BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Penelitian yang dilakukan tidak lepas dari berbagai referensi yang dapat membantu penulis dalam penyusunannya. Berikut adalah penelitian terdahulu:

Tabel 2. 1 Penelitian Sebelumnya

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
1	Rancangan Dokumen *Disaster Recovery Plan* Pada IS/ITD Dinas XYZ [5]	Penelitian sebelumnya membuat perancangan dokumen pemulihan akibat bencana (DRP) yang disesuaikan dengan karakteristik Dinas XYZ Kabupaten Banyumas.	Penelitian ini melakukan pengujian dokumen tersebut dengan standar NIST SP 800-34 guna mengetahui tingkat keberhasilan perancangan dokumen pemulihan akibat bencana (DRP).	Pada penelitian sebelumnya memerlukan mekanisme penangan bencana yang mampu mengatasi dampak dari kerusakan bencana baik itu bencana alam dan kerusakan akibat perbuatan manusia.	Menggunakan metode *Disaster Recovery Plan* yang didukung dengan dilakukannya observasi, studi dokumentasi, wawancara, dan *Framework* & Metode Analisa Data guna membuat prosedur prosedur antara lain kontrol pencegahan, strategi dan rencana kontigensi.	Hasil penelitian ini melakukan abalisa terhadap skema jaringan IS/IT, sistem informasi XYZ, *risk assessment, business impact analysis* (BLA), *Strategy recovery* dan dokumentasi
2	Rancangan *Disaster Recovery* Pada Instansi Pendidikan	Penelitian sebelumnya Memberikan usulan DRP yang sesuai dan bisa diimplementasikan pada	Penelitian ini menggunakan sistem *fail over* dan *mirroring*.	Pada penelitian sebelumnya dapat di kembangkan lebih luas sampai keseluruh prosedur, sumber daya manusia dan lainnya yang	Menerapkan metode aktif pasif, perencanaan pembuatan, penulis menggunakan NDLC (*Network Development*	Hasil penelitian ini mendapatkan DRP pada Universitas Mercu Buana sudah sesuai dengan spesifikasi

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Studi Kasus Universitas Mercu Buana [6]	Universitas Mercu Buana dan Membangun sistem *disaster recovery* untuk meningkatkan kinerja Universitas Mercu Buana.		diharapkan Pengembangan dari DRP berikutnya bisa menyesuaikan dengan teknologi informasi yang terbaru.	*Life Cylce*). Bertujuan agar Universitas Mercu Buana akan lebih cepat melakukan pemulihan sistem komputerisasi mereka saat terjadi bencana.	kebutuhan fungsional yang dibutuhkan pengguna. Dengan request time obejektif tiga detik dan *request point* obejektif sebesar 0 detik.
3	Perancangan *Disaster Recovery Plan* Untuk Teknologi Di Perusahaan PT. XYZ [7]	Penelitian ini memberikan perancangan *Disaster Recovery Plan* pada teknologi terkait jaringan, aplikasi, dan database serta *fileserver* di PT. XYZ serta memberikan rekomendasi jenis *Disaster Recovery Center* untuk PT. XYZ.	Penilitian ini menggunakan pengamanan data dan *Recovery Database*, *Recovery Fileserver*, *Recovery Application*, *Recovery Network* serta *Disaster Recovery Center*.	Penelitian ini menggunakan jenis *disaster recovery center* yang akan digunakan oleh PT. XYZ adalah *public cloud* untuk mengefisiensikan sumber daya yang digunakan oleh perusahaan tanpa mengesampingkan faktor security data yang dibutuhkan oleh PT. XYZ dalam melakukan proses D*isaster Recovery Plan.*	Penelitian ini menggunakan tahap yang diawali dengan identifikasi dokumen arsitektur eksisting yang berisi aset infrastruktur teknologi perusahaan PT. XYZ dan hasil *business impact analysis* yang menentukan RTO dan RPO berbagai *server* yang berada di perusahaan. Tahap selanjutnya adalah tahap desain yang berisi perancangan rekomendasi teknologi data, *application* dan *network* saat bencana terjadi. Dan tahap terakhir yang dilakukan adalah melakukan analisis untuk menyesuaikan	Hasil penelitian ini merancangan *Disaster Recovery Plan* pada teknologi terkait jaringan, aplikasi, dan database serta *fileserver* di PT. XYZ serta memberikan rekomendasi jenis *Disaster Recovery Center* untuk PT. XYZ.

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
					hasil perancangan rekomendasi tersebut.	
4	Perancangan *Business Continuity Plan* dan *Disaster Recovery Plan* Teknologi dan Sistem Infformasi Menggunakan ISO 22301 [8]	Penelitian ini adalah untuk mengidentifikasi risiko dan memberikan mitigasi risiko terhadap aset teknologi informasi pada rumah sakit ananda purwokerto serta untuk merancang proses *Business Continuity Plan* dan *Disaster Recovery Plan* pada rumah ini menggunakan *framework* ISO 22301.	Penelitian ini berdampingan dengan pembuatan BCP sehingga perumusan masalah yang digunakan menggunakan rumusan masalah dari BCP.	Penelitian ini belum mengacu pada *international standard organization* dalam perancangan *Disaster Recovery Plan.*	Penelitian ini akan merancang sebuah Business Continuity Plan dan Disaster Recovery Plan yang secara garis besar penelitian menggunakan lima tahap yaitu pengumpulan permasalahan, pengumpulan data pendukung, melakukan idenfikasi risiko, merancang *Business Continuity Plan* dan merancang *Disaster Recovery Plan* serta memberikan rekomendasi kepada rumah sakit ananda Purwokerto.	Peneliian ini menghasilkan rancangan *Disaster Recovery Plan* yang sesuaikan dengan layanan yang ada pada rumah sakit ananda purwokerto dengan memperhatikan skenario yang mungkin bisa terjadi pada saat ada bencana dan rencana pemulihan yang akan dilakukan oleh rumah sakit ananda Purwokerto pada saat ancaman tersebut terjadi sesuai dengan skenario yang dibuat dengan mengacu pada *Business Impact Analysis.*
5	Perancangan *Disaster Recovery Plan* (DRP) Untuk Meningkatkan Ketersediaan Layanan Sistem Pemerintahan Berbasis	Penelitian ini merancang DRP guna mengamankan Pusat Data dan Sistem Informasi (Pusdatin) yang merupakan salah satu unit kerja di Badan Standardisasi Nasional (BSN) yang memilki	Penelitian ini mempersiapkan tindakan penanganan dan pemulihan bila terjadi kerusakan sistem yang berdampak pada ketersediaan layanan sistem elektronik.	Penelitian ini mendapatkan hasil wawancara dengan pemilik aplikasi) dan apabila ada gangguan, *Disaster Recovery Team* memiliki waktu 30 menit untuk melakukan *recovery*	Penelitian ini melakukan perancangan DRP metode menggunakan studi pustaka seperti menelaah sumber- sumber tertulis seperti jurnal ilmiah, buku referensi, literatur serta	Penelitian ini merancang DRP melalui hasil *risk assessment analysis*, hasil analisa dampak bisnis, mendapatkan proses kritikal, rekomendasi RTO & RPO layanan aplikasi, rencana pemulihan, *backup* dan

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Elektronik (SPBE) Pada Badan Standardisasi Nasional [9]	tanggung Jawab terhadap pengelolaan *data center* yang merupakan sumber utama dari data dan informasi.		sehingga kerugian hanya setengah dari rata-rata frekuensi hits/waktu kerja (8 jam /hari). Penentuan RPO berdasarkan RTO yaitu 15 menit sehingga apabila terjadi suatu bencana maka aplikasi SISPK akan mengalami kehilangan data selama maksimal 15 menit.	sumber-sumber lain yang terpercaya baik dalam bentuk tulisan atau dalam format digital yang relevan dan berhubungan dengan objek yang sedang diteliti.	*recovery application* dan *backup recovery* manual.
6	Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan *Disaster Recovery Plan* pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi. [10]	Pada penelitian ini dilakukan tahapan yang dimulai dengan identifikasi aset, *Business Process Analysis, risk* *assessment* dan *strategy recovery*.	Pada penelitian ini penyusunan dokumen DRP menggunakan kerangka kerja NIST 800-34 yang merupakan dokumen standarisasi dirilis oleh *National Institute of Standards and Technology* NIST).	Pada penyusunan penelitian ini, dokumentasi DRP dilakukan penilaian terhadap aset berdasarkan 3 aspek yakni *Necessity, Recoverability, Replaceability* yang dikombinasikan dengan bobot persentasi penilaian sub sistem SIAK UMMI, sehingga dihasilkan skala prioritas berdasarkan subsistem prioritas teratas hingga terbawah.	Penelitian ini menggunakan tahapan yang dimulai dengan Penetapan Permasalahan dan Tujuan Pengumpulan Data melalui Observasi, Wawancara dan Studi Lapangan Penentuan dan Identifikasi Aset, *Risk Assessment*.	Penelitian ini mendapatkan bahwa identifikasi aset menjadi dasar prioritas mana yang harus didahulukan ketika terjadi ancaman terhadap SIAK UMMI, mendapatkan informasi ancaman tersebut berdasarkan parameter *Likelihood*, Restoriation Time dan Predictability didapatkan Gempa Bumi memiliki nilai tertinggi sebesar 14 dan gangguan padam Listrik sebesar 9, mengetahui sub sistem yang memiliki nilai terendah adalah Sistem Pembimbingan

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
						Akademik dengan nilai dampak persentasi 62%.
7	Perancangan Disaster Recovery Plan Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34 [11]	Penelitian ini mengangkat objek Sistem Informasi Kepegawaian (SIMPEG), Sistem Informasi Alumni dan *Tracer Study* (SIAT), dan Sistem Pendaftaran dan Pendataan Mahasiswa Baru (E-Regist). SISAK POLSRI merupakan hal yang vital dalam keberlangsungan operasional Politeknik Negeri Sriwijaya, sehingga diperlukan suatu upaya preventif. Salah Salah satu upaya yang dapat dilakukan adalah dengan merancang dokumen *Disaster Recovery Plan*.	Penelitianini menggunakan pendekatan kerangka kerja NIST 800-34 yang diinisiasi oleh *Risk Assessment, Business Impact Analysis* dan *Strategy Recovery.*	Penelitian ini memiliki tingkat dampak tertinggi dalam SISAK POLSRI adalah Sistem Informasi Kepegawaian (SIMPEG). Hal ini artinya adalah SIMPEG memiliki kerentanan yang tinggi bila terkena ancaman.	Penelitian ini menggunakan tahapan dalam perancangan *Disaster Recovery Plan* dengan pendekatan kerangka kerja NIST 800-34 yang diinisiasi oleh *Risk Assessment, Business Impact Analysis* dan *Strategy Recovery.*	penelitian ini telah dihasilkan dokumen DRP untuk SISAK POLSRI berdasarkan aspek ancaman dan terurut berdasarkan skala prioritas. Dua sub sistem skala prioritas dalam DRP adalah Sistem Kepegawaian (SIMPEG) dan E-Regist Mahasiswa Baru Polsri, dengan masing-masing bernilai 100% dan 92%.
8	Analisis Rancangan *Disaster Recovery Plan* Pada Industri Pertambangan	Penelitian ini menggunakan sistem *disaster recovery* lebih efektif daripada sebelumnya. Dengan	Penelitian ini menggunakan sistem *snap mirror* dan menggunakan teknologi	Penelitian ini tidak memandinkan metode sisem *Disaster Recovey Plan* lainnya serta pengembanangan DRP	Penelitian ini menggunakan teknik pengumpulan data kualitatif diantaranya	Hasil dari penelitian ini didapatkan untuk melakukan transfer data per jam dibutuhkan bandwith rata -rata sebesar

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Studi Kasus PT. Vale Indonesia, TBK [12]	sistem *snapmirror* penyimpanan data yang berbeda lokasi dan pulau, ini menjadi efesiensi perusahaan dalam menggunakan *server* dan jauh lebih efektif.	dari Netapp untuk menerapakan metode sistem backup penyimpanan data antara 2 *server* PT Vale Indonesia Tbk, yaitu antara Jakarta dan Sorowako.	diharapkan sesuai dengan teknologi terbaru.	adalah pengamatan dengan berpartisipasi *(participant observation*), wawancara mendalam (indepth interview), penyelidikan sejarah hidup (*life historical investigation*) dan analisis konten (*content analysis*).	22.51857618 mb, dan data yang di transfer sebesar 118.7503041 per jam.
9	Short-Term Solutions to a Long-Term Challenge: Rethinking Disaster Recovery Planning to Reduce Vulnerabilities and Inequities. [13]	Penelitian ini menggunakan perancangan *Disaster Recovery Plan* untuk mengurangi kerentanan dan ketidaksetaraan.	Penelitian ini menerapkan kerangka kerentanan atau ketidak setaraan untuk membuat konsep bagaimana merancang *Disaster Recovery Plan* dan menghindari berlanjutnya ketidakadilan ketika menimbang beragam kebutuhan masyarakat.	Peneliian ini sebaiknya menggggunakan pendekatan beulang untuk perancanaan pemulihan dan penggunaan mekanisme formal.	Penelitian ini menggggunakan metode identifikasi contoh kasus dari bencana masa lalu dan menggatur contoh kasus dengan interaksi komponen kerentanan dan ketidaksetaraan.	Peneliian ini mengunakan *frameworks* menyeluruh unuk diskusi tentang isu-isu yang terkait dengan pemulihan bencana, kerenanan dan keidakadilan.
10	Backup Strategy for IT Disaster Recovery Plan Using	Penelitian ini merancang DRP sebagai salah satu asuransi perusahaan di Indonesia yang dibutuhkan sebagai kontol untuk mitigasi	Penelitian ini menggunakan strategi backup guna menjadikan pedoman bagi semua jajaran IT direktorat dalam melaksanakan	*NetBackup* membuat backup data menjadi lebih efektif, efisien dan aman. Untuk mendukung hal tersebut dokumen DRP TI dan sebagai dasar untuk menentukan nilai RPO dan	Penelitian ini menggunakan metode pencadangan bisnis data melalui kombinasi data aktif aplikasi guard dan NetBackup sebagai mitigasi resiko kerusakan	Penelitian ini membuat rancangan DRP dengan mengamankan database yang disimpan baik untuk pemulihan bencana. Setiap *sarver database* memiliki *backup* utama, tetapi file

NO	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Active Data Guard and NetBackup [14]	resiko oprasional terkait teknologi informasi.	pemulihan oprasional acara dari sebuah bencana.	RTO permusahan. Ada banyak alat yang dapat digunakan untuk solusi pencadangan yang lebih baik dan lebih cepat. Kuncinya adalah RPO dan RTO yang lebih rendah maka DRP TI akan lebih baik.	atau hilangnya data karena bencana alam dan untuk menyelesaikan DRP sebagai pedoman standar kelangsungan usaha manajemen perusahaan.	cadangan disimpan di situs yang sama.

Tabel 2.1 merupakan tabel yang berisi batas dan pembanding antara penelitian-penelitian sebelumnya. Pada penelitian sebelumnya digunakan untuk menyusun, menganalisisi, mengevaluasi maupun mengaudit layanan teknologi informasi di berbagai obyek layanan dengan menggunakan kerangka kerja *NIST 300-34* pada perancanagan *DRP* dan salah satu penelitian sebelumnya menggunakan kerangka kerja *ISO 22301*. Adapun penelitian lain yang menggunakan metode *Networking Development Life Cycle (NDLC).*

Penelitian yang sudah dilakukan yaitu menyusun dokumen *Disaster Recovery Plan* untuk meningkatkan indeks keamanan menggunakan pendekatan *NIST 800-34* pada sistem informasi Institut Teknologi Telkom Purwokerto. Dipilihnya *NIST 800-34* karena pada kerangka tersebut telah tersedia kerangka spesifik yang memberikan acuan terkait penyusunan *DRP* sehingga dapat Menyusun dokumen rancangan kontingensi dari sistem informasi yang berjalan. Sedangkan pada kerangka kerja *ISO 22301* dan *NDLC* kurang spesifik dalam menjabarkan identifikasi risiko yang dapat terjadi. Keluaran dari setiap dokumen yang telah dirancang oleh penelitian sebelumnya [6] bahwa kerangka kerja *NIST 800-34* yaitu dokumen *DRP* yang dapat membantu memulihkan sistem informasi apabila terjadi suatu bencana berdasarkan tingkat prioritas risiko dampak yang terjadi.

2.2 Dasar Teori

Dasar teori adalah seperangkat definisi, konsep serta proposisi yang telah disusun rapi serta sistematis tentang variable-variabel dalam sebuah penelitian. Dasar teori ini akan menjadi dasar yang kuat dalam sebuah penelitian yang dilakukan. Pada bagian ini akan dibahas dasar teori yang berkaitan dengan topik DRP diantaranya adalah.

2.2.1 Sistem Informasi

Sistem informasi sangat penting dalam proses kinerja suatu instansi bahkan perusahaan, mengolah berbagai data yang didapat menjadi suatu informasi yang bisa dimengerti dengan mudah. Hal penting yang dilakukan sistem informasi adalah mengubah data yang sering disebut data mentah menjadi suatu informasi yang bernilai. Sistem informasi adalah serangkaian komponen berupa manusia, prosedur, data dan teknologi yang digunakan untuk melakukan sebuah proses yang berguana dalam pengambilan keputusan sebagai penunjang keberhasial di setiap instansi.

Sistem Informasi berisikan jaringan sistem pengolahan data yang dilengkapi dengan berbagai terusan dari komunikasi yang digunakan dalam sistem organisasi data. Sistem informasi memiliki elemen proses antara lain mengumpulkan data (*data gathering*), mengelola data yang tersimpan dan menyebarkan informasi. Sistem informasi juga dapat disebut kombinasi dari teknologi informasi dan aktivitas orang yang menggunakan teknologi tersebut sebagai pendukung tahapan oprasi dan manajemen. Sering digunakan untuk merujuk kepada interaksi antara orang, proses algoritmatik, data dan teknologi merupakan istilah yang sangat luas mengenai sistem informasi [15].

Dilansir dari *website* resmi STI Institut Teknologi Telkom Purwokerto, sistem Informasi Institut Teknologi Telkom Purwokerto atau sering disebut sisfo bagi mahasiswa, dosen dan pekerja lainnya merupakan unit yang mengelola urusan pelayanan civitas berupa layanan *i-Gracias, Learning Management System*, Kartu Tanda Mahasiswa, *Hotspot, Email* dan *Blog*. Bagian STI menyediakan berbagai layanan sistem dan teknologi informasi guna memberikan pelayanan yang prima, cepat dan tanggap dalam mendukung aktifivas kampus yang membutuhkan layanan

teknologi dan sisitem informasi. Dalam upaya memberikan layanan terbaik bagi civitas Institut Teknologi Telkom Purwokerto, STI ITTP terus memperhatikan indeks keamanan informasi guna menjaga sistem dan informasi teknologi tetap berfungsi dengan baik, bahkan meningkatkan keamanan layanan.

2.2.2 Indeks Keamanan Informasi

Indeks KAMI merupakan alat untuk mengukur tingkat persiapan pengamanan informasi di sebuah instansi. Alat evaluasi ini tidak diajukan untuk menganalisis kelayakan atau efektivitas bentuk pengamatan yang ada, melainkan sebagai perangkat untuk gambaran kondisi kesiapan, kelengkapan serta kematangan dari kerangka kerja keamanan informasi kepada pimpinan instansi [3]. Indeks KAMI menerapkan mekanisme pengukuran keamanan informasi suatu instansi mulai dari peran, tata Kelola, resiko keamanan, kerangka kerja, pengelolaan aset dan teknologi. Pengukuran tingkan keamanan informasi diperlukan untuk melihat secara menyeluruh hal-hal yang digunakan oleh instansi dalam melakukan tindakan pengamanan informasi di Institut Teknologi Telkom Purwokerto.

Bentuk evaluasi pada Indeks KAMI dirancang agar dapat digunakan oleh instansi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya tugas pokok dan fungsi yang ada. Data yang digunakan dalam evaluasi dapat memberikan potret indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat menjadi pembanding dalam rangka Menyusun Langkah perbaikan dan menetapkan prioritas [3].

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, yang disusun kembali menjadi 5 (lima) area di bawah ini [3]:

a. Tata Kelola Keamanan Informasi

   Melakukan evaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

b. Pengelolaan Risiko Keamanan Informasi

Melakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

c. Kerangka Kerja Keamanan Informasi

Melakukan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

d. Pengelolaan Aset Informasi

Melakukan evaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

e. Teknologi dan Keamanan Informasi

Melakukan evaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Setelah melakukan penilaian berdasarkan indeks KAMI maka akan diketahui tingkat kematangan dari setiap kriteria yang telah di identifikasi. Tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan kerangka kerj *COBIT* atau *CMMI*. *COBIT* adalah singkatan dari *Control Objective for Information and Related Technology* merupakan kerangka kerja yang dibuat oleh *Information System Audit and Control Associatin* untuk tata Kelola manajeman TI, sedangkan *CMMI* merupakan singkatan dari *Capability Maturity Model Integration* adalah kerangka kerja (*framework*) yang dapat digunakan untuk mengembangkan proses di dalam perusahaan. Terdapat lima tingkat kematangan pada indeks KAMI yaitu Tingkat I merupakan kondisi awal, Tingkat II berkaitan dengan kerangka kerja dasar, Tingkat III yaitu kegiatan instansi yang terdefinisi dan konsisten, Tingkat IV yaitu terkelola dan terstrukturnya kegiatan instansi dan Tingkatan V berkaitan dengan optimal [2].

Dalam mendapatkan hasil assessment indeks KAMI maka diperlukan perhitungan yang sudah memiliki tetapannya masing-masing. Pada perhitungan Tata Kelola Keamanan Informasi sudah ditetapkan pertanyaan seputar fungsi atau organisasi keamanan informasi berjumlah 22 pertanyaan yang masing masing pertanyaan memiliki keluaran ststus tidak dilakukan memiliki nilai skor 0, dalam ststus perencanaan memiliki skor 1, dalam status penerapan atau diterapkan

sebagaian memiliki skor 2, dan dalam status diterapkan secara menyeluruh memiliki skor 3. Maka dapat ditemukan total nilai evaluasi tata kelola dengan menjumlahkan keseluruhan skor pada Tata Kelola Keamanan Informasi. Tata kelola memiliki nilai skor minimum untuk tingkat kematangan II yaitu 12, tingkat kematangan III yaitu 8, tingkat kematangan IV yaitu 24. Pada perhitungan Pengelolaan Risiko Keamanan Informasi dilakukan kajian risiko keamanan informasi yang terdiri dari 16 pertanyaan dan tiap pertanyaan memiliki keluaran status tidak dilakukan dengan nilai skor 0, dalam status perencanaan memiliki nilai skor 2, dalam status penerapan atau diterapkan sebagian memiliki nilai skor 4, dan dalam status diterapkan secara menyeluruh memiliki nilai skor 6. Maka dapat ditemukan total nilai evaluasi pengelolaan risiko keamanan informasi dengan menjumlahkan keseluruhan skor pada kajian risiko keamanan informasi. Pengelolaan Risiko memiliki nilai skor minimum untuk tingkat kematangan II yaitu 14, tingkat kematangan III yaitu 4, tingkat kematangan IV yaitu 8, tingkat kematangan V yaitu 12. Sedangkan pada perhitungan Kerangka Kerja Pengelolaan Keamanan Informasi dilakukan penyusunan dan pengelolaan kebijakan serta prosedur keamanan informasi yang terdiri dari 19 pertanyaan dan 10 pertanyaan untuk mengevaluasi pengelolaan strategi dan program keamanan informasi. Pada tiap pertanyaan memiliki keluaran ststus tidak dilakukan dengan nilai skor 0, dalam status perencanaan memiliki nilai skor 3, dalam status penerapan atau diterapkan sebagian memiliki nilai skor 6, dan pada status diterapkan secara menyeluruh memiliki nilai skor 9. Kerangka Kerja Pengelolaan Keamanan Informasi memiliki nilai skor minimum untuk tingkat kematangan II yaitu 15, tingkat kematangan III yaitu 45, tingkat kematangan IV yaitu 15, dan tingkat kematangan V yaitu 12. Pada penilaian Pengelolaan Aset Informasi dilakukam evaluasi kelengkapan pengamanan aset informasi termasuk keseluruhan siklus penggunaan aset melalui 38 pertanyaan dengan keluaran status tidak dilakukan dengan skor 2, status dalam perencanaan dengan skor 4, status dalam penerapan atau diterapkan sebagian dengan skor 6, status diterapkan secara menyeluruh dengan skor 8. Pengelolaan Aset Informasi memiliki skor minimum tingkat kematangan II yaitu 25 dan minimum skor tingkat kematangan III yaitu 35. Sedangkan menentukan penilaian

pada teknologi dan keamanan informasi dengan cara menjawab 26 pertanyaan yang memiliki keluaran status tidak dilakukan dengan nilai skor 0, dalam status perencanaan memiliki nilai skor 2, dalam status penerapan atau diterapkan sebagian memiliki nilai skor 4, dan pada status diterapkan secara menyeluruh memiliki nilai skor 6. Teknologi dan Keamanan Informasi memiliki nilai skor minimum untuk tingkat kematangan II yaitu 18, tingkat kematangan III yaitu 40, tingkat kematangan IV yaitu 15, dan tingkat kematangan V yaitu 6.

Keamanan informasi bagian yang harus dijalankan agar sistem tersebut terhindar dari segala macam risiko. Sistem informasi wajib memiliki pengaman serta pengendalian agar dapat meminimalisir terjadinya pencurian dan penyalahgunaan terhadap berbagai data yang dapat merugikan instansi. Berbagai ancaman internal, yaitu ketidaktahuan, ketidakpatuhan, memberikan atau bertukar password. Sedangkan pada ancaman eksternal, yaitu *virus, spyware, hacker* dan kegiatan penyusupan lainnya merupakan gambar sebuah struktur organisasi yang terdiri dari macam-macam komponen pendukung relasinya.

2.2.3 *Business Impact Analysis (BIA)*

Business Impact Analysis (BIA) merupakan alat bantu untuk mengidentifikasi garis besar proses bisnis serta kemungkinan risiko yang dapat timbul pada proses bisnis tersebut sebagai landasan sebelum membuat strategi pemulihan. *BIA* bukan merupakan alat bantu untuk membuat strategi pemulihan (*Recovery Strategy*) pada proses bisnis setelat terjadi bencana atau gangguan. *BIA* adalah kumpulan pengaruh akibat terjadinya sistem yang tidak berfungsi. *BIA* merupakan hal pokok yang harus dipertimbangkan agar oprasional dapat berjalan dengan normal, oleh karena itu kumpulan dampak yang terjadi harus di Analisa menggunakan *BIA*.

Analisa dampak bisnis adalah pemahaman akan proses mana yang vital dalam suatu bisnis untuk berjalannya oprasional serta mengerti dampak dari ketergantungan berbagai proses tersebut [16]. Pengaruh dari sistem yang tidak berfungsi adalah hal pokok yang harus dipertimbangkan agar oprasional dapat berjalan dengan normal, oleh sebab itu berbagai dampak yang terjadi harus dianalisa menggunakan *Business Impact Analysis*. Selain berbagai hal yang

disebutkan diatas, *BIA* juga dapat membantu instansi dalam memahami potensi kerugian bahkan dampak lain yang tidak diharapkan [17]. *BIA* mengumpulkan data berdasarkan tingkat gangguan [18].

Tahapan dalam pencarian *business impact analist* yaitu setelah dilakukannya *risk assessment* yang dapat membantu peneliti dalam mengetahui bencana yang akan terjadi yang perlu di analisa lebih dalam mengenai dampak dari tiap sub sistem yang ada bencana tersebut [10]. Dampak adalah hal-hal yang kemungkinan akan terjadi, dengan menganalisa dampak akan membentuk gambaran apasaja yang akan terjadi saat terjadinya bencana.

Setiap Instansi memiliki faktor kunci yang menjadi acuan dari proses bisnis didalamnya, hal yang wajib dilakukan adalah memahami serta memelihara faktor tersebut sebaik baiknya. Instansi yang memiliki risiko terbesar dari tingkat kerugian yang dihasilkan, maka didalamnya terdapat berbagai faktor kunci yang perlu lebih lanjut dimengerti oleh pihak penyusun *Disaster Recovery Plan*. Salah satu metode terbaik untuk mengidentifikasi faktor kunci yang berpengaruh dalam proses bisnis adalah dengan menggunakan analisa risiko. *BIA* bertujuan menghubungkan antara komponen sistem secara spesifik terhadap layanan kritis yang disediakan dan menyatakan karakteristik dari akibat yang muncul terhadap gangguan pada komponen sistem tersebut.

2.2.4 *Disaster Recovery Plan*

Seringkali kesalahan mendasar suatu instansi adalah menggampangkan peristiwa yang akun terjadi, sehingga tidak membuat perencanaan pemulihan bencana. Berfikir peristiwa buruk tidak akan terjadi, merasa dapat menanggulangi masalah, merasa keamanan informasi yang dimiliki terlalu besar dan canggih untuk gagal, merasa bukan target *cyber*, mengandalkan asuransi saat terjadi peristiwa buruk terhadap keamanan informasi. Perencanaan pemulihan bencana atau *Disaster Recover Plan (DRP)* adalah bagian dari *business continuity* yang berkaitan langsung dengan dampak yang dihasilkan dari bencana atau peristiwa yang terjadi. *DRP* membantu instansi saat pemulihan pemadaman *server*, pelanggaran keamanan

bahkan bencana alam seperti angin topan, gempa, banjir, tanah longsor yang merupakan kategori ancaman.

Disaster Recovery Plan adalah rencana tertulis yang menggambarkan langkah langkah yang akan diambil perusahaan atau instansi guna memulihkan operasi komputer jika terjadi bencana. Setiap perusahaan, depertemen, maupun instansi baiknya memiliki sendiri rancangan *Disaster Recovery Plan*. *DRP* sebagai acuan yang berisikan prosedur guna mengatasi hilangnya sumber daya sistem informasi dalam sebuah perusahaan yang diakibatkan oleh bencana, tersedia oprasi cadangan selama sistem utama berhenti, serta mengelola proses pemilihan dan penyelamatan data untuk meminimalisir kerugian yang dialami perusahaan [6].

Disaster Recovery Plan merupakan bagian dari *Business Continuity Plan* dijadikan acuan yang berisikan prosedur guna merespon kejadian yang mengakibatkan hilangnya sumber daya sistem informasi oleh bencana, menyediakan operasi cadangan selama sistem terhenti, dan mengelola proses pemulihan serta penyelamatan sehingga dapat meminimalisir kerugian yang terjadi pada instansi. Sebagai pegangan saat terjadinya keadaan darurat, *Disaster Recovery Plan* tidak dapat disusun secara sembarangan, *Disaster Recovery Plan* yang tidak sesuai dapat berakibat lebih buruk bagi keberlangsungan instansi daripada bencana itu sendiri. *Disaster Recovery Plan* menyediakan kemampuan dalam menerapkan proses kritis di lokasi lain dan mengembalikannya ke lokasi dan kondisi semula dengan batasan waktu yang singkat, sehingga dapat memperkecil kerugian kepada instansi, dengan pelaksanaan prosedur *recovery* yang cepat [7].

DRP merupakan langkah tepat dalam membangun penanganan gangguan dan bencana terhadap infrastruktur sistem layanan teknologi informasi pada suatu institusi. Perancangan ini diperlukan guna meminimalisir dampak risiko yang terjadi terhadap ancaman bencana yang mengancam infrastruktur layanan IT [19]. *DRP* akan melakukan kegiatan yang harus dilakukan dalam penanganan bencana. Rancangan pemulihan bencana ini akan menyediakan cara yang efektif dan efisien untuk pulih dari bencana yang mempengaruhi sistem TI dalam organisasi. Kerugian

bencana dapat diminimalisir dengan menyusun DRP yang baik pada setiap subsistem bisnis dan oprasi dalam suatu instansi [20].

Setiap bencana memiliki satu bahkan lebih sebab dan akibat. Dapat disebabkan oleh manusia atau mekanis, alami, bahkan dapat terjadi dari kasus sederhana seperti *micro hardware* atau komponen *software* yang tidak dapat berfungsi pada peristiwa bencana alam seperti gempa bumi, kebakaran dan banjir. Efek dari bencana yang ditimbulkan berkisar dari gangguan kecil hingga penutupan bisnis proses secara keseluruhan selama berhari-hari bahkan berbulan-bulan. Sasaran pokok *Disaster Recovery Plan* adalah untuk menyediakan kemampuan dalam menerapkan proses kritis di lokasi lain dan mengembalikannya ke lokasi dan kondisi semula dalam suatu batasan waktu yang memperkecil kerugian kepada instansi, dengan pelaksanaan prosedur *recovery* yang cepat.

Apabila suatu instansi ingin memiliki keberlangsungan layanan dan siap untuk menghadapi bencana, minimal memiliki enam komponen *IT DRP*, yaitu struktur organisasi, *risk assessment* dan *BIA*, strategi *recovery*, fasilitas dan teknologi, pelatihan dan pengujian dan administrasi perencanaan. Terdapat siklus penyusunan *DRP*, diawali dengan penetapan kebijakan *disaster recovery* bertujuan menganalisa konteks instansi, penetapan lingkungan *disaster recovery*, penyusunan kebijakan *disaster recovery*, persetujan dan publikasi. Setelah itu, lakukan *risk assessment* dan *business impact analysis* bertujuan mengidentifikasi proses bisnis prioritas, penetapan kontrol pencegahan pada aset TI, penetapan *RTO, RPO, MTD*, penilaian dampak bisnis dan memprioritaskan proses bisnis dan aset [19]. Berikutnya lakukan penyusunan disaster recovery plan berisi identifikasi strategi untuk recovery dan penyusunan *disaster recovery plan*. Siklus terakhir adalah testing, pemeliharaan dan audit.

2.2.5 *Risk Management*

Risk Management adalah proses identifikasi, pengukuran dan kontrol dari sebuah risiko yang mengancam aset dan dapat mengakibatkan kerugian penghasilan dari sebuah instansi atau proyek [21]. *Risk Management* merupakan suatu bidang ilmu yang menempatkan berbagai pendekatan manajemen secara lengkap serta

sistematis yang membahas tentang bagaimana suatu instansi menerapkan ukuran dalam memetakan berbagai masalah yang ada. *Risk Management* merupakan proses menghilangkan risiko yang tidak dapat diterima dengan mengidetifikasi, menganalisis, mengevaluasi, mengendalikan, menghindari dan meminalisir terjadinya risiko [22]. Berikut beberapa langkah awal yang harus dilakukan dalam *Risk Management* yang mengidentifikasi aset lalu mengidentifikasi risiko:

a. *Threats* (Identifikasi ancaman)

   Identifikasi ancaman merupakan tahap pembuatan daftar ancaman yang dapat terjadi ke suatu instansi. Dalam mengidentifikasi ancaman ada beberapa kategori ancaman yang harus diperhatikan, yaitu ancaman tersebut berasal dari internal dan eksternal instansi (*Internal or External*), ancaman disebabkan oleh kejadian alami atau buatan manusia (*Natural or man-made-Natural*) dan ancaman terjadi secara disngaja atau tidak di sengaja (*Intentinal or Accidental*) [23].

b. *Vulnerabilities* (Identifikasi Kerentanan)

   Saat terjadi ancaman pada suatu instansi maka aka nada kerentanan. Berikut beberapa cara untuk mengidentifikasi kerentanan, antara lain [23].

   1. *Audit*, hal ini dilakukan untuk memverifikasi sitem dan proses dari suatu instansi, bahwa instansi tersebut mematuhi aturan dan hukum yang ada.
   2. Catatan sertifikasi dan Akreditasi, hal ini dilakukan untuk mengidentifikasi potensial dan kelemahan yang ada di suatu instansi.
   3. *System Log*, dalam mengidentifikasi ancaman juga dapat dilakukan menggunakan Log. Hal ini berguna untuk mengetahui mengetahui aktivitas lalu lintas yang mencoba menembus jaringan dan mengabil data sensitive.
   4. Kejadian Sebelumnya, *history* atau kejadian yang lalu sangan membantu dalam dalam kontrol kejadian yang terulang kembali.
   5. Laporan Masalah, sebagian besar instansi mengidentifikasi kelemahan menggunakan database untuk mendokumentasi masalah.
   6. Tim Responden Insiden, beberapa instansi mengidentifikasi insiden kelemahan yang terjadi pada instansi mereka. Tim ini seringkali

membantu mengurangi risiko yang terjadi. Hanya beberapa instansi saja yang menerapkan atau mempunyai Tim Respon Insiden.

c. Menggunakan tujuh domain dari infrastruktur TI untuk mengidentifikasi kelemahan [23].

1. *User Domain*, keamanan *link* akan melemah jika tidak di protrksi. Misalnya *password* enkripsi atau dikonversi menjadi kode rahasia agar tidak mudah di retas.
2. *Workstation Domain*, domain ini akan rentan terkena eksploitasi jika tidak mengunakan antivirus sehingga akan lebih mudah untuk terinfeksi.
3. *LAN Domain*, setiap perangkat individu dijaringan harus terlindungi. Misal kata sandi yang lemah akan mudah dipecahkan dan mendapat izin akses yang tidak sah.
4. *LAN-to-WaN Domain*, saat pengguna mengunduh *software* yang berbahaya dari web, makan dapat memungkinkan memberikan akses ke jaringan internal dari internet.
5. *WAN Domain*, unggahan *anonym* dari *server file transfer protocol* (FTP) yang memungkinkan dapat melakukan *hosting warez* dari peretas *blackhat*.
6. *Remote access Domain*, virus akan lebih mudah menginfeksi perangkat computer Ketika perangkat tersebut terhubung dengan jaringan internet jarak jauh tanpa diketahui oleh penggunannya.
7. *System/application Domain*, *server* basis data juga dapat terkena serangan injeksi *SQL*, dimana serangan injeksi *SQL* tersebut dapat merubah data yang ada di dalam database.

d. *Likehood* (Perkiraan kemungkinan ancaman mengeksploitasi kerentanan)

Untuk mengurangi risiko harus menyesuaikan antara ancaman dengan kerentanan. Agar dapat menyesuaikan ancaman dengan kerentanan formula yang dapat digunakan yaitu dengan mengkalikan *Threat* dengan *Vulnerability*, maka akan mendapatkan risiko dari hasil perkalian tersebut. Jika nilai aset dapat diidentifikasi maka rumus atau formula yang digunakan

yaitu dengan mengkalikan antara *Threat, Vulnerability* dan aset. Dengan menengendalikan ketiga hal tersebut akan mendapatkan hasil yang berupa total risiko [23].

2.2.6 *Risk Assessment*

Risk Assesment adalah proses untuk mengidentifikasi potensi bahaya serta menganalisis peristiwa berbahaya yang dapat terjadi [24]. Pada tahapan ini, setiap ancaman bencana yang sudah teridentifikasi akan diberi nilai disetiap atribut serta mengidentifikasi berbagai ancaman yang mungkin terjadi dari internal maupun eksternal perusahaan. Proses ini berguna untuk mengumpulkan informasi dan mengevaluasi kemungkinan dan konsekuensi dari berbagai jenis bahaya di perusahaan dan menentukan tindakan pengendalian risiko yang tepat untuk mengurangi risiko ke tingkat yang dapat diterima.

Pada *risk assessment* membahas berbagai aset dan seperti apa potensi risiko keberlangsungan pada aset. Setelah mengetahui potensi risiko, maka perlu mempersiapkan *contol preventive*. Mengidentifikasi pengendalian pencegahan adalah langkah langkah yang bertujuan untuk mengurangi efek dari gangguan sistem dan dapat meningkatkan ketersediaan sistem dan mengurangi biaya [25]. Potensi risiko akan lebih kecil jika mempersiapkan control preventive diawal. *Preventive contols* terbagi menjadi enam elemen, yaitu *fire suppression system, sensor air* di *data center, emergency master system shutdown switch, offsite backup media (non electronic record), technical security controls (cryptography and access control)* dan *backup data*.

2.2.7 *Recovery Time Objective (RTO)*

Recovery Time Objective adalah waktu maksimum sebuah sistem untuk down sebelum adanya dampak yang tidak diinginkan dari rangkaian sistem lainnya yang mendukung proses bisnis sebuah instansi [7]. RTO juga berarti waktu yang tersedia untuk memulihkan suatu sistem dan sumber daya dari operasional TI akibat bencana yang terjadi.

2.2.8 *Recovery Point Objective (RPO)*

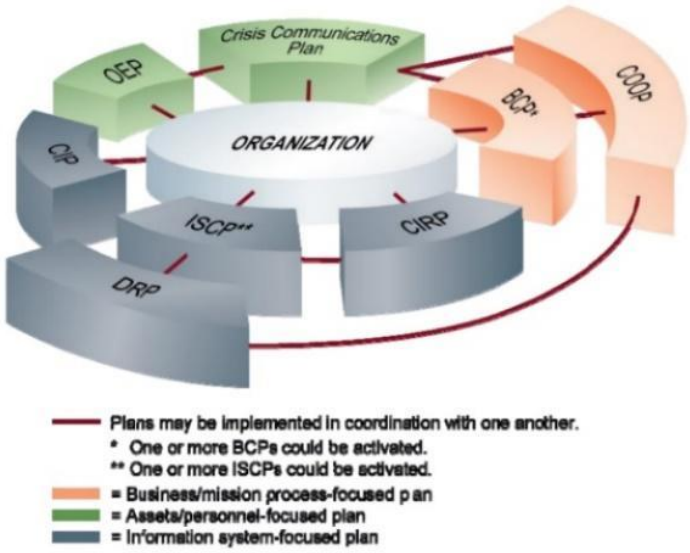
Recovery Point Objective adalah jumlah toleransi minimum data dari sebuah system yang dapat di perbarui dari proses pemulihan yang dilakukan [7]. RPO juga bermakna jumlah waktu maksimal atas kehilangan data dari proses bisnis yang sedang berjalan. RPO dapat ditoleransi oleh instansi.

2.2.9 Prioritas *Recovery*

Pada tahapan menentukan prioritas maka diperlukann *Business Impact Analysis (BIA)*. Penilaian dampak risiko dilihat berdasarkan sistem informasi yang menjadi acuan penilaian yaitu layanan *i-Gracias, Learning Management System*, Kartu Tanda Mahasiswa, *Hotspot*, *Email* dan *Blog*. Setelah mendapatkan nilai dampak yang ada maka di tentukan prioritas pemulihan sistem.dalam membuat tingkat prioritas yaitu menggabungkan nilai dampak dari setiap sistem, penjabarannya dengan kategori tinggi memiliki 3 poin, kategori sedang memiliki 2 poin, dan kategori rendah memiliki 1 poin [26]. Jika nilai rata-rata dampak tinggi maka diasumsikan menjadi prioritas pemulihan utama. Penyusunan dokumen DRP dapat membantu pemulihan sistem informasi apabila terjadi suatu bencana dengan tingkat prioritas risiko dampak yang terjadi.

2.2.10 *NIST 800-34*

Tahapan dalam perancangan disaster recovery plan dapat dilakukan dengan kerangka kerja NIST 800-34 yang diinisiasi oleh risk assessment, bussines impact analysis dan strategy recovery [11]. NIST 300-34 merupakan satu dari sekian dokumen yang berasal dari National Institute of Standars and Technology (NIST). Kerangka kerja ini berasal berisi rekomendasi, petunjuk dan pertimbangan Ketika Menyusun rencana kontigensi [27]. NIST 800-34 diterbitkan pada tahun 2010 pada bulan Mei [25]. Secara teknis tahapan dalam perancangan DRP dengan kerangka kerja NIST 800-34 terdapat pada gambar berikut.



(Lampiran 5) Gambar 2. 1 Kerangka Kerja NIST 800-34.

Pada gambar 2.1 memuat beberapa prosedur yaitu *Business Continuity Plan (BCP)* dan *BIA*, sehingga menghasilkan *DRP*. Ada beberapa hal yang harus diperhatikan dalam perancangan *DRP*, antara lain strategi apa yang digunakan dalam pemulihan aset teknologi atau sistem informasi, teknologi yang digunakan pada masing-masing teknologi atau sistem informasi, dan bagaimana tim yang dilibatkan dalam pelaksanaan kegiatan perancangan pemulihan bencana. Dalam *NIST 800-34* terdapat proses pemulihan bencana yang dibagi menjadi tiga bagian, yaitu [25]:

a. *Activation and Notification*

Tahap ini merupakan tahap pengambilan keputusan ketika terjadi bencana dan memberitahukan kejadian tersebut kepada tim pemulihan anggota untuk mengimplementasikan IT-DRP. Pada akhir tahap ini, tim pemulihan harus siap untuk melakukan proses pemulihan yang direncanakan.

b. *Recovery*

Bagian ini adalah tahap memulihkan layanan sistem dan teknologi informasi secara keseluruhan sehingga proses bisnis dapat berjalan lagi. Pada akhir tahap ini, sistem informasi dan teknologi sudah berjalan lancar.

c. *Recontruction*

Tahap ini merupakan tahap dimana semua sistem telah berhasil restart meskipun sementara. Terlebih lagi, pada tahap ini, semua kegiatan

operasional dikembalikan ke kondisi awal sebelum bencana terjadi. Jika fasilitas awal tidak dapat dipulihkan, maka siapkan yang baru fasilitas dan tempat sesuai dengan kegiatan yang direncanakan pada tahap ini.