneliti menentukan waktu pemulihan ancaman dan risiko. Maka dilakukan dengan menggunakan hasil dari analisis risiko dengan metode *QRA.* Untuk menentukan waktu pemulihan ancaman dan risiko mana yang harus di tentukan maka dilakukan pembobotan nilai dengan mengukur 3 aspek atau indikator, pembobotan nilai yakni *Likelihood, Restoration Time* dan *Predictablitity* yang secara jelas dapat dilihat pada tabel 3.3 dan 3.4. :

Table 3. 3: Penjelasan dari *Likelihood, Restoration Time* dan *Predictablitity sumber (Isa, 2020)*

No	Keterangan	Penjelasan
1	*Likelihood (0-11)*	Nilai yang sangat tinggi akan melihatkan bahwa ancaman atau resiko dari bencana yang akan terjadi sangat tinggi pula.
2	*Restoration Time (0-11)*	Nilai yang sangat tinggi akan melihatkan bahwa semakin sangat lamanya waktu yang diperlukan untuk memulihkan aset IT.
3	*Predictablitity (0-3)*	Nilai yang sangat tinggi akan melihatkan bahwa semakin susahnya memprediksi akan terjadinya ancaman, sehingga akan sangat sedikit waktu yang digunakan untuk mengindarinya.

Table 3. 4: Penjelasan Rinci *Likelihood, Restoration Time* dan *Predictablitity sumber (Isa, 2020)*

NO	Kolom		
	Likelihood	***Restoration Time***	***Predictability***
0 dan 1	Tidak Akan Terjadi	Tidak Tersedia	Bisa diprediksi dengan jelas bahkan sebelum datangnya bencana
2	Terjadi Lebih dari 5 Tahun sekali	1-4 menit	Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah
3	Terjadi 2-5 tahun sekali	5 Menit – 1 Jam	Prediksi bisa dilakukan setelah ada tanda tanda bencana
4	Terjadi 1-2 tahun	1-6 jam	Tidak bisa diprediksi
5	Terjadi 6-12 bulan sekali	6-12 jam	
6	Terjadi 2-6 bulan sekali	12-24 jam	
7	Terjadi 1-2 bulan sekali	1-4 hari	
8	Terjadi 2-4 minggu sekali	5-9 hari	
9	Terjadi 1-2 minggu sekali	10-14 hari	
10	Terjadi 1-7 Hari sekali	15-30 Hari	
11	Terjadi beberapa kali dalam kurun waktu 24 jam	Membutuhkan waktu kurang dari 1 bulan	

Setelah melakukan penilaian terhadap ke-3 kriteria yakni *likelihood, restoration time*, dan *predictability* dilakukan penjumlahan untuk mendapatkan score yang nantinya akan menjadi informasi bagi Unit XYZ untuk mengetahui ancaman mana yang harus dijadikan prioritas terlebih dahulu jika ancaman tersebut terjadi. maka antisipasi dan langkah mitigasi yang optimal perlu dilakukan. dengan menggunakan data yang telah ditetentukan ini maka selanjutnya akan dijadikan acuan dalam melakukan *Business Impact Analysis* (BIA). Adapun hubungan dari metode QRA dan framework NIST 800-34 yaitu

identifikasi asset IT yang dihasilkan pada metode QRA berupa asset IT tangible dan intagible, asset IT intagible akan dianalisis lebih dalam pada framework NIST 800 34 dan kategori ancaman menurut (J,W merrit) dalam metode QRA akan di identifikasi dan dianalisis untuk dibuat dokumen DRP dengan menggunakan pedoman NIST 800-34.

3.2.3 Melakukan Analisa Dampak Bisnis

Business Impact Analysis (BIA) merupakan fase atau tahapan dalam penyusunan DRP dalam aktivitasnya yakni mengetahui proses bisnis mana yang paling penting dalam instansi. Secara penjelasan menurut (Tammineedi, 2010) BIA sendiri merupakan sebuah proses penentuan proses bisnis atau layanan yang terjadi ancaman atau risiko yang menghambat jalannya proses bisnis pada suatu organisasi.

Tujuan tahapan BIA sendiri yakni membantu Unit IT ini mengetahui dan memahami dampak yang diakibatkan dari suatu bencana atau ancaman apabila terjadi. pada tahapan BIA aktivitas yang pertama kali dilakukan adalah mengetahui layanan apa saja yang dipunyai oleh Unit IT Perguruan Tinggi XYZ. Setelah mengetahui layanan apa saja yang dimiliki oleh Unit IT. Proses selanjutnya adalah menentukan derajat dampak risiko terhadap layanan dari Unit IT. Terdapat 3 aspek atau kategori untuk derajat risiko, yakni rendah, sedang dan tinggi.

3.2.4 Pembuatan Strategi Kontingensi

Penyusunan strategi kontingensi yang digunakan adalah *strategi recovery*. *strategi recovery* sebuah proses untuk melaksanakan pemulihan ketika akan terjadi ancaman pada aset atau layanan pada Unit XYZ. Dalam prosesnya dilakukan melalui skenario bagaimana melakukan tindakan pemulihan dan mitigasi resiko apabila aset dan layanan IT/IS telah terjadi ancaman .

3.2.5 Penyusunan Laporan

Pada tahapan ini memuat tentang pedoman dan rekomendasi yang berupa dokumen DRP yang didalamnya berisikan *strategy recovery* yang dibuat berdasarkan framework NIST 800 34. Pada framework ini menargetkan untuk menghasilkan rencana *strategy recovery* untuk menjadi pedoman pada objek penelitian.

BAB IV
PEMBAHASAN

4.1.Identifikasi dan Analisis Risiko Berdasarkan Metode *Quantitave Risk Analys* (QRA)

4.1.1 Menentukan Ruang Lingkup

Untuk menentukan ruang lingkup ada beberapa hal yang perlu dilakukan yakni menentukan sebuah objek yang perlu di identifikasi yakni tempat serta aset yang nantinya akan dianalisis. Lalu menentukan metode pengumpulan data untuk menganalisis risiko serta menentukan kategori atau aspek mana yang paling memperlukan perbaikan.

4.1.1.1. Menentukan Objek

Pada tahapan ini hal yang perlu dilaksanakan adalah menentukan lokasi serta menentukan aset IT mana yang akan dievaluasi. Tempat lokasi yang dipilih yakni Unit IT yang dimiliki oleh perguruan tinggi yang ada di Bojonegoro. Unit IT ini bertugas menjalankan informasi dan data yang ada diperguruan tinggi tersebut sehingga Unit IT ini tidak akan lepas dari penggunaan Aset IT.

Pada Unit IT mempunyai beberapa layanan informasi diantara lain yakni layanan administrasi keuangan, layanan sistem informasi akademik, layanan perpustakaan, layanan kepegawaian.

4.1.1.2. Pengumpulan Data

Pada tahapan ini dilaksanakan pengumpulan data dengan tujuan agar memperoleh aset IT yang akan dievaluasi nantinya serta memperoleh gambaran risiko aset IT pada unit IT yang pernah terjadi bencana atau serangan. Pengumpulan data dilaksanakan pada bulan maret sampai april 2023 terdapat beberapa metode pengumpulan data antara lain:

1. Wawancara : pada proses ini peneliti melaksanakan wawancara kepada narasumber yaitu bapak Sugito S.Kom. M.E. beliau selaku ketua Unit IT di perguruan tinggi yang ada dibojonegoro. Narasumber dipilih dikarenakan paling kompeten dalam bidang teknologi di perguruan tinggi tersebut dan telah bekerja selama 7 tahun di unit IT. Selain melakukan wawancara peneliti mengumpulkan data yang diperoleh dari buku inventaris barang pada tahun 2020 sampai 2023.

2. Studi dokumentasi : pada tahapan ini peneliti menganalisis dokumen yang diperoleh dari hasil wawancara serta mempelajari dokumen proses bisnis yang berjalan pada Unit IT.

4.2.1 Menetapkan Aset

Untuk menentukan aset IT pada Unit IT Perguruan tinggi XYZ, peneliti juga melaksanakan studi lapangan dengan menganalisis serta mengamati keadaan lapangan. Pengamatan dilakukan dengan berfokus pada keadaan aset IT di Unit IT, Aset IT meliputi layanan, informasi dan data yang terdapat pada objek penelitian ini. Sebelum melakukan wawancara peneliti melakukan penyusunan list pertanyaan yang akan ditanyakan pada saat wawancara. List pertanyaan tersebut mengacu pada metode yang digunakan yakni *Quantitave Risk Analys* (QRA) dan *framework* NIST 800 34 dengan menyesuaiakan kebutuhan yang ada pada Unit IT. Wawancara dilaksanakan pada tanggal 2 maret 2023 pukul 14:00 bertempat di ruang unit IT Perguruan tinggi XYZ.

Berdasarkan list pertanyaan terdapat pertanyaan yang meliputi aset IT dengan nominal harga masing masing aset tersebut, narasumber memberikan jawaban bahwa data aset tersebut terdapat pada buku inventaris dengan rentang tahun 2020 sampai 2023 beserta nominal harga masing masing item tersebut. Jenis Aset pada Unit IT Perguruan Tinggi XYZ dijelaskan pada tabel 4.1 :

Table 4. 1 : List Aset IT

No	Jenis Aset
1	PC
2	CCTV
3	Smart TV
4	Router
5	Acces Point
6	Laptop
7	Printer
8	Kamera
9	Switch
10	Lcd Proyektor
11	Pointing Device
12	Server

13	Baindwith
14	Scanner
15	Virtual Server Hosting
16	Modem
17	Kabel UTP
18	Keyboard
19	Monitor
20	Uninterruptible Power Supply
21	Layanan administrasi Keuangan
22	Jaringan Internet
23	Memori Virtual
24	Layanan Kepegawaian
25	Layanan Perpustakaan
26	Layanan Sistem Informasi Akademik

Berdasarkan aset tersebut ditemukan 27 aset IT di Unit IT perguruan tinggi XYZ. Aset IT tersebut masih tergolong aset yang tangible dan intangible maka daripada itu peneliti akan melakukan klasifikasi terhadap aset IT tersebut. Menurut (Tan, 2002) Aset IT tangible yakni aset yang mempunyai manfaat secara jelas dan dapat dirasakan kepada pengguna untuk kepentingan pribadi ataupun bersama. Klasifikasi tersebut akan dijelaskan pada tabel 4.2 berikut ;

Table 4. 2 : Identifikasi Aset

No	Aset IT *Tangible*	Aset IT *Intangible*
1	PC	
2		Layanan administrasi Keuangan
3	CCTV	
4	Smart TV	
5		Layanan Perpustakaan
6	Router	
7	Acces Point	
8		Jaringan Internet
9	Laptop	

10	Printer	
11	Kamera Canon	
12	Switch	
13	Lcd Proyektor	
14		Layanan Sistem Informasi Akademik
15	Server	
16		Baindwith
17		Virtual Server Hosting
18	Scanner	
19	Modem	
20		Layanan Kepegawaian
21	Keyboard	
22	Monitor	
23	Uninterruptible Power Supply	
24		Memori Virtual
25	Kabel UTP	
26	Pointing Device	

Dari hasil konsep *IT aset Tangible* dan *Intagible* maka ditemukan 18 aset yang masuk dalam kriteria tangible dan 7 aset yang masuk dalam kriteria intagible. Dari 18 *aset tangible* yang ada pada Unit IT Perguruan Tinggi XYZ nantinya akan dianalisis pada tahapan berikutnya.

Setelah melaksanakan identifikasi aset, langkah berikutnya adalah menetapkan aset yang ada pada Unit IT perguruan tinggi XYZ. Ada dua point yang harus dilakukan pertama adalah menetapakan jumlah dari masing masing aset dam point kedua adalah menentukan harga dari masing masing aset IT dengan melihat data inventaris barang yang ada pada di Unit IT, berikut pada tabel 4.3 merupakan jumlah masing masing aset yang ada pada Unit IT :

Table 4. 3 : Penetapan Aset

No	Jenis Aset	Jumlah
1	PC	5 Unit
2	CCTV	8 Unit

3	Smart TV	23 Unit
4	Router	2 Unit
5	Acces Point	1 Unit
6	Laptop	3 Unit
7	Printer	2 Unit
8	Kamera	1 Unit
9	Switch	1 Unit
10	Lcd Proyektor	4 Unit
11	Pointing Device	3 Unit
12	Server	1 Unit
13	Scanner	2 Unit
14	Modem	2 Unit
15	Kabel UTP	7 Unit
16	Keyboard	8 Unit
17	Monitor	8 Unit
18	Uninterruptible Power Supply	2 Unit

Dalam menentukan harga masing masing aset IT maka dilakukan pencarian pada data inventaris barang yang dimiliki oleh Unit IT. Dengan dibantu staff IT peneliti mencari harga masing masing aset IT yang akan dijelaskan pada tabel berikut :

Table 4. 4 Harga Aset IT

No	Jenis Aset	Jumlah	Total Harga
1	PC	5 Unit	Rp.15.104.000
2	CCTV	8 Unit	Rp.2.600.000
3	Smart TV	23 Unit	Rp.50.370.000
4	Router	2 Unit	Rp.2.360.000
5	Acces Point	1 Unit	Rp.2.455.000
6	Laptop	3 Unit	Rp.14.835.000
7	Printer Apson	2 Unit	Rp.4.100.000
8	Kamera Canon	1 Unit	Rp.4.300.000
9	Switch Cisco	1 Unit	Rp.1.900.000
10	Lcd Proyektor	4 Unit	Rp.5.670.000

11	Pointing Device	3 Unit	Rp.1.700.000
12	Server	1 Unit	Rp. 43.000.000
13	Scanner	1 Unit	Rp.1.400.000
14	Modem	2 Unit	Rp.1.298.000
15	Kabel UTP	7 Unit	Rp.14.700.000
16	Keyboard	8 Unit	Rp.12.000.000
17	Monitor	8 Unit	Rp.4.400.000
18	Uninterruptible Power Supply	2 Unit	Rp.1.834.000

Dari tabel diatas menunjukkan dalam menetapkan aset IT yang terdiri dari jumlah per unit serta total harga dari masing masing aset. Dari harga yang telah dijelaskan tersebut maka diketahui nominal harga dari semua aset IT yang telah diidentifikasi yakni sebesar Rp. 184.026.000.

4.3.1 Menetapkan Risiko dan Ancaman

Untuk menetapkan risiko dan ancaman yang berpotensi merusak aset IT maka pada penetapan aset pada penelitiian ini menggunakan 15 kategori yang dibuat oleh (J.W. Merrit 2000) yang telah dijelaskan pada bab sebelumnya. Setelah menentukan risiko dan ancaman yang berpotensi merusak maka tahap berikutnya adalah menentukan Nilai ARO *(Annualized Rate Occurance)* yang merupakan presentase nilai setiap risiko pada aset IT dalam kurun waktu satu tahun. Dalam menentukan Nilai ARO pada penelitian ini yakni dengan menentukan nilai presentase yang berpotensi terjadi ancaman pada aset IT di Unit IT Perguruan Tinggi XYZ yang dapat menimbulkan kerugian sampai kerusakan dalam kurun waktu satu tahum. Presentase Nilai didapatkan dari hasil wawancara dengan Bapak Sugito S.Kom, M.E Selaku ketua Unit IT dan pasti tahu akan keadaaan aset IT. Dalam wawancara dengan beliau peneliti menanyakan perihal persentase nilai terjadinya risiko pada aset yang telah di paparkan di atas dalam jangka waktu satu tahun. Adapun hasil wawancara sebagai pada tabel 4.5 berikut :

Table 4. 5: Hasil ARO

No	Ancaman	Nilai Aro
1	Kehilangan daya	0,4
2	Kehilangan Komunikasi	0,18
3	Kehilangan integritas data	0,2

4	Kesalahan tidak sengaja	0,11
5	Virus Computer	0,7
6	Penyalahgunaan hak akses	0,4
7	Bencana alam	0,2
8	Usaha orang luar untuk mengakses sistem	0,5
9	Pencurian dan penghancuran aset dan layanan IT	0,6
10	Penghancuran data	0,2
11	Penyalahgunaan hak akses oleh pengguna lain	0,1
12	Pihak luar yang berhasil mengakses sistem	0,1
13	Penghentian proses tanpa bencana	0,2
14	Kebakaran	0,0
15	Gempa Bumi	0,4

Tabel diatas menjelaskan bahwa presentase nilai ARO pada 15 ancaman yang telah dijelaskan diketahui bahwa ancaman yang mendapatkan presentase tertinggi adalah Virus computer dengan nilai ARO 0,7 dan yang mendaptkan presentase terendah adalah kebakaran dengan nilai ARO 0,0.

4.4.1 Menentukan Koefisensi Dampak

Dalam melakukan analisis aset IT hal yang perlu diperhatikan adalah mengetahui aset yang berpotensi hilang atau rusak atau yang disebut juga *Exposure Factor* dengan nilai yang telah dijabarkan pada tabel 3.2. Untuk mendapatkan persentase nilai yang di inginkan maka diperlukan sebuah wawancara lebih lanjut dengan narasumber yang telah diwawancarai sebelumnya, tahapan ini peneliti mengajukan pertanyaan dengan berfokus pada persentase dampak kehilangan atau kerusakan pada tabel 4.5 yang sudah di identifikasi sebelumnya. Untuk menentukan koefisien dampak, maka hasil wawancara dan jenis ancaman digabungkan lalu dilakukan penilaian berdasarkan nilai *exposure factor,* Hasil penilaian tersebut disebut dengan hasil koefisien dampak yang dapat dilihat tabel 4.6 :

Table 4. 6 : Hasil Koefisien Dampak (EF)

Jenis Aset	Kehilangan Daya	Kehilangan Komunikasi	Kehilangan Integritas data	Kesalahan Tidak Sengaja	Virus Computer	Penyalahgunaan Hak akses	Bencana Alam	Usaha orang luar mengakses sistem	Pencurian dan penghancuran aset dan layanan IT	Penghancuran data	Penyalahgunaan Hak akses pengguna lain	Pihak Luar berhasil akses sistem	Pengehentian Proses Tanpa bencana	Kebakaran	Gempa Bumi
	Nilai Koefisensi Dampak														
PC	0,3	0,5	0,7	1	0,5	0,3	1	0,5	0,7	1	0,3	0,5	0	1	0,7
CCTV	0,5	0	0,3	0,5	0	0,5	1	0,5	0	0	0,7	0,7	0,5	1	0,5
Smart TV	0,5	0,7	0,5	0,7	0	0,5	0,7	0,3	0	0	0,5	0,3	0,3	1	0,7
Router	0,3	0,5	0,7	1	0,3	0,5	1	0,5	0,3	1	0,5	0,3	0,5	0,5	1
Acces Point	0,7	0,5	0,7	0.7	0,3	0,5	0,5	0,7	0	0	0,3	0,5	0,7	1	0,7
Laptop	0,5	0,5	0,3	1	0,7	1	0	0,5	0,5	1	0,5	1	0,5	1	1
Printer	0,3	0,5	0	0,3	0,3	0	0,7	0,5	0	0	0,5	0	0	1	1
Kamera	0,1	0,5	0,3	1	0	1	0	1	0,3	1	0,5	0,3	0,7	1	1
Switch	0,3	0,5	0,7	1	0	0,5	0,3	0,7	0,5	1	0,5	0,7	1	0,7	1
Lcd Proyektor	0,1	0	0	1	0	1	0	1	0,5	0	0,3	0,5	0	1	0,7
Pointing Device	0,5	0,5	0	0,5	0	0,5	0,3	0,5	1	1	0,5	0,7	0,5	1	1
Server	0,3	0,3	0,5	0	0,3	1	1	0,5	0,3	0	0,5	0,5	0,5	1	1
Scanner	0,5	0	0,5	0	0,5	0,7	0,5	0,7	1	0	1	0,5	0,7	1	0,7
Modem	0	0,5	0,7	0,3	0,5	1	0,5	0,3	0,5	1	0,5	0,3	0,5	1	1
Kabel UTP	0,3	0,5	0,7	0,5	0	0,5	0,7	0,5	1	0	0,5	0,5	1	0,5	1
Keyboard	0	0	0	0,5	0	0	0	0	0,5	0	0	0	0	0	0,5
Monitor	0,1	0	0	0,3	0	0,3	0	0	1	0	0,5	0	1	1	1
UPS	0,7	0,5	0,5	0,7	0,5	1	0	0,5	0,7	0	0,5	1	0,5	1	1

4.5.1 Evaluasi

Pada evaluasi kelompok ini dilaksanakan secara tatap muka dengan orang berperan penting di Unit IT. Pembahasan pertama evaluasi yaitu ancaman (*Threat)* dengan menerangkan kembali pada narasumber 1 ancaman yang ada didalam metode QRA serta mengevaluasi nilai ARO yang telah didapatkan apakah cocok dengan keadaan Unit IT dalam evaluasi kelompok mengenai 1 ancaman dan nilai ARO narasumber setuju dengan apa yang telah ditentukan.

Untuk evaluasi pada *exposure factor* peneliti mempresentasikan kepada narasumber akan hasil nilai persentase dari dampak risiko dalam evaluasi kedua kali ini narasumber setuju akan nilai yang didapatkan dan dirasa sudah cocok dengan adanya kejadian yang terjadi di Unit IT. Untuk evaluasi pada harga aset IT yang telah disesuaikan dengan buku notaris pembelian dengan memberikan beberapa list harga aser IT kepada narasumber kemudian mempersilahkan untuk memberikan masukan atau koreksi pada harga aset IT yang telah disesuaikan dalam evaluasi harga aset ini narasumber menyatakam bahwa harga aset IT telah sesuai dan dirasa sudah cocok.

4.6.1 Kalkulasi

Untuk memudahkan tahapan kalkulasi peneliti mengumpulkan semua nilai yang didapatkan dari nilai harga aset IT, Nilai ancaman dan risiko serta nilai koefiesian dampak (*Exposure Factor*). Nilai tersebut akan dikumpulkan menjadi satu menggunakan spreadsheet dengan meletakkan nilai harga aset IT ke sumbu vertikal lalu meletakkan nilai ancaman ke sumbu horizontal serta meletakkan nilai yang didapatkan dari koeefisen dampak diantara nilai harga dan ancaman. Berikut akan dijelaskan pada tabel 4.7:

Table 4. 7 : Perkumpulan Nilai

Aset IT	PC	CCTV	Smart TV	Router	Acces Point	Laptop	Printer	Kamera Canon	Switch	Lcd Proyektor	Pointing Device	Server	Scanner	Modem	Kabel UTP	Keyboard	Monitor	UPS
Nilai Harga Aset IT	.15.104.000	2.600.000	50.370.000	2.360.000	2.455.000	14.835.000	4.100.000	4.300.000	1.900.000	5.670.000	1.700.000	43.000.000	1.400.000	1.298.000	14.700.000	12.000.000	4.400.000	1.834.000
Ancaman																		
Kehilangan daya	0,3	0,5	0,5	0,3	0,7	0,5	0,3	1	0,3	0,1	0,5	0,3	0,5	0	0,3	0	1	0,7
Kehilangan Komunikasi	0,5	0	0,7	0,5	0,5	0,5	0,5	0,5	0,5	0	0,5	0,3	0	0,5	0,5	0	0	0,5
Kehilangan integritas data	0,7	0,3	0,5	0,7	0.7	0,3	0	0,3	0,7	0	0	0,5	0,5	0,7	0,7	0	0	0,5
Kesalahan tidak sengaja	1	0,5	0,7	1	0,7	1	0,3	1	1	1	0,5	0	0	0,3	0,5	0,5	0.3	0,7
Virus Computer	0,5	0	0	0,3	0,3	0,7	0,3	0	0	0	0	0,3	0,5	0,5	0	0	0	0,5
Penyalahgunaan hak akses	0,3	0,5	0,5	0,5	0,5	1	0	1	0,5	1	0,5	1	0,7	1	0,5	0	0,3	1
Bencana alam	1	1	0,7	1	0,5	0	0,7	0	0,3	0	0,3	1	0,5	0,5	0,7	0	0	0
Usaha orang luar untuk mengakses sistem	0,5	0,5	0,3	0,5	0,7	0,5	0,5	1	0,7	1	0,5	0,5	0,7	0,3	0,5	0	0	0,5
Pencurian dan penghancuran aset dan layanan IT	0,7	0	0	0,3	0	0,5	0	0,3	0,5	0,5	1	0,3	1	0,5	1	0,5	1	0,7
Penghancuran data	1	0	0	1	0	1	0	1	1	0	1	0	0	1	0	0	0	0

Penyalahgunaan hak akses oleh pengguna lain	0,3	0,7	0,5	0,5	0,3	0,5	0,5	0,5	0,5	0,3	0,5	0,5	1	0,5	0,5	0	0,5	0,5
Pihak luar yang berhasil mengakses sistem	0,5	0,7	0,3	0,3	0,5	1	0	0,3	0,7	0,5	0,7	0,5	0,5	0,3	0,3	0	0	1
Penghentian proses tanpa bencana	0	0,5	0,3	0,5	0,7	0,5	0	0,7	1	0	0,5	0,5	0,7	0,5	0,5	0	1	0,5
Kebakaran	1	1	1	0,5	1	1	1	1	0,7	1	1	1	1	1	1	0	1	1
Gempa Bumi	0,7	0,7	0,7	1	0,7	1	1	1	1	0,7	1	1	0,7	1	1	0,5	1	1

Dari tabel 4.7 menunjukkan bahwa pada ancaman kebakaran dan gempa bumi mempunyai nilai koefisen dampak tertinggi dan aset keyboard tidak mempunyai nilai koefisen dampak.

Langkah berikutnya adalah menghitung nilai dari *Single Loss Expectancy* (SLE), tujuan dari menghitung nilai SLE adalah mencari suatu nilai yang hilang jika terjadi satu kali ancaman atau gangguan aset IT. Dalam menghitung SLE memperlukan rumus yang sudah dijelaskan pada bab 3.2.2.6 pada tahapan Kalkulasi.

Table 4. 8 Kalkulasi Nilai SLE (Single Loss Expectancy)

Aset IT	PC	CCTV	Smart TV	Router	Acces	Laptop	Printer	Kamera	Switch	Lcd Proyektor	Pointing Device	Server	Scanner	Modem	Kabel UTP	Keyboard	Monitor	UPS
Ancaman																		
Kehilangan daya	4.531.200	1.300.000	25,185,000	708.000	1.718.500	7.417,500	1.230.000	4.300.00	570.000	567.000	850.000	12.900.000	700.000	0	4.410.000	0	4.400.00	1.283.800
Kehilangan Komunikasi	7.552.000	0	35.259.000	1.180.000	1.227.500	7.417.500	2.050.000	2.150.000	950.000	0	850.000	12.900.000	0	649.000	7.350.000	0	0	917.000
Kehilangan integritas data	10.572.800	780.000	25.185.000	1.652.000	1.718.5000	4.450.500	0	1.290.000	1.330.000	0	0	21.500.000	700.000	908.600.000	10.290.000	0	0	917.000
Kesalahan tidak sengaja	15.104.000	1.300.000	35.259.000	2.360.000.	1.718.500	14.835.000	1.230.000.	4.300.000.	1.900.000	5.670.000	850.000	0	0	389.400.	7.350.000	6.000.000	1.320.000	1.283.800.
Virus Computer	7.552.000	0	0	708.000	736.500	10.384.5000	1.230.000	0	0	0	0	12.900.000	700.000.	649.000	0	0	0	917.000
Penyalahgunaan hak akses	4.531.200.	1.300.000	25.185.000	1.180.000	1.227.500.	14.835.000	0	4.300.000	950.000	5.670.000	850.000	43.000.000	980.000	1.298.000	7.350.000	0	1.320.000	1.834.000
Bencana alam	15.104.000	2.600.000	35.259.000	2.360.000	1.227.500	0	2.870.000	0	570.000	0	510.000	43.000.000	700.000	649.000	10.290.000	0	0	0
Usaha orang luar untuk mengakses sistem	7.552.000	1.300.000	15.111.000	1.180.000	1.718.500	7.417.500	2.050.000	4.300.000	1.330.000	5.670.000	850.000	21.500.000	980.000	389.400	7.350.000	0	0	917.000
Pencurian dan penghancuran aset dan layanan IT	10.572.800	0	0	708.000	0	7.417.500	0	1.290.000	950.000	2.835.000	1.700.000	12.900.000	1.400.00	649.000	14.700.000	6.000.000	4.400.000	1.283.800
Penghancuran data	15.104.000	0	0	2.360.000	0	14.835.000	0	4.300.000	1.900.00	0	1.700.000	0	0	1.298.000	0	0	0	0
Penyalahgunaan hak akses oleh pengguna lain	4.531.200.	1.820.000	25.185.000	1.180.000	736.500.	7.417.500	2.050.000	2.150.000	950.000	1.701.000	850.000	21.500.000	1.400.000	649.000	7.350.000	0	2.200.000	917.000
Pihak luar yang berhasil	7.552.200.	1.820.000	15.111.000	708.000	1.227.500	14.835.000	0	1.290.000	1.330.000	2.835.000	1.190.000	21.500.000	700.000	389.400	4.410.000	0	0	1.834.000

mengakses sistem																		
Penghentian proses tanpa bencana	0	1.300.000	15.111.000	1.180.000	1.718.500	7.417.500	0	3.010.000	1.900.000	0	850.000	21.5000.000	980.000	649.000	7.350.000	0	4.400.000	917.000
Kebakaran	15.104.000	2.6000.00	50.370.000	1.180.000	2.445.000	14.835.000	4.100.000	4.300.000	1.330.000	5.670.000	1.700.000	43.000.000	1.400.000	1.298.000	14.700.000	0	4.400.000	1.834.000
Gempa Bumi	10.572.800	1.820.000	35.259.000	2.360.000	1.718.500	14.835.000	4.100.000	4.300.000	1.900.00	3.969.000	1.700.000	43.000.000	980.000	1.298.000	14.700.000	6.000.000	4.400.000	1.834.000

Langkah Berikutnya adalah menghitung nilai dari ALE (*Annualized Loss Expectancy)* dengan tujuan mengetahui suatu nilai yang hilang akibat suatu ancaman pada aset IT dengan jangka waktu satu tahun. Dalam menghitung ALE terdapat rumus yakni sudah dijelaskan pada Bab 3.2.2.6 pada tahapan Kalkulasi.

Table 4. 9 Kalkulasi Ale *(Annualized Loss Expectancy)*

Aset IT	PC	CCTV	Smart TV	Route	Acces Point	Laptop	Printer	Kamera	Switch	Lcd Proyektor	Pointing Device	Server	Scanner	Modem	Kabel UTP	Keyboard	Monitor	UPS
Ancaman																		
Kehilangan daya	1.812.480.	520.000	10.074.000	283.2000.	687.400	2.967.000	492.000	1.720.000	228.000	226.000	340.000	5.160.000	280.000	0	1.764.000	0	1.760.000	513.520.
Kehilangan Komunikasi	1.359.360.	0	6.346.620	212.400	220.950	1.335.150.	369.000	387.000	171.00	0	153.000	2.322.000	0	166.820.	1.323.000	0	0	165.060
Kehilangan integritas data	2.114.500	156.00	5.037.000	330.400	343.700	890.100	0	258.000	266.000	0	0	4.300.000	140.000	181.720.	2.058.000	0	0	183.400.
Kesalahan tidak sengaja	1.661.440	143.000	3.878.490	259.600	189.035	1.631.850	135.300	473.000	209.000	623.700	93.500	0	0	42.834	808.500	660.000	145.200	141.218
Virus Computer	5.286.400	0	0	495.600	515.550	7.269.150	861.000	0	0	0	0	9.030.000	490.000	454.300	0	0	0	641.900
Penyalahgunaan hak akses	1.812.480	520.000	10.074.000	472.000	491.000	5.934.000	0	1.720.000	380.000	2.268.000	340.000	17.200.000	392.000	519.2000	2.940,000	0	528.000	733.600
Bencana alam	3.020.800	520.000	7.051.800	472.000	245.500	0	574.000	0	114.000	0	102.000	8.600.000	140.000	129.000	2.058.000	0	0	0
Usaha orang luar untuk mengakses sistem	3.776.000	650.000	7.555.500	590.000	859.250	3.708.750	1.025.000	2.150.000	665.000	2.835.000	425.000	10.750.000	490.000	194.000	3.675.000	0	0	458.500
Pencurian dan penghancuran aset dan layanan IT	6.343.680	0	0	424.800	0	4.450.500	0	774.000	570.000	1.701.000	1.020.000	7.740.000	840.000	389.400	8.820.00	3.600.000	2.640.000	770.280.
Penghancuran data	3.020.800	0	0	472.000	0	2.967.000	0	860.000	380.000	0	340.000	0	0	259.600	0	0	0	0
Penyalahgunaan hak akses oleh pengguna lain	453.120	182.000	2.518.500	118.000	73.650	741.750.	205.000	215.000	95.000	170.100	85.000	2.150.000	140.000	64.900	735.000	0	220.000	91.700

Pihak luar yang berhasil mengakses sistem	755.200	182.000	1.511.100	70.800	122.750	1.483.500	0	129.000	133.000	283.500	119.000	2.150.000	70.000	38.940	441.000	0	0	183.400
Penghentian proses tanpa bencana	0	260.000	3.022.200	236.000	343.700	1.483.50 0	0	602.000	380.000	0	0	4.3000.000	196.000	129.800	1.470.000	0	880.000	183.400
Kebakaran	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gempa Bumi	6.041.6000	1.040.000	20.148.000	472.000	982.000	5.934.000	1.640.000	1.720.000	532.000	2.268.000	680.000	17.2000.000	560.000	519.200	5.880.000	0	1.760.000	733.000

4.7.1 Hasil Analisis

Tahapan akhir dalam menggunakan metode quantitative risk analys adalah menganalisis hasil yang didapatkan dari perhitungan *SLE* dan *ALE*. Tahapan ini bertujuan agar memperoleh asset mana yang akan dijadikan prioritas pemulihan. Dalam menentukan analisis terdapat dua metode yang harus dikerjakan pertama *analysis across asset* kedua *analysis across risk*. Dalam memperoleh *analysis across asset* yakni menjumlahkan masing masing nilai asset IT yang didapatkan dari perhitungan. Sedangkan untuk memperoleh hasil *analysis across* risk yakni dengan menjumlahkan masing masing nilai ancaman pada asset IT, Berikut hasil analisa akan dijelaskan pada tabel 4.10 dan 4.11 :

Table 4. 10: Hasil *Analisis Across Asset*

No	Asset It	Analysis Across Asset
1	Server	95.202.000
2	Smart TV	82.254.210
3	Laptop	42.276.750
4	PC	38.968.320
5	Kabel UTP	33.442.500
6	Kamera Canon	11.438.000
7	Lcd Proyektor	10.943.100
8	Monitor	8.373.000
9	Printer	5.711.300
10	Acces Point	5.319.985
11	Router	5.026.800
12	Uninterruptible Power Supply	4.799.578
13	CCTV	4.433.000
14	Keyboard	4.260.000
15	Switch	4.256.000
16	Scanner	3.878.000
17	Pointing Device	3.867.500
18	Modem	3.171.014

Table 4. 11: Hasil *Analysis Across Risk*

No	Ancaman	Analysis Across Risk
1	Gempa Bumi	68.110.400
2	Penyalahgunaan hak akses	47.944.280
3	Usaha orang luar untuk mengakses sistem	40.415.200
4	Pencurian dan penghancuran aset dan layanan IT	37.212.660
5	Kehilangan daya	29.314.400
6	Virus Computer	25.894.400
7	Bencana alam	23.432.900
8	Kehilangan integritas data	17.068.880
9	Kehilangan Komunikasi	14.991.660
10	Penghentian proses tanpa bencana	13.486.600
11	Kesalahan tidak sengaja	10.658.417
12	Penghancuran data	9.109.400
13	Penyalahgunaan hak akses oleh pengguna lain	8.461.200
14	Pihak luar yang berhasil mengakses sistem	7.956.690
15	Kebakaran	0

Lalu analisis risiko pada metode *qualitative risk analys* menggunakan framework NIST 800-34. Tujuan dilakukannya analisis risiko untuk mengidentifikasi seluruh kemungkinan risiko yang terjadi pada layanan IT yakni pada asset IT *Intagible*. Analisis risiko pada tahapan ini sebagai proses untuk mengetahui karasteristik risiko yang dapat dilakukan untuk menentukan tingkat risiko kecil sampai besar. Untuk mengetahui kemungkinan risiko yang dapat terjadi pada unit IT dilakukanlah proses wawancara dengan membahas data yang diperoleh dari ancaman dan risiko dibuat oleh (J.W merrit). Hasil analisis risiko pada layanan IT dilihat pada table 4.12 berikut :

Table 4. 12 : Hasil Analisis Risiko

Jenis Ancaman	Dampak Yang Terjadi	Penyebab
Gempa Bumi	Merusak Gedung dan ruangan, Merusak sarana, Merusak Device.	Kejadian Alam

	Merusak dokumen atau file penting Unit IT	
Penyalahgunaan hak akses	Bocornya informasi,Kerusakan data	Kurangya penjagaan pada system, Keamanan pada PC yang digunakan terlalu mudah dibobol
Usaha orang luar untuk mengakses sistem	Redudansi data, penyusupan privasi	Kesalahan input data
Pencurian dan penghancuran aset dan layanan IT	Kerugian pada Instansi	Kurangya penjagaan seperti tidak adanya CCTV, Kelalaian manusia
Kehilangan daya	Kerusakan Hadware pada alat yang digunakan, system error dan crash	Tegangan listrik tidak stabil, Listrik padam
Virus Computer	Output system tidak valid, *Undefiined Error*	Serangan virus malware, Lampiran email dapat disisipi, antivirus belum update
Bencana alam	Merusak Gedung dan ruangan, Merusak sarana, Merusak Device. Merusak dokumen atau file penting Unit IT	Kejadian alam
Kehilangan integritas data	Bocornya informasi,Kerusakan data	Kesalahan manusia dan alat yang digunakan
Kehilangan Komunikasi	Sistem error, *system crash*	Kurangnya komunikasi antar pegawai
Penghentian proses tanpa bencana	Jaringan lambat, *Unstoppable Looping*	Server rusak, traffic data tinggi
Kesalahan tidak sengaja	Redudansi data, Output data tidak valid	Kesalahan input data, kesalahan prosedur
Penghancuran data	Kerugian instansi Unit IT	Kurangnya penjagaan seperti tidak adanya CCTV, Kelalaian manusia

Penyalahgunaan hak akses oleh pengguna lain	Bocornya informasi , kerusakan data	Kurangya penjagaan pada system, Keamanan pada PC yang digunakan terlalu mudah dibobol
Pihak luar yang berhasil mengakses sistem	Serangan hacker, Ddos, Sniffing,	Serangan Cyber, System Vulnability
Kebakaran	Merusak Gedung dan ruangan, Merusak sarana, Merusak Device. Merusak dokumen atau file penting Unit IT	Hubungan arus listrik, Terdapat banyak bahan yang mudah terbakar, kelalaian manusia

Setelah ditentukan ancaman atau risiko yang didapatkan dari hasil wawancara, perhitungan sampai analisis terdapat ancaman yang bisa dikategorisasikan sering terjadi hingga tidak pernah terjadi, ancaman tersebut juga telah diverifikasi kepada narasumber bahwasanya benar terjadi pada kurun waktu 5 tahun terakhir sehingga proses operasional menjadi terhambat. Oleh karena itu Langkah antisipasi perlu dilakukan karena mempertimbangkan bahwasanya ancaman tidak bisa diprediksi kapan akan terjadi. Langkah antisipasi yang tepat dan optimal dapat mencegah terjadinya bencana.

Langkah selanjutanya adalah menilai ancaman tersebut menggunakan 3 aspek yakni *likelihood, restoration time dan predictability* guna memperoleh nilai atau score dari masing masing ancaman serta nilai yang didapatkan akan mendapatkan prioritas dalam *strategy recovery*. *Likehood* yakni nilai seberapa sering terjadi bencana di waktu yang telah ditentukan, pada penilaian *likehood* harus adanya kejadian yang benar terjadi dan bukan adanya prediksi atau ramalan sedangkan restoration time merupakan nilai kurun waktu yang dibutuhkan oleh layanan atau system agar kembali normal beroperasi Kembali. Lalu untuk *predictability* yakni nilai yang bisa atau tidak diprediksi akan terjadinya suatu bencana, jika bencana dapat diprediksi adanya maka akan ada Tindakan untuk menghindarinya sehingga akan sedikit kerusakan yang akan menimpa. Ketiga aspek tersebut sudah dijelaskan secara rinci pada table 3.3 dan 3.4 . Selanjutnya

akan dilakukan proses penilaian menggunakan 3 aspek yakni *likelihood, Restoration time* dan *probabilit*y pada tabel 4.13 :

Table 4. 13: Penilaian Kriteria *Likelihood*

No	Ancaman	Likelihood	Terjadi (5 Tahun Terakhir)
1	Gempa Bumi	3	2 Kali dalam 5 Tahun
2	Penyalahgunaan hak akses	5	7 Kali dalam 5 Tahun
3	Usaha orang luar untuk mengakses sistem	4	4 Kali dalam 5 Tahun
4	Pencurian dan penghancuran aset dan layanan IT	2	1 Kali dalam 5 Tahun
5	Kehilangan daya	4	4 Kali dalam 5 Tahun
6	Virus Computer	6	11 Kali dalam 5 Tahun
7	Bencana alam	2	1 Kali dalam 5 Tahun
8	Kebakaran	2	0 Kali dalam 5 Tahun
9	Kehilangan integritas data	2	1 Kali dalam 5 Tahun
10	Kehilangan Komunikasi	3	2 Kali dalam 5 Tahun
11	Penghentian proses tanpa bencana	5	6 Kali dalam 5 Tahun
12	Kesalahan tidak sengaja	6	10 Kali dalam 5 Tahun
13	Penghancuran data	3	2 Kali dalam 5 Tahun
14	Penyalahgunaan hak akses oleh pengguna lain	2	1 Kali dalam 5 Tahun
15	Pihak luar yang berhasil mengakses sistem	2	1 Kali dalam 5 Tahun

Tabel diatas menunjukkan bahwa hasil penilaian pada aspek likelihood pada unit IT XZY. Diketahui bahwa ancaman yang sering terjadi adalah ancaman virus computer yang terjadi 11 kali dalam kurung waktu 5 tahun dan ancaman kesalahan tidak sengaja yang terjadi 10 kali dalam kurun waktu 5 tahun sehingga kedua

ancaman tersebut mendapatkan nilai 6 . Sedangkan ancaman yang tidak pernah terjadi adalah ancaman kebakaran sehingga mendapatkan nilai 2. Walaupun ancaman kebakaran belum pernah terjadi di Unit IT XYZ maka perlu adanya antisipasi untuk mengatasi ancaman tersebut dengan sering maintenance arus listrik atau hal lain yang mengakibatkan ancaman tersebut bisa terjadi. Selanjutnya adalah proses penilaian pada aspek restoration time.

Table 4. 14 : Penilaian Kriteria *Restoration Time*

No	Ancaman	Kriteria Restoration Time	Keterangan
1	Gempa Bumi	10	15-30 Hari
2	Penyalahgunaan hak akses	6	12-24 jam
3	Usaha orang luar untuk mengakses sistem	5	6-12 jam
4	Pencurian dan penghancuran aset dan layanan IT	5	6-12 jam
5	Kehilangan daya	4	1-6 jam
6	Virus Computer	4	1-6 jam
7	Bencana alam	8	5-9 hari
8	Kebakaran	10	15-30 Hari
9	Kehilangan integritas data	6	12-24 jam
10	Kehilangan Komunikasi	3	5 menit – 1 jam
11	Penghentian proses tanpa bencana	4	1-6 jam
12	Kesalahan tidak sengaja	3	5 menit – 1 jam
13	Penghancuran data	6	12-24 jam
14	Penyalahgunaan hak akses oleh pengguna lain	6	12-24 jam
15	Pihak luar yang berhasil mengakses sistem	6	12-24 jam

Tabel diatas menunjukkan hasil penilaian pada aspek restoration time pada unit IT XYZ. Diketahui bahwasanya pada aspek restoration time yang memiliki score tertinggi adalah gempa bumi dan kebakaran yang mendapatkan score 10 dengan membutuhkan restoration time 15-30 hari untuk memulihkan jika suatu bencana terjadi. Sedangkan score terendah dimiliki oleh ancaman kehilangan komunikasi dan kesalahan tidak sengaja yang mendapatkan score kriteria 3 dengan perlu membutuhkan restoration time selama 5 menit – 1 jam.

Table 4. 15 : Penilaian Kriteria *Predictability*

Ancaman	Kriteria Predictability	Keterangan
Gempa Bumi	4	Tidak bisa diprediksi
Penyalahgunaan hak akses	3	Prediksi bisa dilakukan setelah ada tanda tanda
Usaha orang luar untuk mengakses sistem	2	Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah
Pencurian dan penghancuran aset dan layanan IT	4	Tidak bisa diprediksi
Kehilangan daya	2	Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah
Virus Computer	3	Prediksi bisa dilakukan setelah ada tanda tanda
Bencana alam	4	Tidak bisa diprediksi
Kebakaran	4	Tidak bisa diprediksi
Kehilangan integritas data	3	Prediksi bisa dilakukan setelah ada tanda tanda
Kehilangan Komunikasi	2	Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah
Penghentian proses tanpa bencana	2	Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah
Kesalahan tidak sengaja	2	Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah
Penghancuran data	3	Prediksi bisa dilakukan setelah ada tanda tanda
Penyalahgunaan hak akses oleh pengguna lain	3	Prediksi bisa dilakukan setelah ada tanda tanda
Pihak luar yang berhasil mengakses sistem	3	Prediksi bisa dilakukan setelah ada tanda tanda

Tabel diatas menujukkan hasil penilaian pada kriteria predictability pada unit IT XYZ. Peniilaian pada kriteria ini diawali dengann ancaman bisa diprediksi sebelum bencana terjadi hingga tidak bisa diprediksi sama sekali. Diketahui bahwa

kriteria *predictability* yang memiliki score tertinggi dengan nilai 4 yakni pada ancaman gempa bumi, bencana alam, kebakaran serta pencurian dan penghancuran asset atau layanan IT dengan keterangan tidak bisa diprediksi kapan akan terjadinya bencana atau ancaman tersebut. Sedangkan yang mendaptakan kriteria terendah dengan score 2 yaitu Prediksi Bisa dilakukan sebelum bencana akan terjadi, tetapi tingkat kepercayaan yang dihasilkan sangat rendah kriteria tersebut dimiliki pada ancaman Usaha orang luar untuk mengakses system, Kehilangan daya, Kehilangan Komunikasi Penghentian proses tanpa bencana Kesalahan tidak sengaja .

Setelah dilakukan penilaian pada 3 aspek atau kriteria yakni likelihood, restoration time dan predictability maka akan dilakukan penjumlahan pada semua score yang didapatkan guna memperoleh informasi bagi Unit IT XYZ dalam mengetahui ancaman atau bencana apa saja yang harus mendapatkan prioritas terlebih dahulu.

Table 4. 16 : Hasil Penilaian Kriteria *Likehood, Restoration Time, Predictability.*

Ancaman	Likehood	Restoration time	Predictability	Total
Gempa Bumi	3	10	4	17
Penyalahgunaan hak akses	5	6	3	14
Usaha orang luar untuk mengakses sistem	4	5	2	11
Pencurian dan penghancuran aset dan layanan IT	2	5	4	11
Kehilangan daya	4	4	2	10
Virus Computer	6	4	3	13
Bencana alam	2	8	4	14
Kebakaran	2	10	4	16
Kehilangan integritas data	2	6	3	11
Kehilangan Komunikasi	3	3	2	8
Penghentian proses tanpa bencana	5	4	2	11
Kesalahan tidak sengaja	6	3	2	11
Penghancuran data	3	6	3	12

Penyalahgunaan hak akses oleh pengguna lain	2	6	3	11
Pihak luar yang berhasil mengakses sistem	2	6	3	11

Dari Hasil tersebut akan dilakukan perangkingan atau pengurutan dari nilai terbesar sampai terkecil agar bertujuan memperoleh informasi ancaman mana yang harus diprioritaskan dalam hal *strategy recovery*. Hasil perangkingan pada tabel 4.17 :

Table 4. 17: Hasil Perangkingan Nilai 3 kriteria

Ancaman	Likehood	Restoration time	Predictability	Total
Gempa Bumi	3	10	4	17
Kebakaran	2	10	4	16
Penyalahgunaan hak akses	5	6	3	14
Bencana alam	2	8	4	14
Virus Computer	6	4	3	13
Penghancuran data	3	6	3	12
Usaha orang luar untuk mengakses sistem	4	5	2	11
Pencurian dan penghancuran aset dan layanan IT	2	5	4	11
Kehilangan integritas data	2	6	3	11
Penghentian proses tanpa bencana	5	4	2	11

Kesalahan tidak sengaja	6	3	2	11
Penyalahgunaan hak akses oleh pengguna lain	2	6	3	11
Pihak luar yang berhasil mengakses sistem	2	6	3	11
Kehilangan daya	4	4	2	10
Kehilangan Komunikasi	3	3	2	8

Dari hasil penilaian diatas diperoleh score tertinggi yakni pada ancaman gempa bumi dengan score 17 dikarenakan ancaman tersebut akan mengalami kerusakan atau kerugian yang sangat besar jika terjadi. Selain itu kategori ancaman bencana yang lain juga mempunyai score tertinggi yakni pada ancaman kebakaran yang memiliki score 16 dan ancaman sejenis bencana alam yang memiliki score 14. Score tersebut didapatkan dari penjumlahan pada 3 aspek atau kriteria yakni likelihood, restoration time dan predictability. akan tetapi kategori ancaman bencana alam sangat besar pengaruhnya pada aspek restoration time mengingat bencana alam tidak bisa diprediksi kapan akan terjadi lalu dampak yang dihasilkan akan berakibatkan kerusakan yang sangat parah pada asset di Unit IT XYZ.

Selanjutnya pada ancaman yang lain seperti virus computer, Penghancuran data, Usaha orang luar untuk mengakses sistem Pencurian dan penghancuran aset dan layanan IT, Pencurian dan penghancuran aset dan layanan IT, Kehilangan integritas data, Kesalahan tidak sengaja, Penghentian proses tanpa bencana, Penyalahgunaan hak akses oleh pengguna lain, Pihak luar yang berhasil mengakses system, Kehilangan Komunikasi. Ancaman ini masuk kedalam kategori sedang karena dampak yang dihasilkan akan menghambat kegiatan operasional saja. Beberapa ancaman yang telah dinilai diatas bisa diprediksi hingga tidak bisa diprediksi maka dengan itu antisipasi dan mitigasi risiko perlu dilakukan agar lm ancaman semakin kecil adanya, setelah dilakukan proses penilaian dan identifikasi risiko mengenai ancaman yang terjadi Langkah selanjutnya adalah menggunakan

data yang diperoleh ini untuk dijadikan acuan dalam melakukan proses *Business Impact Analysis (*BIA)

4.2.Analisa Dampak Bisnis (BIA)

Analisa dampak bisnis merupakan tahapan terpenting dalam penyusunan Disaster Recovery Plan (DRP) tahapan ini dilakukan untuk mengetahui layanan operasioanal mana yang paling penting pada suatu instansi. Tujuan BIA sendiri membantu Unit IT dalam memahami dampak yang diakibatkan bila suatu bencana terjadi.

Langkah awal dalam melakukan Analisa dampak bisnis yakni mengetahui layanan apa saja yang dimiliki oleh Unit IT. Pada asset intangible pada table 4.2 disebutkan bahwasanya terdapat beberapa layanan yang dimiliki Unit IT XYZ . layanan tersebut akan dijelaskan pada table berikut:

Table 4. 18 : Jenis Layanan IT di Unit IT XYZ

NO	Layanan	Keterangan Layanan
1	Layanan Administrasi Keuangan	Bagian pencatatan keuangan yang berkaitan dengan pembayaran mahasiswa serta pencatatan keluar masuknya saldo yang dimiliki Unit IT XYZ.
2	Layanan Sistem Informasi Akademik	Bagian yang memuat tentang beberapa layanan mahasiswa dan dosen dalam menunjang perkuliahan
3	Layanan Perpustakaan	Layanan dalam meminjam buku yang diperolehkan Untuk mahasiswa
4	Layanan Kepegawaian	Layanan dalam memuat tentang data kepegawaian

Tabel diatas menunjukkan bahwasanya Unit IT XYZ mempunyai 4 layanan utama yang sangat penting dalam menunjang kegiatan operasionalnya. Walaupun ke empat layanan tersebut sangat penting besaran dampak yang dimilik juga sangat besar jika hal ini terjadi sehingga layanan tersebut dapat mengalami gangguan. Pada

semua layanan yang dimiliki unit IT XYZ masing masing memiliki kerentanan akan ancaman yang telah ditemukan dari hasil risk assessment.

Proses selanjutnya adalah menentukan nilai derajat dampak risiko pada ke empat layanan, dampak risiko diperoleh pada framework NIST 800-34 yang terdapat 3 kategori yakni derajat risiko rendah, sedang, tinggi yang akan dijelaskan pada table berikut :

Table 4. 19 : Derajat Dampak Risiko Menurut Framework NIST 800 34

NO	Derajat Dampak	Penjelasan
1	Rendah	Dampak kerugian yang dihasilkan kecil bagi instansi. Usaha untuk meghentikan dampak tersebut juga sedikit.
2	Sedang	Sistem apa pun yang jika terganggu akan menyebabkan masalah sedang bagi organisasi. Membutuhkan usaha yang lebih untuk menghentikan dampak tersebut.
3	Tinggi	Kerusakan atau gangguan pada sistem ini akan menyebabkan dampak paling besar pada organisasi atau perusahaan. Membutuhkan usaha yang sangat besar untuk menghentikan dampak tersebut.

Pada proses analisa dampak bisnis (BIA) data ancaman yang digunakan yakni mengacu pada hasil *risk assessment* pada table 4.16 pada masing masing layanan akan diketahui tingkat derajat dampak dari rendah, sedang dan tinggi dari ancaman setiap ancaman yang telah di identifikasi. Berikut akan dijelaskan tingkat derajat dari masing masing layanan pada ancaman yang telah diidentifikasi sebagai berikut :

Table 4. 20: Dampak Dari Gempa Bumi

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Memperhambat seluruh proses transaksi di Unit IT XYZ	Tinggi
2	Layanan Sistem Informasi Akademik	Proses layanan terhenti karena Gedung hingga PC	Tinggi

		yang rusak akibat gempa bumi	
3	Layanan Perpustakaan	Proses layanan terhenti karena Gedung hingga PC yang rusak akibat gempa bumi	Tinggi
4	Layanan Kepegawaian	Proses layanan terhenti karena Gedung hingga PC yang rusak akibat gempa bumi	Tinggi

Table 4. 21: Dampak Dari Kebakaran

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Menghentikan proses transaksi karena dokumen penting yang digunakan terbakar	Tinggi
2	Layanan Sistem Informasi Akademik	Menghentikan Layanan SIM karena dokumen penting sampai device yang digunakan terbakar	Tinggi
3	Layanan Perpustakaan	Menghentikan Layanan perpustakaan karena buku yang dipinjamkan serta dokumen penting sampai device yang digunakan terbakar	Tinggi
4	Layanan Kepegawaian	Menghentikan Layanan kepegawaian karena dokumen penting sampai	Tinggi

		device yang digunakan terbakar	

Table 4. 22 : Dampak Dari Penyalahgunaan hak akses

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Terjadinya perubahan atau manipulasi data transaksi keuangan	Tinggi
2	Layanan Sistem Informasi Akademik	Terjadi gangguan akses pada Layanan SIM	Tinggi
3	Layanan Perpustakaan	Terjadi gangguan akses pada Layanan Perpustakaan	Tinggi
4	Layanan Kepegawaian	Terjadi gangguan akses pada Layanan Kepegawaian	Tinggi

Table 4. 23 : Dampak Dari Bencana alam

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	proses transaksi di unit IT menjadi terhenti karena bangunan hingga device rusak akibat bencana alam	Tinggi
2	Layanan Sistem Informasi Akademik	Proses Kegiatan pada layanan SIM di unit IT terhentikan karena bangunan hingga device rusak akibat bencana alam	Tinggi

3	Layanan Perpustakaan	Proses Kegiatan pada layanan perpustakaan di unit IT terhentikan karena bangunan hingga device rusak akibat bencana alam	Tinggi
T4	Layanan Kepegawaian	Proses Kegiatan pada layanan Kepegawaian di unit IT terhentikan karena bangunan hingga device rusak akibat bencana alam	Tinggi

Table 4. 24: Dampak Dari Virus Computer

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Proses operasioanal layanan keuangan terhenti karena device yang dipakai terserang virus	Sedang
2	Layanan Sistem Informasi Akademik	Kegiatan Layanan SIM terhambat karena device yang dipakai mengalami serangan virus yang berimbas pada data mahasiswa dan dosen yang corrupt	Sedang
3	Layanan Perpustakaan	Kegiatan layanan perpustakaan terhambat karena device yang dipakai mengalami serangan virus yang berimbas pada data peminjam yang corrupt	Sedang

4	Layanan Kepegawaian	terhambat karena device yang dipakai mengalami serangan virus yang berimbas pada data pegawa yang corrupt	Sedang

Table 4. 25 : Dampak Dari Penghancuran Data

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Kegiatan transaksi keuangan mengalami hambatan karena data yang digunakan hancur	Sedang
2	Layanan Sistem Informasi Akademik	Proses Layanan SIM mengalami hambatan karena data-data yang dipakai hancur	Sedang
3	Layanan Perpustakaan	Proses layanan perpustakaan terhambat karena data peminjam diperpustakaan hancur	Sedang
4	Layanan Kepegawaian	Proses Layanan Kepegawaian mengalami hambatan karena data-data pegawai yang dipakai hancur	Sedang

Table 4. 26 : Dampak Dari Usaha orang luar untuk mengakses sistem

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Proses kegiatan transaksi terhenti karena orang luar mengakses system yang digunakan	Tinggi
2	Layanan Sistem Informasi Akademik	Kegiatan operasioanal Layanan SIM terhenti karena orang luar mengakses system yang digunakan	Tinggi
3	Layanan Perpustakaan	Kegiatan operasioanal Layanan perpustakaan terhenti karena orang luar mengakses system yang digunakan	Tinggi
4	Layanan Kepegawaian	Kegiatan operasioanal Layanan Kepegawain terhenti karena orang luar mengakses system yang digunakan	Tinggi

Table 4. 27: Dampak Dari Pencurian dan penghancuran aset dan layanan IT

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Seluruh kegiatan transaksii terhenti karena kehilangan asset yang digunakan	Tinggi
2	Layanan Sistem Informasi Akademik	Proses operasioanal layanan SIM terhenti	Tinggi

		karena kehilangan asset yang digunakan	
3	Layanan Perpustakaan	Layanan Perpustakaan terhenti karena kehilangan asset yang digunakan	Tinggi
4	Layanan Kepegawaian	Proses layanan kepegawaian terhenti karena kehilangan asset yang digunakan	Tinggi

Table 4. 28: Dampak Dari Kehilangan integritas data

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Kegiatan transaksi terhenti akibat kehilangan integritas data yang digunakan	Sedang
2	Layanan Sistem Informasi Akademik	Kegiatan terhenti akibat kehilangan integritas data yang digunakan	Sedang
3	Layanan Perpustakaan	Kegiatan terhenti akibat kehilangan integritas data yang digunakan	Sedang
4	Layanan Kepegawaian	Kegiatan terhenti akibat kehilangan integritas data yang digunakan	Sedang

Table 4. 29 : Dampak Dari Penghentian proses tanpa bencana

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Layanan Transaksi terhenti akibat pemberhentian proses tanpa bencana	Rendah
2	Layanan Sistem Informasi Akademik	Layanan SIM terhenti akibat pemberhentian proses tanpa bencana	Rendah
3	Layanan Perpustakaan	Layanan Perpustakaan terhenti akibat pemberhentian proses tanpa bencana	Rendah
4	Layanan Kepegawaian	Layanan Perpustakaan terhenti akibat pemberhentian proses tanpa bencana	Rendah

Table 4. 30 : Dampak Dari Kesalahan tidak sengaja

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Data yang digunakan dalam proses transaksi tidak valid akibat kesalahan yang tidak sengaja	Rendah
2	Layanan Sistem Informasi Akademik	Layanan SIM menjadi terhambat karena data yang diinputkan tidak valid	Rendah

		akibat kesalahan tidak sengaja	
3	Layanan Perpustakaan	Layanan Perpustakaan menjadi terhambat karena data yang diinputkan tidak valid akibat kesalahan tidak sengaja	Rendah
4	Layanan Kepegawaian	Layanan Kepegawaian menjadi terhambat karena data yang diinputkan tidak valid akibat kesalahan tidak sengaja	Rendah

Table 4. 31: Dampak dari Penyalahgunaan hak akses oleh pengguna lain

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Kehilangan data keuangan hingga perbedaan jumlah saldo pada pencatatan sebelumnya.	Tinggi
2	Layanan Sistem Informasi Akademik	Kehilangan data yang diguanakan dalam proses layanan SIM	Tinggi
3	Layanan Perpustakaan	Kehilangan data peminjam buku dalam proses layanan perpustakaan	Tinggi
4	Layanan Kepegawaian	Data pegawai hilang yang memperhambat proses operasional pegawai	Tinggi

Table 4. 32: Dampak Dari Pihak luar yang berhasil mengakses sistem

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Data keuangan hilang sehingga Unit IT mengalami kerugian yang sangat parah	Tinggi
2	Layanan Sistem Informasi Akademik	Proses layanan terhenti diakibatkan password berubah pada orang yang berhasil mengakses system	Tinggi
3	Layanan Perpustakaan	Proses layanan terhenti diakibatkan password berubah pada orang yang berhasil mengakses system	Tinggi
4	Layanan Kepegawaian	Proses layanan terhenti diakibatkan password berubah pada orang yang berhasil mengakses system	Tinggi

Table 4. 33 : Dampak Kehilangan daya

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Kegiatan transaksi mengalami hambatan karena device yang dipakai memerlukan daya	Sedang
2	Layanan Sistem Informasi Akademik	Kegiatan Layanan SIM mengalami hambatan	Sedang

		karena device yang dipakai memerlukan daya	
3	Layanan Perpustakaan	Kegiatan Layanan Perpustakaan mengalami hambatan karena device yang dipakai memerlukan daya	Sedang
4	Layanan Kepegawaian	Kegiatan Layanan Kepegawaian mengalami hambatan karena device yang dipakai memerlukan daya	Sedang

Table 4. 34: Dampak Dari Kehilangan Komunikasi

NO	Layanan	Dampak	Tingkat Dampak
1	Layanan Administrasi Keuangan	Kegiatan transaksi mengalami hambatan dikarenakan diantara staff satu sama lain hilang komunikasi	Rendah
2	Layanan Sistem Informasi Akademik	Layanan SIM mengalami hambatan dikarenakan diantara staff satu sama lain hilang komunikasi	Rendah
3	Layanan Perpustakaan	Layanan Perpustakaan mengalami hambatan dikarenakan diantara staff satu sama lain hilang komunikasi	Rendah

4	Layanan Kepegawaian	Layanan Kepegawaian mengalami hambatan dikarenakan diantara staff satu sama lain hilang komunikasi	Rendah

Setelah proses analisa dampak bisnis selesai maka proses selanjunya adalah pembuatan dokumen DRP itu sendiri, adapun hasil dari BIA yang digunakan dalam proses pembuatan DRP adalah hasil dampak yang paling tinggi, rendah dan sedang dari ancaman atau gangguan yang didapatkan

4.3. Pembuatan Dokumen DRP Berdasarkan Framework NIST 800-34

Tahapan berikut merupakan penyusunan dokumen disaster recovery plan (DRP), Pembuatan DRP merupakan kegiatan dalam memulihkan ketika terjadi ancaman pada system atau layanan operasioanal Unit IT XYZ. Didalam proses pemuihan ancaman harus dilakukan proses scenario dalam menerapkan mitigasi risiko yang akan diterapkan, Beberapa ancaman terhadap Sistem tau layanan IT terdapat pada proses identifikasi atau penilaian risiko. Adapun pembuatan DRP menggunakan ancaman paling tinggi, sedang, rendah yang dapat merusak layanan sistem yang mengakibatkan proses layanan itu menjadi terhenti, dokumen DRP akan diletakkan pada lampiran pada halaman akhir penelitian.

4.4. Hasil Validasi

Setelah melakukan pengerjaan sebuah dokumen disaster recovery plan maka selanjutnya adalah tahapan validasi. Kegiatan Validasi dilakukan bersama pihak unit IT Perguruan Tinggi XYZ dengan memprensentasikan hasil kepada narasumber yakni bapak sugito S.Kom. M. E pada tanggal 28 april 2023. Menurut narasumber hasil dari pengerjaan dokumen DRP telah sesuai dengan permasalahan yang terjadi pada unit IT seperti analisis risiko dan ancaman serta hasil sebuah strategy recovery terhadap ancaman yang mungkin terjadi. Berikut adalah foto kegiatan validasi yang sudah dilakukan:

Gambar 4. 1 Kegiatan Validasi Di Unit IT

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

DRP merupakan dokumen yang penting bagi Unit IT XYZ untuk dapat menjamin dalam keberlansungan operasioanal layanan IT. DRP dibuat dengan berdasarkan hal yang mungkin akan terjadi pada objek penelitian dengan disesuaikan pada kondisi yang ada. Dalam menyusun dokumen ini melewati beberapa tahapan dimulai dari Risk Assesment dengan mengidentifikasi dan analisis resiko menggunakan metode QRA (*Quantitive Risk Analys),* melakukan analisa dampak bisnis serta melakukan Strategy Recovery dengan sesuai pedoman *framework National Insitute Standart Of* Technology (NIST 800 34) sehingga dapat penelitian ini terdapat beberapa kesimpulan antara lain :

1. Pada analisa aset IT didapatkan jenis aset yang paling mempunyai dampak kerugian finansial tertinggi adalah Server dengan Nominal Rp. 95.202.000
2. Pada analisa risiko atau ancaman yang paling mempunyai risiko tertinggi adalah Gempa Bumi dengan kerugian sebesar Rp. 68.110.400.
3. Penilaian pada risiko dan ancaman menggunakan 3 aspek yakni *likehood, restoration time dan predictability* untuk mendapatkan nilai RPO dan RTO sehingga ancaman mana yang mungkin mendapatkan prioritas pemulihan analisa dampak bisnis dilakukan dengan melihat dampak yang mungkin terjadi pada kegiatan layanan IT pada Unit IT XYZ.
4. DRP dibuat berdasarkan layanan IT yang berintegrasi pada Unit IT XYZ berdasarkan ancaman yang sudah diidentifikasi.

5.2 Saran

Pada penelitian yang telah dilakukan masih dikatakan belum sempurna maka untuk penelitian berikutnya terdapat saran sebagai berikut:

1. Pemilihan objek penelitian dengan penggunaan layanan sistem informasi yang lebih luas
2. Prosedur pemulihan dalam rencana kontingensi masih sedikit dan terbatas maka saran untuk penelitian selanjutnya adalah prosedur dapat dibuat dengan mengumpulkan beberapa pandangan dari pihak yang terlibat dalam tim IT dengan bentuk *Forum Group Discouussion* (FGD) disesuaikan pada framework NIST 800-34.
3. Setelah dibuatnya dokumen disaster recovery plan, Unit IT Perguruan tinggi XYZ diharapkan mampu membentuk sebuah *Emergency Response Team* yang bertugas mengimplementasikan dokumen tersebut.

DAFTAR PUSTAKA

Alifian, M. H., & Priharsari, D. (2021). Penyusunan Disaster Recovery Plan (DRP) menggunakan framework NIST SP 800-34 (Studi Kasus pada Perusahaan IT Nasional). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer E-ISSN*, *2548*, 964X.

Budiarto, R. (2017). Manajemen risiko keamanan sistem informasi menggunakan metode fmea dan iso 27001 pada organisasi xyz. *CESS (Journal of Computer Engineering, System and Science)*, *2*(2), 48–58.

Daud, J. C. (2016). Pembuatan Disaster Recovery Plan (DRP) Berdasarkan ISO/IEC 24762: 2008 Di ITS Surabaya (Studi Kasus di Pusat Data dan Jaringan BTSI ITS). *Jurnal Teknik Pomits*, *11*.

Galliers, R., & Leidner, D. E. (2014). *Strategic information management: Challenges and strategies in managing information systems*. Routledge.

Isa, I. G. T. (2018). Kansei engineering approach in software interface design. *Journal of Science Innovare*, *1*(01), 22–26.

Isa, I. G. T. (2020). Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi. *Jurnal Ilmiah Ilmu Komputer*, *15*.

Agung, M. Z. (2019). Perancangan Disaster Recovery Plan Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34. *Jurnal Teknologi Rekayasa*, *4*(2), 157–166.

Bahrudin, M., & Firmansyah, F. (2018). Manajemen keamanan informasi di perpustakaan menggunakan Framework SNI ISO/IEC 27001. *Media Pustakawan*, *25*(1), 43–50.

Fitrah, M. (2018). *Metodologi penelitian: Penelitian kualitatif, tindakan kelas & studi kasus*. CV Jejak (Jejak Publisher).

Isa, I. G. T. (2020). Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi. *Jurnal Ilmiah Ilmu Komputer*, *15*.

Meritt, J. W. (2000.). *A Method for Quantitative Risk Analysis*.

Muslim, B. (2018). Quantitative risk analysis of asset information technology at STT Pagaralam. *Prosiding STTA Yogyakarta (Senatik 2018), STTA*, 501–509.

Prabowo, W. A., & Saputri, M. E. (2020). Pemetaan Resiko Teknologi Informasi dengan Integrasi IT Balanced Scorecard dan NIST SP 800-34 Rev. 1. *JEPIN (Jurnal Edukasi Dan Penelitian Informatika)*, *6*(3), 370–378.

Rubil, R. (2012). Business Impact Analysis Terkait Penanganan dan Pemulihan Terhadap Bencana di PT Bank XYZ. *ComTech: Computer, Mathematics and Engineering Applications*, *3*(2), 892–900.

Sari, I. N., Lestari, L. P., Kusuma, D. W., Mafulah, S., Brata, D. P. N., Iffah, J. D. N., Widiatsih, A., Utomo, E. S., Maghfur, I., & Sofiyana, M. S. (2022). *Metode penelitian kualitatif*. UNISMA PRESS.

Tammineedi, R. L. (2010). Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective*, *19*(1), 36–50.