# BAB II
# TINJAUAN PUSTAKA DAN LANDASAN TEORI

## 2.1 Tinjauan Pustaka

Tinjauan pustaka dalam penelitian penting dilakukan karena didalam kajian pustaka berisi referensi yang relevan dengan tema penelitian yang diambil. Pada bab tinjauan pustaka ini menguraikan teori, temuan, dan bahan penelitian lain yang mengarahkan untuk menyusun kerangka konsep yang akan digunakan pada penelitian ini. Tinjauan pustaka ini didapatkan melalui *review* jurnal penelitian yang sejenis menggunakan *Business Continuity Plan (BCP).* Berikut ini Tabel 2.1 yang memaparkan penelitian terdahulu yang relevan dengan penelitian ini yang berkaitan dengan BCP :

**Tabel 2. 1 Penelitian Terdahulu BCP**

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| 1 | Penerapan *Business Continuity Management* Pada Masa Pandemi Covid-19 di PT | Penelitian ini dilakukan dengan tujuan untuk menilai risiko yang memiliki tingkat paling tinggi dalam penerapan *Business Continuity* | Penelitian ini menyusun *Business Continuity Management* yang bertujuan untuk membangun strategi keamanan informasi | Pengumpulan data pada penelitian ini dilakukan dengan wawancara hanya dengan direktur unit dan diberikan data berupa eksplorasi | Penelitian yang sudah dilakukan ini menggunakan standar ISO 22301 dengan metode *Failure Mode and Effect Analysis* | Berdasarkan penelitian yang sudah dilakukan ini menghasilkan bahwa terdapat enam risiko dengan level sangat tinggi 75% untuk *Business Continuity* |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | Brantas Abipraya[11] | *Management* Masa Pandemi Covid-19 di PT Brantas Abipraya. | perusahaan ketika ada bencana dengan standar ISO 22301 sebagai dasar perancangan BCM. Sedangkan penelitian yang akan dilakukan bertujuan untuk menilai dan mengidentifikasi risiko dari keamanan informasi organisasi pendidikan menggunakan *Business Continuity Plan.* | alasan dari pelaku pelanggaran yang tidak melaksanakan peraturan yang ditetapkan oleh perusahaan. | (FMEA) yang akan menghasilkan *Risk Probability Number* (RPN). | *Management* PT Abipraya selama Covid-19. |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| 2 | Perancangan *Business Continuity Plan* dan *Disaster Recovery Plan* Teknologi dan Sistem Informasi Menggunakan ISO 22301[12] | Penelitian ini berfungsi untuk menstabilisasi proses bisnis perusahaan ketika ada bencana sehingga tidak mengalami gangguan pada proses bisnisnya menggunakan metode *Business Continuity Plan* dan *Disaster Recovery Plan* dengan *framework* ISO 22301. | Penelitian ini tidak hanya dilakukan menggunakan metode *Business Continuity Plan* tetapi juga *Disaster Recovery Plan* yang berfungsi untuk mencegah dampak dari adanya gangguan yang terjadi dan risiko yang dapat mengganggu proses bisnis organisasi dengan *framework* ISO 22301. Sedangkan penelitian yang akan dilakukan untuk menguji dan | Pengumpulan data pada penelitian ini dilakukan dengan wawancara, dokumentasi, dan kuesioner. Jumlah responden kuesioner tidak ditulis jumlahnya secara jelas hanya diberikan kepada pengguna teknologi dan kepala TI. | Analisis pada penelitian ini berdasarkan *framework* ISO 22301 dengan melakukan siklus *Plan*, *Do*, *Check*, dan *Act* (PDCA) menggunakan 10 klausal yang harus dianalisis. | Hasil penelitian ini berdasarkan analisis metode *Business Continuity Plan* bahwa Rumah Sakti Ananda Purwokerto belum menerapkan secara keseluruhan *Business Continuity Plan* sehingga dirancang dan disusun sebuah dokumen yang megacu ISO 22301 klausul 4,5,6, dan 7. |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | | mengidentifikasi keamanan informasi layanan pada perguruan tinggi berdasarkan klausul dari *Business Continuity Plan* standar ISO 22301dan mengacu pada kerangka BCP Griffith University. | | | |
| 3 | Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan | Penelitian ini dilakukan untuk menganalisis, melakukan pemetaan, meninjau skala prioritas terhadap | Penelitian ini dilakukan untuk mengevaluasi dan memahami kondisi tata kelola keamanan teknologi informasi | Pengumpulan data pada penelitian ini tidak disertakan dengan jelas sumbernya tetapi memberikan tabel | Penelitian ini dilakukan dengan melakukan *assessment* dan memetakan kesenjangan | Hasil dari penelitian ini adalah Diskominfotik Kabupaten Bandung Barat masih jauh dalam pemenuhan syarat sesuai dengan standar |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2014 (Studi Kasus Diskominfotik Kabupaten Bandung Barat)[13] | risiko yang timbul kemudian Menyusun dokumen sesuai standar ISO 27001:2013 yang dapat direkomendasikan yang mendukung proses bisnis perusahaaan. | dan meninjau skala prioritas terhadap risiko yang ada pada Diskominfotik Kabupaten Bandung Barat berdasarkan standar ISO 27001:2013. Sedangkan penelitian yang akan dilakukan untuk menguji keamanan teknologi informasi pada layanan pada organisasi pendidikan mengacu pada metode *Business Continuity Plan* dan klausul ISO | hasil dari *assessment* kesesuaian standar ISO 27001:2013. | terhadap risiko berdasarkan klausal ISO 27001:2013. | ISO 27001:2013 dan profil risiko masih belum dimitigasi. |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | | 22301 serta berdasarkan kerangka BCP Griffith University. | | | |
| 4 | Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang atau Jasa Secara Elektronik (LPSE) di Dinas Komunikasi | Penelitian ini dilakukan melalui tahap pembangunan SMKI dengan tujuan agar keamanan informasi pada layanan LPSE dapat terjamin proses bisnisnya dengan baik, mengurangi dampak risiko, dan terjada dari aspek kerahasiaan, keutuhan, dan | Penelitian ini dilakukan karena adanya permasalahan yang sering terjadi pada infrastruktur TI Unit LPSE yang mengganggu berjalannya proses bisnis perusaan disebabkan kurangnya kesadaran akan pentingnya keamanan informasi. Sedangkan | Data yang digunakan sebagai pendukung berhasilnya penelitian ini yaitu dengan melakukan wawancara bersama kepala unit LPSE dan beberapa kabid terkait, observasi secara langsung ke LPSE Dinas Kominfo Kabupaten Cianjur, dan kuesinoer yang | Penelitian ini disusun berdasarkan analisis SMKI dan evaluasi keamanan informasi berdasarkan klausul SNI ISO 2700:2013. | Hasil dari penelitian yang sudah dilakukan ini adalah sebuah kerangka kerja SNI ISO/IEC 27001:2013 terdapat 21 klausul pemetaan terhadap layanan LPSE Dinkominfo Kabupaten Cianjur. |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | dan Informatika Kabupaten Cianjur Dengan Menggunakan SNI ISO/IEC 27001:2013[14] | ketersediaan yang disusun berdasarkan standar SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 27005:2013. | penelitian yang akan dilakukan untuk mengidentifikasi risiko dan meninjau keamanan informasi standarisasi ISO 22301 dan mengacu pada kerangka BCP Griffith University.. | disebarkan hanya kepada sekretaris kepala unit LPSE, bidang administrasi, bidang registrasi, dan verifikasi saja. | | |
| 5 | *Business Continuity Plan Using ISO 22301:2012 In IT Solution Company (PT ABC)*[15] | Penelitian ini dilakukan dengan tujuan untuk memelihara dan mengevaluasi layanan *cloud* dan pusat data milik PT ABC yang mendukung | Penelitian ini dilakukan dengan tujuan untuk memenuhi GAP standarisasi ISO 22301:2012 pada layanan *cloud* dan pusat data milik PT | Porses pengumpulan data pada penelitian ini yaitu dengan melakukan review dokumen kemudian melakukan interview dengan direktur teknis dan manajem sumber | Penelitian ini dirancang dengan menyusun dokumen didukung dengan *framework Operational Critical Threat Asset dan Vulnerability* | Hasil dari penelitian ini yaitu menghasilkan nilai yang menunjukkan bahwa PT ABC siap untuk menerapkan ISO 22301:2012 karena 47,6% GAP sudah terpenuhi dan 11,88% |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | kelangsungan proses bisnisnya sehingga membutuhkan dokumen *Business Continuity Plan* dengan standar ISO 22301:2012. | ABC. Sedangkan penelitian yang akan dilakukan bertujuan untuk mengidentifikasi risiko dan meninjau keamanan informasi standarisasi ISO 27001. | daya manusia saja. | *Evaluation (OCTAVE)* dan dirumuskan menggunakan diagram MED. | tidak sesuai dengan proses inisiasinya sehingga siap diterapkan tetapi perlu ada evaluasi lanjutan. |
| 6 | *Business Continuity Management Impementation in the Malaysian Public Sector*[16] | Penelitian ini dilakukan bertujuan untuk membentuk sebuah kerangka pengimplementasian *Business Continuity Management* (BCM) di public sektor | Penelitian ini untuk mengidentifikasi faktor yang mempengaruhi implementasi terbaik terbaik BMC di organisasi sesuai standar ISO 27001. | Pengumpulan data pada penelitian ini dengan melakukan wawancara terhadap praktisi BMC dari Pemerintah dan menyebarkan kuesioner dengan 38 | Analisis data pada penelitian ini menggunakan bantuan alat statistic yaitu IBM *Statisctical Package for the Social Science* (SPSS) | Hasil penelitian ini yaitu memperoleh hasil perhItungan angka 57,9% dianggap relatif baru dalam penerapan BMC pada proses bisnis organisasi dan 42,1% program BMC |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | Malaysia. | Sedangkan penelitian yang akan dilakukan bertujuan untuk mengidentifikasi risiko dan meninjau keamanan informasi organisasi pendidikan mengacu pada metode *Business Continuity Plan* dan klausul ISO 22301 serta berdasarkan kerangka BCP Griffith University. | tanggapan saja yang bisa diterima dan digunakan sebagai pendukung penelitian. | Version 20 dan menggunakan Cronbach's Alpha untuk skala koefisien realibitas. | pada organisasi sudah dianggap matang dan diimplementasikan lebih dari 3 tahun. |
| 7 | Information SecurTIy Assessment | Penelitian ini dilakukan bertujuan untuk mengukur | Penelitian ini dilakukan menggunakan objek | Penelitian ini menggunakan teknik triangulasi yaitu | Analisis data penelitian ini menggunakan GAP | Hasil penelitian ini memberikan informasi bahwa sistem informasi |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | Using ISO/IEC 27001:2013 Standard On Government Institution[17] | tingkat kematangan layanan pada sistem informasi yang dimiliki oleh pemerintah X dan meninjau GAP yang ada dengan tujuan mendapatkan sertifikasi ISO/IEC 27001:2013. | instansi pemerintah dengan tujuan untuk mengukur tingkat kematangan dan mendapatkan sertifikasi ISO/IEC 27001:2013 pada layanan sistem informasi instansi. Sedangkan penelitian yang akan dilakukan bertujuan untuk mengidentifikasi risiko dan meninjau keamanan informasi organisasi pendidikan mengacu pada metode *Business Continuity* | melakukan wawancara, observasi, dan dokumentai untuk penunjang validasi data yang dibutuhkan. | Analisis dan *CapabilTIy MaturTIy Model for Integration* (CMMI) untuk mengukur tingkat kematangan pada layanan sistem informasi pemerintah X. | yang diterapkan pada pemerintah X belum sesuai dengan standar ISO/IEC 27001:2013 karena berdasarkan analisis dan validasi data terdapat 114 kontrol objektif hanya ada 56.14% saja yang sudah diterapkan. Sedangkan berdasarkan tingkat kematangannya menunjukkan bahwa lampiran terkecil terdapat pada kebijakan keamanan informasi dan lampiran terbesar pada *Human Resource* |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | | *Plan* dan klausul ISO 22301 serta berdasarkan kerangka BCP Griffith University. | | | *Security*. |
| 8 | Perancangan *Disaster Recovery Plan* Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34[18] | Penelitian ini dilakukan dengan tujuan untuk melindungi sistem selama pengimplementasian pendukung proses bisnis organisasi terutama ketika terjadi gangguan dengan menyusun dokumen *Disaster Recovery* | Penelitian dilakukan dengan menyusun dokumen *Disaster Recovery Plan* dengan pendekatan kerangka kerja NIST 800-34 yang tujuannya untuk melindungi sistem informasi selama pengimplementasian pendukung proses bisnis organisasi | Penelitian ini tidak menjelaskan jumlah narasumber yang dimintai informasi terkait topik dan permasalahan yang sesuai dan tidak menuliskan sumber studi dokumen dengan jelas. | Penelitian ini seharusnya menjelaskan detail sumber data sebagai penunjang penelitian yang dilakukan dan dibagian kesimpulan menjelaskan detail dari hasil secara keseluruhan dalam penelitian ini. | Hasil penelitian yang disusun ini berupa dokumen DRP yang menghasilkan 9 rancangan *Strategy Recovery* terhadap ancaman terhadap sistem dan 8 sub sistem SISAK POLSRI. Dua sub sistem terdapat skala priorTIas yairu Sistem Kepegawaian |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | *Plan* dengan pendekatan kerangka kerja NIST 800-34. | pendidikan terutama ketika terjadi gangguan. Sedangkan penelitian yang akan dilakukan bertujuan untuk mengidentifikasi risiko dan meninjau keamanan informasi organisasi pendidikan mengacu pada metode *Business Continuity Plan* dan klausul ISO 22301 serta berdasarkan kerangka BCP Griffith University. | | | (SIMPEG) dan E-Regist Mahasiswa Baru Polsri dengan nilai 100% dan 92%. |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| 9 | Pelatihan Penyusunan Dokumen Keamanan Data di Bisma Informatika Indonesia[19] | Penelitian sebelumnya ini memiliki persamaan dengan penelitian yang akan dilakukan yaitu untuk memahami kondisi layanan sistem informasi saat ini yang mencakup SDM, teknologi, dan pendukung proses bisnis menggunakan lingkup PDCA dan objek yang dTIelTIi yaitu organisasi pendidikan. | Penelitian sebelumnya ini bertujuan untuk memahami kondisi layanan sistem informasi saat ini yang mencakup SDM, teknologi, dan pendukung proses bisnis mengguankan kerangka ISO 27001, analisis GAP, dan menggunakan KAMI untuk evaluasi. Sedangkan penelitian yang akan dilakukan bertujuan untuk mengidentifikasi risiko dan meninjau | Penelitian sebelumnya ini tidak menjelaskan hasil GAP kondisi data yang diperoleh ketika melakukan observasi dan wawancara bersama narasumber. | Penelitian ini seharusnya memberikan penjelasan detail mengenai kondisi saat ini ketika observasi dan wawancara bersama narasumber sehingga dapat dibuat tabel perbandingan dengan hasil analisis menggunakan PDCA ISO 27001 dan menyesuaikan dengan indeks KAMI. | Hasil penelitian sebelumnya ini adalah adanya perbaikan tatakelola keamanan data dengan adanya prosedur keamanan data berupa backup data dan implementasi berdasarkan indeks KAMI dan secara periodek berdasarkan PDCA. |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | | | keamanan informasi organisasi pendidikan mengacu pada metode *Business Continuity Plan* dan klausul ISO 22301 serta berdasarkan kerangka BCP Griffith University. | | | |
| 10 | Tinjauan Kesiapan Terhadap Implemetasi Business Continuity Management Systems (BCMS) | Penelitian sebelumnya memiliki persamaan dengan penelitian yang akan dilakukan yaitu menyusun dokumen BCMS dengan standar ISO 22301 dan ISO 27001 dengan tujuan untuk | Penelitian sebelumnya ini menyusun BCMS dengan standar ISO 22301 pendekatan control objective, ISO 27001 untuk Information SecurTIy of BCMS, menyusun analisis GAP, dan | Pengumpulan data pada penelitian sebelumnya ini dilakukan dengan wawancara dan kuesioner. Membuat pertanyaan wawancara sebanyak 83 tetapi perlu ada data yang | Penelitian ini menambahkan 49 pertanyaan menggunakan materi *in-depth-interview* dan *control objective* ISO 27001 untuk mendapatkan infomasi yang lebih | Hasil penelitian yang sudah dilakukan ini yaitu dari 83 pertanyaan kuesioner terdapat 51.81% bersifat Comply dan sisanya bernilai 48.19%. nilai tersebut mendapatkan dukungan |

| No | \Judul | *Comparing* | *Contrasting* | *Criticize* | *Synthesize* | *Summarize* |
|---|---|---|---|---|---|---|
| | Berbasis ISO 22301 dan ISO 27001 (Studi Kasus PT JPK)[9] | melakukan pengukuran terhadap kondisi dan kesiapan sistem informasi di PT JPK. | mempunyai SOP yang baik hingga dapat mendapatkan sertifikasi ISO 22301. Sedangkan penelitian yang akan dilakukan bertujuan untuk mengidentifikasi risiko dan meninjau keamanan informasi organisasi pendidikan mengacu pada metode *Business Continuity Plan* dan klausul ISO 22301 serta berdasarkan kerangka BCP Griffith University. | lebih valid. Selain Itu, penelitian sebelumnya ini perlu merumuskan ulang ketika akan menerapkan standar BCMS ISO 22301 karena dianggap terlalu luas dan kurang mendukung pada analisis suatu perusahaan tertentu. | valid. | Top Management untuk pengimplementasian BCMS pada PT JPK dengan memperbaiki alur dan prosedur selama implementasi BCMS pada perusahaan. |

Berdasarkan pada tabel 2.1 dapat disimpulkan bahwa perbedaan penelitian yang sudah dilakukan dengan penelitian yang akan dilakukan saat ini terdapat beberapa perbedaan yaitu objek penelitian dan standar ISO yang digunakan. Objek yang digunakan di penelitian sebelumnya yaitu keamanan layanan sistem informasi digunakan oleh sebuah instansi pemerintah dan perusahaan. Sedangkan pada penelitian yang akan dilakukan yaitu mengukur tingkat keamanan layanan sistem informasi yang digunakan oleh perguruan tinggi. Perbedaan lainnya yaitu standar ISO yang diterapakan untuk mengukur manajemen risiko layanan sistem informasi yaitu ada yang menggunakan standarisasi ISO 22301 karena standar ini menyediakan kerangka kerja praktik terbaik untuk mendukung organisasi mengelola dampak gangguan terhadap operasi normalnya secara efektif dengan melakukan siklus *Plan, Do, Check,* dan *Act* (PDCA) .

Penelitian ini akan menggunakan metode *Failure Mode and Effect Analysis* (FMEA), karena berdasarkan perbandingan dengan metode-metode lainnya pada tabel 2.1 metode FMEA dianggap lebih mudah diimplementasi untuk studi kasus pengembangan sistem informasi karena metode ini memudahkan untuk menganalisis potensi kegagalam risiko dan dampak yang ditimbulkan dijelaskan menggunakan skala numerik yang disebut dengan *Risk Priority Number (RPN)*[20]. Selain itu metode FMEA juga memiliki kelebihan lain diantaranya metode ini lebih berorientasi kepada pengguna sehingga lebih sesuai dengan kebutuhan organisasi.

## 2.2 Landasan Teori

Landasan teori yang digunakan pada penelitian ini sebagai berikut :

### 2.2.1 Layanan

Layanan menjadi salah satu hal penting dari berjalannya proses bisnis perusahaan atau organisasi karena layanan adalah tindakan memberikan *act of service* terhadap pihak yang membutuhkan dengan baik bertujuan untuk membangun citra perusahaan dan memperoleh kepuasan dari pihak yang membutuhkan pelayanan[16]. Layanan yang baik diberikan oleh penyedia layanan akan berpengaruh positif terhadap

kepuasan konsumen. Selama empat dekade layanan memiliki beragam definisi yaitu menurut Gronroos tahun 1990 layanan didefinisikan sebagai serangkaian aktivitas yang memiliki wujud tetapi tidak ada suatu keharusan adanya interaksi antara dua pihak yang terlibat sebagai pemecah masalah konsumen.

Definisi layanan menurut Parasuraman et al. tahun 1985 terbagi menjadi faktor kualitas layanan dan dimenasi kualitas layanan. Kualitas layanan memiliki fungsi yang berbeda antara sudut pandang dengan harapan apabila dikaitkan dengan kualitas. Pada tahun 1992 O'Connor, Powers, dan Bowers melakukan adaptasi konsep dari sebuah kualitas layanan untuk mengukur kualitas layanan di rumah sakti. Selanjutnya konsep yang diadaptasi tersebut dilanjutkan oleh peneliti yang lainnya. Tahun 2018 oleh Javed dan Ilyas memberikan teori baru dalam kualitas layanan kesehatan yaitu aksesibilitas dan keterjangkauan menjadi hal yang penting untuk diidentifikasi lebih lanjut dalam penerapan kualitas layanan kesehatan[21]. Layanan dapat dikelompokkan menjadi dua yaitu[22]:

#### 2.2.1.1 Layanan Kontak Tinggi

Pengelompokan layanan ini dikatakan sangat tinggi karena hubungan antara penyedia layanan dengan pengguna layanan tinggi karena pengguna layanan ingin terlibat dalam proses layanan yang diberikan tersebut.

#### 2.2.1.2 Layanan Kontak Rendah

Pengelompokan layanan ini tidak terlalu tinggi karena hubungan antara penyedia layanan dengan pengguna layanan tidak intensif hanya terjadi di depan meja saja.

### 2.2.2 Risiko

Risiko memiliki definisi yaitu sebuah bentuk ancaman yang tidak dapat diprediksi akibat dari adanya sebuah proses yang dilakukan dalam perusahaan atau organisasi dan tujuan yang belum dipahami secara

menyeluruh sehingga dapat menimbulkan kerugian[23]. Timbulnya risiko akan mempengaruhi proses bisnis dari perusahaan atau organisasi jika tidak segera diberikan solusi terbaiknya. Terdapat beberapa definisi dari risiko salah satunya yaitu dari Vaughan (1978) yaitu [23]:

#### 2.2.2.1 *Risk is the Chance of Loss*

Berarti risiko adalah peluang kerugian artinya menunjukkan kondisi yang memiliki peluang terhadap timbulnya kerugian.

#### 2.2.2.2 *Risk is the Possibility of Loss*

Berarti risiko adalah memiliki kemungkinan kerugian artinya terdapat kondisi yang masih memiliki kemungkinan terjadi antara titik nol dan satu.

#### 2.2.2.3 *Risk is Uncertainty*

Berarti risiko adalah ketidakpastian artinya terdapat kondisi yang tidak pasti pada hal yang menimbulkan risiko.

Berdasarkan definisi risiko diatas dapat ditarik kesimpulan bahwa risiko adalah suatu kejadian yang tidak dapat diprediksi adanya kemungkinan terjadi sesuatu hal yang tidak diharapkan oleh perusahaan atau organisasi.

### 2.2.3 Manajemen Risiko

Manajemen risiko adalah proses meninjau dan mengidentifikasi potensi risiko yang dapat terjadi pada perusahaan atau organisasi. Potensi risiko yang dapat kapan saja terjadi dan mengganggu proses bisnis perusahaan atau organisasi seperti adanya bencana alam, kebakaran, kerusakan server, dan lain sebagainya. Manajemen risiko disusun tidak hanya untuk proses peninjauan potensi risiko saja tetapi juga proses perhItungan dan mengukur pengaruh terhadap objek yang akan dTIinjau. Manajemen risiko memiliki definisi secara rinci oleh Vaughan, 1978; Wirawan, 2012 [24] :

#### 2.2.3.1 *On Going Process*

Penilaian manajemen risiko dilakukan secara *continue* atau berkelanjutan yang dapat dipantau dalam jangka waktu yang pendek.

#### 2.2.3.2 *Effected by People*

Proses perumusan dan penilaian manajemen risiko ditentukan dan dilaksanakan oleh pihak tertentu sesuai bidangnya pada suatu perusahaan atau organisasi.

#### 2.2.3.3 *Applied in Strategy Setting*

Suatu perusahaan atau organisasi yang baru berdiri harus memiliki dokumen yang berisi perencanaan dokumen manajemen risiko dalam jangka pendek atau jangka panjang bertujuan untuk mempersiapkan strategi dan solusi dari risiko yang akan dihadapi untuk setiap unit di perusahaan atau organisasi.

#### 2.2.3.4 *Applied Across the Enterprise*

Dokumen manajemen risiko yang sudah disusun oleh top management harus diimplementasikan dan ditinjau secara berkelanjutan pada masing – masing unit dalam perusahaan atau organisasi untuk meminimalisir terjadinya risiko yang berdampak buruk pada kinerja perusahaan atau organisasi.

#### 2.2.3.5 *Designed to Identify Potencial Events*

Perumusan, peninjauan, dan penyusunan manajemen risiko bertujuan untuk memperkecil kemungkinan risiko yang bisa terjadi kapan saja yang dapat mengganggu proses bisnis dan mempelambat tercapainya tujuan perusahaan atau organisasi.

#### 2.2.3.6 *Provide Reasonable Assurance*

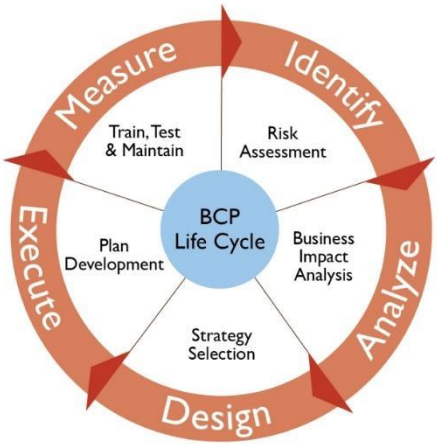
Penyusunan dan pengimpmentasin manajemen risiko yang tepat dan optimal pada setiap divisi perusahaan atau organisasi maka proses bisnis perusahaan atau organisasi akan berjalan secara efektif.

#### 2.2.3.7 *Geared to Achieve Objectives*

Penyusunan manajemen risiko diharapkan menjadi sebuah pedoman bagi perusahaan atau organisasi selama proses bisnis berjalan dan untuk mencapai tujuan dari perusahaan atau organisasi.

### *2.2.4 Business Continuity Plan*

*Business Continuity Plan* atau disingkat dengan BCP merupakan sebuah kerangka yang terdiri dari rancangan, strategi, dan rencana berkelanjutan untuk menilai risiko menggunakan sebuah sistem bertujuan untuk mencegah dampak yang terjadi akibat adanya bencana alam, kebakaran, kerusakan server, dan lain sebagainya sehingga proses bisnis perusahaan dapat dikendalikan dengan baik. *Bussiness Continuity Plan* dapat dilihat melalui gambar 2.1 dibawah ini :




**Gambar 2. 1 *Business Continuity Plan***[25]

#### 2.2.4.1 *Identify (Risk Assessment)*

Tahap pertama dalam *Business Continuity Plan Life Cycle* yaitu *risk assessmen*t dengan melakukan identifikasi terhadap proses bisnis perusahaan atau organisasi berkaTIan dengan risiko yang memiliki potensi mengganggu tercapainya tujuan perusahaan atau organisasi dirumuskan dari skala terkecil hingga terbesar. Risk assessment memiliki tiga tahapan proses untuk meninjau risiko yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko[4].

#### 2.2.4.2 *Analyze (Business Impact Analysis)*

Hasil identifikasi risiko pada tahap *identify* sebelumnya kemudian dianalisis lebih lanjut dampak yang dapat terjadi pada risiko masing – masing divisi dan asset milik perusahaan atau organisasi. Pada *Business Impact Analysis* memberikan solusi berupa strategi yang dapat dilakukan ketika risiko yang diidentifikasi sebelumnya terjadi sehingga perusahaan atau organisasi dapat meminimalisir dampak yang terjadi pada proses bisnis perusahaan atau organisasi. *Business Impact Analysis* memiliki tiga tujuan dalam penyusunannnya yaitu menentukan skala prioritas, merancang jangka waktu terjadinya waktu henti, dan mengidentifikasi kebutuhan sumber daya[3].

#### 2.2.4.3 *Design (Strategy Selection)*

Fase *strategy selection* merupakan proses menyusun dan menentukan strategi yang dapat diterapkan untuk mengurangi dampak risiko yang mungkin terjadi pada proses bisnis perusahaan atau organisasi. Fase ini terdapat beberapa tahapan proses yang perlu untuk diidentifikasi yaitu pertama, proses memilih penggunaan sumber daya seperti perangkat keras dan perangkat lunak yang dapat dilindungi ketika terjadi bencana,

kedua, menyusun strategi cadangan dan pemulihan secara cepat yang disusun untuk jangka pendek dan jangka panjang, ketiga, menyusun strategi memilih lokasi sesuai *Disaster Recovery* dengan beberapa pertimbangan seperti faktor keamanan, infrastruktur, mitigasi bencana, akses yang mudah, dan faktor pendukung lainnya[3].

#### 2.2.4.4 *Execute (Plan Development)*

Fase *Plan Development* ini melakukan pengembangan dokumen BCP yang terdiri dari setiap tahapan mitigasi bencana. Fase ini dilakukan dengan menyusun kerangka metodologi yang akan dilakukan dan menghasilkan output dokumen *Bussiness Continuity Plan* sesuai dengan kebutuhan perusahaan atau organisasi.

#### 2.2.4.5 *Measure (Training, Testing, and Maintain)*

Fase *Training, Testing,* dan *Maintain* ini dilakukan untuk mengukur keefektifan implementasi dokumen *Bussiness Continuity Plan* yang sudah disusun pada perusahaan atau organisasi sesuai dengan kebutuhannya. Pengimplementasian *Bussiness Continuity Plan* harus berdasarkan skala priorTIas disesuaikan dengan SOP perusahaan atau organisasi kemudian diuji keberlangsungan implementasinya berjalan sesuai kerangka yang disusun sebelumnya. Setelah melakukan training dan testing dokumen *Bussiness Continuity Plan* pada proses bisnis perusahaan atau organisasi kemudian tahap selanjutnya dilakukan evaluasi keberlanjutan terhadap perubahan yang dianggap kurang efektif selama pengimplementasiannya dan disusun kembali menyesuaikan kebutuhan perusahaan atau organisasi[4].

### 2.2.5 Definisi *Bussiness Continuity Plan* menurut Griffith University

Griffith University merupakan universitas riset publik yang menduduki peringkat 2 terbaik di dunia dan peraih peringkat 33 terbaik dalam QS World Uiversity Ranking tahun 2021[26]. Griffith University berdiri pada tahun 1971 dan dibuka pada tahun 1975 yang terletak di Queesland, Australia. Griffith University mengeluarkan sebuah standar berupa kerangka kerja yang memiliki fokus untuk organisasi pendidikan dalam implementasinya kerangka ini disusun berdasarkan standar internasional yaitu ISO 22301 yang membahas mengenai keamanan manajemen sistem. Kerangka kerja Griffith University ini diangkat sebagai referensi dalam penelitian ini karena fokus utama penelitiannya sama yaitu organisasi pendidikan.

*Business Continuity Plan* adalah fungsi dalam program *Bussiness Continuity*. BCP adalah proses lanjutan untuk mengidentifikasi bahaya dan kerentanan risiko pada universitas, kemungkinan gangguan, konsekuensi potensial pada tujuan yang sensitif terhadap waktu dan keberhasilan strategis, efektivitas kontrol yang ada dan strategi untuk meningkatkan kinerja dan efisiensi. Hal ini mempertimbangkan risiko dari waktu ke waktu ketika staf, aset, atau proses yang tidak tersedia[27]. Penyusunan BCP harus memperhatikan beberapa konsep utamanya yang penting untuk dipahami agar berjalan dengan baik dan hasil yang efektif. Konsep utama dari BCP yaitu[27] :

#### 2.2.5.1 *Understand the Business*

Mengembangkan BCP harus memiliki pemahaman bisnis yang baik karena melibatkan proses identifikasi terhadap misi bisnis dan target sesuai tujuan bisnis, identifikasi input dan output dari proses kritis dan ketergantungan fungsional, memprioritaskan proses dan kebutuhan sumber daya, serta menentukan pasokan eksternal dan pengaturan kontrak terhadap perusahaan.

#### 2.2.5.2 *Assess the Risks*

Penilaian risiko adalah kegiatan utama dalam proses penyusunan dokumen BCP. Langkah awal yang penting untuk dipahami kemungkinan yang bisa terjadi dan konsekuensi masalah terkait gangguan bisnis, menentukan selera risiko, dan ruang lingkup kebutuhan BCP yaitu dengan melakukan proses identifikasi, analisis, dan evaluasi terhadap risiko.

#### 2.2.5.3 *Prepare a Business Continuity Plan*

Keluaran utama dari proses keberlangsungan bisnis adalah dokumen BCP. BCP merupakan alat komunikasi dan pendukung keputusan yang telah ditentukan, melalui proses uji, dan sudah disetujui manajemen. Rencana tersebut dijalankan untuk menampilkan respons terhadap gangguan bisnis.

#### 2.2.5.4 *Test the Plan*

Ketika terjadi gangguan pada proses bisnis, staf terkait harus memahami jobdesknya. Staf dengan tanggung jawab harus secara teratur mengoptimalkan peran mereka untuk menguji BCP secara praktis, memvalidasi, mengkonfirmasi kompetensi, dan menguji asumsi seputar akses ke sumber daya. Proses BCP ini diarahkan untuk memberikan kenyamanan kepada dewan universitas, serta pemangku kepentingan universitas, bahwa jika yang terburuk terjadi, universitas memiliki kapasitas untuk pulih dengan cepat, aman, dan dengan biaya seefektif mungkin.

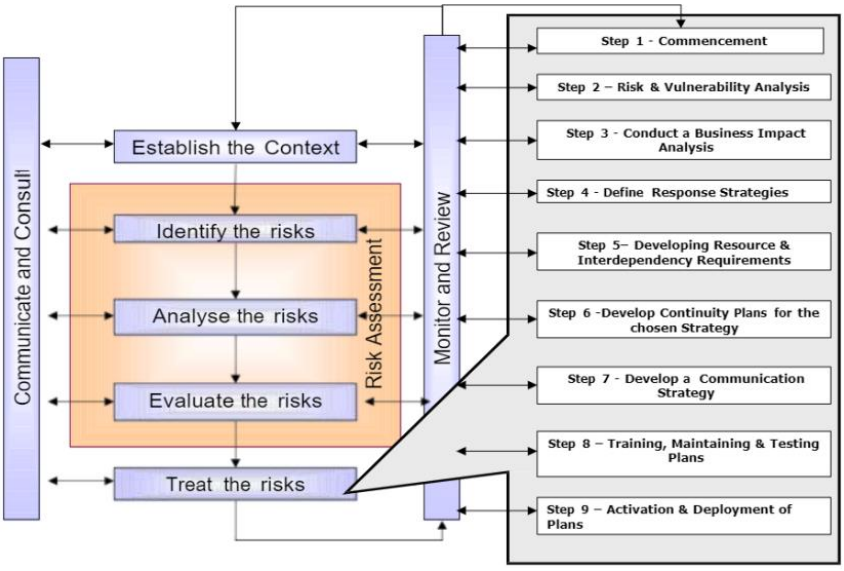
BCP memiliki tujuan dalam pengimplemetasiannya, berikut adalah tujuan dari penyusunan BCP menurut Griffith University[27] :

1. Mendokumentasikan proses bisnis yang penting untuk dipertahankan
2. Mendokumentasikan sumber daya yang diperlukan untuk mendukung proses bisnis yang dinilai kritis
3. Mendokumentasikan waktu tunggu pada proses bisnis sebelum risiko bahaya atau kerugian terjadi dapat mengganggu tujuan bisnis

4. Mendokumentasikan waktu pemulihan untuk memulihkan fungsi bisnis
5. Memahami garis besar untuk mengidentifikasi akomodasi alternatif
6. Mendokumentasikan detail penyimpanan dan dokumen penting untuk mendukung dimulainya kembali bisnis
7. Menetapkan rantai kesamaan, tanggung jawab, dan personel cadangan
8. Mendomentasikan prosedur informasi dan eskalasi dokumen

### 2.2.6 Kerangka Kerja *Business Continuity Plan* menurut Griffith University

Pengimplentasian kerangka BCP menurut Griffith University yang berbasis risiko dengan fokus utama dunia pendidikan yaitu akan meningkatkan pemahaman tentang risiko terkait gangguan, perencanaan berkelanjutan dan manajemen respons serta meningkatkan kewaspadaan dan kompetensi staf untuk mengatasi gangguan bisnis hingga pemulihan fungsionalitas secara penuh atau mode operasi baru diterapkan. Berikut ini gambar 2.2 dari kerangka kerja BCP menurut Griffith University :




**Gambar 2. 2 Kerangka Kerja BCP menurut Griffith University**[26]

Kerangka kerja BCP menurut Griffith University memiliki 9 tahapan proses penyusunan BCP yaitu :

**2.2.6.1 *Commencement* (Awal Mula)**

Tahapan proses pertama yaitu dengan mengidentifikasi manajemen risiko yang diimplementasikan selama proses bisnis berjalan.

**2.2.6.2 *Risk and Vulnerability Analysis* (Analisis risiko)**

Tahapan proses kedua yaitu analisis risiko dengan memberikan pemahaman tentang fungsi utama bisnis di universitas, proses kritis, aset (segala sesuatu yang bernilai material atau berguna), besaran kontribusi setiap asset, paparan dan kerentanan atau proses dan aset terhadap gangguan. Menindaklanjuti proses analisis risiko dapat dilakukan oleh top management yaitu :

1. Melakukan identifikasi ancaman bahaya terhadap kelangsungan fungsi bisnis inti dan proses, sistem, informasi, karyawan, aset, mitra outsourcing, dan sumber daya lain yang mendukung
2. Melakukan analisis kemungkinan dan konsekuensi gangguan, serta tingkat konsekuensi dalam kerangka manajemen risiko
3. Mengevaluasi risiko terkait gangguan yang memerlukan penanganan lebih lanjut
4. Melakukan identifikasi manajemen risiko yang berkaitan dengan tujuan BC dan risiko Universitas.

Jika analisis risiko awal tidak memberikan informasi yang cukup konkrit atau apabila setelah melakukan identifikasi dan analisis awal risiko ternyata masalah yang terjadi tidak dapat ditoleransi, maka akan dilakukan studi yang lebih rinci yang disebut *Business Consequence Analysis* (BCA).

#### 2.2.6.3 *Conduct a Business Impact Analysis* (Analisis dampak bisnis)

*Business Impact Analysis* (BIA) atau analisis dari dampak suatu bisnis adalah proses untuk menentukan kerusakan pengoperasian yang mendukung proses bisnis dari waktu ke waktu ketika aset tidak tersedia untuk mendukung proses bisnis dan efeknya pada fungsi bisnis. Pentingnya memahami hubungan antara fungsi utama universitas, operasi, proses bisnis, dan tingkat harapan pelanggan untuk menganalisis konsekuensi masalah yang timbul dan menentukan proses mana yang penting untuk kelangsungan bisnis.

BIA diidentifikasi dengan tujuan untuk membangun dan memahami konsekuensi yang mengganggu atau masalah potensial yang memerlukan penanganan khusus dan munculnya kemungkinan yang membutuhkan pengecekan oleh manajemen secara rutin atau memerlukan kemampuan manajemen tambahan. BIA mengidentifikasi konsekuensi operasional (kualitatif) dan keuangan (kuantitatif) dari gangguan dan menyusun dasar untuk pengembangan keberlanjutan yang layak dan strategi pemulihan yang akan diberlakukan bila diperlukan untuk memulihkan operasi dalam kerangka waktu yang diperlukan. Keluaran dari penilaian risiko awal dan BIA harus dikonsolidasi terlebih dahulu sehingga kemungkinan terjadi gangguan proses bisnis terkait konsekuensi keseluruhan dan strategi mitigasi risiko sudah dicatat dalam daftar risiko universitas.

#### 2.2.6.4 *Define Responses Strategies* (Mendefinisikan Strategi Respons)

Tahapan proses keempat yaitu penentuan dan pemilihan strategi didasarkan pada keluaran dari BIA. Manajemen senior akan menentukan strategi kelangsungan bisnis yang tepat untuk melindungi fungsi utama dari universitas dan proses bisnis, menstabilkan, mempertahankan, dan memulihkan fungsi, layanan, proses kritis dan dependensinya serta sumber daya pendukungnya.

Strategi respons akan diinformasikan melalui jangka waktu yang disetujui untuk pemulihan proses kritis. Ketika memilih strategi respons, hal-hal berikut harus dipertimbangkan :

1. Jenis bahaya yang memiliki kemungkinan terjadi pada organisasi
2. Prosedur alternatif untuk menjalankan proses sampai selesai atau ke tingkat minimal yang dapat diterima sampai pemulihan dapat dilakukan
3. Kemampuan pemrosesan secara manual dan biaya terkait
4. Penggunaan asuransi
5. Pengaturan oleh pihak ketiga, kemitraan bisnis, saling membantu lingkup sektoral
6. Siklus bisnis dan periode puncak
7. Kemampuan sumber daya internal, rantai pasokan, dan manajemen vendor
8. Aksesibilitas data
9. Pilihan untuk tidak melakukan apapun atau memutuskan seberapa besar kerugian yang bisa ditanggung bisnis

#### 2.2.6.5 *Developing Resources and Interdependency Requirements*

Tahapan proses kelima yaitu BCP akan menunjukkan kebutuhan sumber daya untuk mendukung proses kritis dan memastikan ketetapan penggunaan sumber daya. Jenis sumber daya yang perlu dipertimbangkan :

1. Sumber daya manusia
2. Informasi dan data
3. Bangunan, lingkungan kerja dan utilitas terkait
4. Fasilitas, peralatan, dan bahan habis pakai
5. Sistem *Information and Communication Technology* (ICT)
6. Transportasi dan logistik
7. Keuangan
8. Mitra

#### *2.2.6.6 Develop Business Continuity Plans*

Tahapan proses keenam yaitu BCP akan menetapkan :

1. Proses kritis untuk dilanjutkan
2. Menentukan peran dan tanggung jawab serta detail kontak untuk orang dan tim yang memiliki wewenang selama dan setelah peristiwa yang mengganggu
3. Proses untuk meminta dan meningkatkan respons
4. Sumber daya yang diperlukan untuk mendukung respons
5. Sebuah strategi komunikasi
6. Detail hubungan interdependensi
7. Detail pemasok penting dan pengaturan alternatif
8. Daftar catatan vital, penyimpanan, dan detail akses yang relevan
9. Strategi untuk mengelola hilangnya gangguan pada orang, properti, *platform*, penyedia

#### *2.2.6.7 Develop a Communication Strategy*

Tahapan proses ketujuh yaitu menetapkan bagian penting dalam proses pengelolaan setiap adanya peristiwa yang mengganggu adalah menyusun strategi komunikasi dan konsultasi yang jelas dan efektif. Strategi harus diterapkan dengan cara yang mencerminkan besarnya konsekuensi bisnis. Manajemen senior harus menetapkan, menerapkan, dan memelihara prosedur yang bertujuan untuk :

1. Mendeteksi peristiwa yang mengganggu
2. Memantau acara secara teratur
3. Mengelola komunikasi internal dari pihak yang berkepentingan
4. Menjamin ketersediaan sarana komunikasi selama acara
5. Memfasilitasi komunikasi terstruktur dengan responden darurat
6. Mencatat informasi penting tentang acara, tindakan yang diambil, dan keputusan yang dibuat

#### *2.2.6.8 Training, Testing, and Maintaining Plans*

Tahapan proses kedelapan terbagi menjadi tiga metode yaitu pelatihan, pemeliharaan, dan pengujian. Berikut ini penjelasan setiap metodenya :

1. *Training*

   *Training* atau pelatiha dilakukan bertujuan untuk memberikan kepastian setelah melakukan tahap pengembangan dan pendokumentasian dalam BCP memungkinkan unit bisnis untuk mempertahankan proses bisnis yang penting setelah terjadi peristiwa yang mengganggu. Pendidikan dan pelatihan merupakan komponen penting dari proses BCM dan memerlukan komitmen dari personel Universitas yang terlibat dalam perencanaan, respon dan operasi pemulihan. Berikut ini cara untuk yang dapat dilakukan untuk pelatihan yaitu meliputi:

   1. Mengadakan rapat perencanaan bersama dewan dan tim atau membahas perencanaan harian
   2. Orientasi karyawan
   3. Melakukan pelatihan manajemen risiko
   4. Pelatihan khusus untuk BC
   5. Melakukan uji coba terhadap evakuasi darurat

   Proses pelatihan ini disusun dengan pembuatan, penerapan, pengujian, dan pemeliharaan BCP yang akan diselenggarakan melalui unit risiko dan kelangsungan bisnis.

2. *Testing*

   *Testing* atau pengujian bertujuan untuk mengukur indikator keberhasilan yang kritis, dievaluasi secara teratur, hasil didokumentasikan dan perbaikan diterapkan. Proses ini akan memberikan pengukuran yang pasti, relevan, terkini, dan efektif. Tindakan respons dan pemulihan harus dipraktikkan di bawah kondisi simulasi untuk menjalankan strategi dan

rencana dan menantang asumsi, melatih orang-orang dengan peran dan tanggung jawab BCM. Pelaksanaan BCP dapat dilakukan dalam berbagai bentuk termasuk :

1. *Call Tree Testing*

   Menguji nomor kontak yang terdaftar dan pengetahuan mengenai peran setiap individu.

2. *Desk Check Test*

   Meninjau dokumen BCP yang sudah dirumuskan dan disusun.

3. *Walk Through Test*

   Menyusun perencanaan terhadap peserta untuk melakukan *Walk Through Test* melalui prosedur rencana dalam menanggapi skenario untuk memvalidasi pengetahuan peran mereka dan mengkonfirmasi kelayakan rencana terhadap tujuan bisnis dan lingkungan risiko.

3. *Maintaining*

   *Maintaining* atau pemeliharaan bertujuan untuk menyusun jadwal untuk pemeliharaan BCP yang berkelanjutan harus ditetapkan dan dilaporkan sebagai bagian dari proses jaminan kualitas proses bisnis. Dukungan jadwal yang tersusun akan diberikan melalui unit risiko dan kelangsungan bisnis di bawah otoritas layanan perusahaan.

#### *2.2.6.9 Activation and Deployment of Plans*

Tahapan proses kesembilan yaitu ketika peristiwa yang mengganggu terjadi dan mengakibatkan aktivasi prosedur BC, maka manajemen senior dan personal terkait yang terlibat harus melakukan *briefing* pasca-acara dan mencatat pengamatan serta merekomendasikan untuk memberikan informasi perencanaan tindakan selanjutnya.

### 2.2.7 Metode Pembanding Keamanan Sistem Informasi

Keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. (G. J. Simons, 2018). Keamanan sistem informasi adalah informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan. (Whitman & Mattord, 2011). Dimensi atau indikator keamanan sistem informasi adalah memiliki dua sisi yaitu relevan dengan pengetahuan lingkungannya dan patuh terhadap dasar yang ada (Herver, 2004). Di dalam upaya penanganan maupun pengendalian terhadap Keamanan Sistem Informasi, kiranya harus mempertimbangkan tiga aspek penting dalam keamanan informasi yang akrab dengan kependekan CIA (*Confidentiality*, *Integrity*, *Availability*)[28].

a. Kerahasiaan atau *Confidentiality* merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang.
b. Integritas atau *Integrity* merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi.
c. Ketersediaan atau *Availability* merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan, kapanpun dan dimanapun.

Analisis keamanan sistem informasi dapat menggunakan beberapa *framework* atau metode yang berbeda sesuai dengan kebutuhan penelitian. Berikut tabel 2.2 yang menjelaskan setiap metode yang dapat digunakan untuk analisis keamanan sistem informasi :

**Tabel 2. 2 Metode Pembanding Keamanan Sistem Informasi**

| NO | METODE KEAMANAN SISTEM INFORMASI | PENJELASAN |
|---|---|---|
| 1 | *National Institute of Standards and Technology* (NIST) | Metode yang paling lama berjalan dan didirikan pada tahun 1990. Menawarkan panduan terperinci tentang segala hal mulai dari penilaian risiko dan pemantauan berkelanjutan hingga respons insiden dan pelatihan kesadaran. NIST tidak hanya menawarkan rencana komprehensif untuk perlindungan data dan mitigasi risiko, tetapi juga metodologi untuk membatasi dampak kejadian buruk. Asumsi kerangka kerja NIST melengkapi kebutuhan industri, kerangka ini sangat berfokus pada keamanan informasi dan mungkin tidak cukup komprehensif untuk meningkatkan efektivitas program keamanan siber secara keseluruhan di seluruh manusia, proses, dan teknologi[29]. |
| 2 | *Control Objectives for Information Related Technology* (COBIT) | COBIT adalah kerangka kerja solid yang memandu proses dengan cara yang memungkinkan eksekutif bisnis untuk meluncurkan kebijakan dan prosedur utama di seluruh strategi, inovasi, manajemen risiko, manajemen aset, dan lainnya. Tidak seperti NIST dan ISO yang sangat berpusat pada IT, bagaimanapun, COBIT mendefinisikan komponen dan faktor desain untuk membangun dan mempertahankan sistem tata kelola keseluruhan yang paling sesuai. Ini juga bekerja dengan baik dengan kerangka kerja manajemen risiko TI yang menjadikannya pilihan yang bagus sebagai kerangka kerja payung untuk menyatukan proses di seluruh organisasi. Model Inti COBIT mencakup 40 tujuan tata kelola dan manajemen untuk menetapkan program tata kelola dan pada akhirnya membantu menyelaraskan tujuan bisnis dengan tujuan TI dengan membangun hubungan antara keduanya dan menciptakan proses yang dapat membantu menjembatani kesenjangan antara TI - atau silo TI - dan departemen luar. Namun, beberapa kritikus mengatakan bahwa kerangka kerja tersebut terlalu tinggi[30]. |
| 3 | TOGAF | TOGAF adalah kerangka kerja umum dan dimaksudkan untuk digunakan dalam berbagai macam lingkungan, ia menyediakan konten kerangka kerja yang fleksibel dan extensible yang mendasari seperangkat pengiriman arsitektur generik. Fokus utama TOGAF sendiri adalah pada siklus |

| NO | METODE KEAMANAN SISTEM INFORMASI | PENJELASAN |
|---|---|---|
| | | implementasi dan proses bisnis yang dijalankan dengan kunci TOGAF adalah dengan metode Architecture Development Method (ADM) untuk mengembangkan suatu arsitektur enterprise yang membahas kebutuhan bisnis. TOGAF bersifat open source, sehingga bersifat netral terhadap teknologi dari vendor tertentu. Elemen kunci dari TOGAF adalah Architecture Development Method (ADM) yang memberikan gambaran spesifik untuk proses pengembangan arsitektur enterprise[31]. |
| 4 | ISO | ISO dirancang untuk menyediakan kerangka kerja untuk mencapai tingkat sertifikasi kepatuhan keamanan data yang memenuhi standar penilaian eksternal. Tapi di mana NIST dirancang oleh pemerintah federal AS, ISO dibangun di atas dasar internasional, dikembangkan oleh Organisasi Internasional untuk Standardisasi (ISO) dan Komisi Elektroteknik Internasional (IEC). standar keamanan siber ISO dirancang untuk membantu organisasi memastikan tingkat privasi dan kerahasiaan data yang tidak hanya membantu mereka menghindari tuntutan, tetapi juga untuk memaksimalkan efisiensi operasional melalui pengurangan kerentanan terhadap serangan yang mengganggu. Organisasi Internasional untuk Standardisasi (ISO) bertujuan untuk menawarkan praktik terbaik dan saran perbaikan untuk standar SMKI tersebut. Kerangka kerja ini sangat berfokus pada TI dan memungkinkan tim TI untuk secara efektif mengidentifikasi dan mengelola penyimpangan dalam infrastruktur keamanan[30]. |

Berdasarkan tabel diatas yang menjelaskan metode pembanding didapatkan fokus dari setiap metode keamanan sistem informasi seperti metode NIST berfokus pada keamanan informasi dan mungkin tidak cukup komprehensif untuk meningkatkan efektivitas program keamanan siber secara keseluruhan. Metode COBIT mendefinisikan komponen dan faktor desain untuk membangun dan mempertahankan sistem tata kelola keseluruhan yang paling sesuai. Metode TOGAF berfokus pada

*Architecture Development Method* (ADM) yang memberikan gambaran spesifik untuk proses pengembangan arsitektur enterprise. Metode ISO Kerangka kerja ini sangat berfokus pada TI untuk memastikan tingkat privasi dan kerahasiaan data yang tidak hanya membantu mereka menghindari tuntutan, tetapi juga untuk memaksimalkan efisiensi operasional melalui pengurangan kerentanan terhadap serangan yang mengganggu. Metode yang sesuai digunakan untuk standarisasi penelitian ini yaitu metode ISO 22301 untuk menganalisis keamanan sistem informasi terhadap layanan TI organisasi yang didukung oleh PDCA *life cycle* dan 10 klausul sehingga penelitian ini akan lebih terstruktur pada setiap tahapan analisis risikonya.

### 2.2.8 ISO 22301

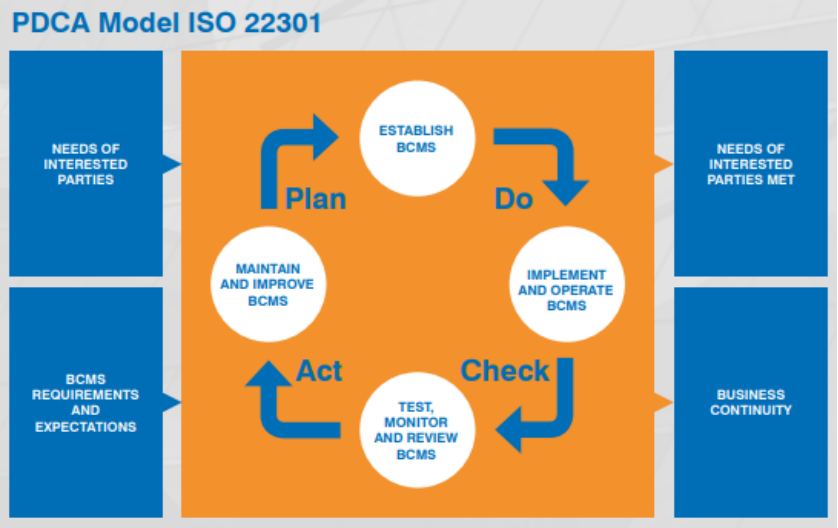
ISO 22301 adalah versi terbaru dari standar internasional untuk *Business Continuity Management System*. Standar ini menyediakan kerangka kerja praktik terbaik untuk mendukung organisasi mengelola dampak gangguan terhadap operasi normalnya secara efektif. Tujuan dari standar ini tidak selalu untuk mencapai mitigasi total dampak dari gangguan tetapi untuk mendukung organisasi dalam jumlah dan jenis dampak yang bersedia diterimanya setelah gangguan. Setelah itu organisasi mengembangkan sistem kelangsungan bisnis yang berukuran tepat untuk kebutuhan organisasi. Banyak organisasi akan mengalami gangguan bisnis yang disebabkan oleh masalah yang mengganggu. Organisasi harus dapat berpikir secara dinamis tentang lanskap ancaman yang berubah ini dan menyusun rencana yang tepat untuk mengurangi dampaknya[32].

Awal mula disusunnya standar ISO 22301 kembali ke komite teknis ISO ISO/TC 23, yang berfokus pada penanganan masalah yang terkait dengan keamanan masyarakat. Standar sekarang dikelola oleh keamanan dan ketahanan ISO/TC 292. Iterasi pertama dari standar ISO

22301 diterbitkan pada tahun 2012. Edisi kedua diterbitkan pada Oktober 2019 dan menjadi fokus dari panduan implementasi ini[32].

#### 2.2.7.1 PDCA *Cycle*

ISO 22301 didasarkan pada siklus *Plan-Do-Chechk-Action* (PDCA) yang juga dikenal sebagai *Deming Wheel* atau *Shewhart cycle*. Siklus PDCA dapat diterapkan tidak hanya pada sistem manajemen secara keseluruhan tetapi pada setiap elemen individu untuk memberikan fokus berkelanjutan pada peningkatan berkelanjutan. Berikut gambar 2.4 PDCA *Cycle* secara singkat[32]:




**Gambar 2.4 PDCA *Life Cycle[32]***

1. *Plan*

   Memahami konteks eksternal dan kebutuhan pihak yang berkepentingan. Identifikasi risiko dan peluang. Menetapkan tujuan dan sumber daya yang dibutuhkan.

2. *Do*

   Melaksanakan apa yang telah direncanakan. Dari BCMS baru hingga perubahan proses kecil.

3. *Check*

Memantau dan mengukur efektivitas kelangsungan usaha. Uji BCP dan pantau hasilnya.

4. *Action*

   Mengambil tindakan jika perlu berdasarkan pemantauan, pengukuran, dan pendorong tindakan lainnya.

#### 2.2.7.1 Klausa ISO 22301

ISO 22301 terdiri dari bagian yang dikenal sebagai klausa. Seperti kebanyakan standar sistem manajemen ISO lainnya, persyaratan ISO 22301 yang harus dipenuhi ditentukan dalam klausa 4 - 10, organisasi harus mematuhi semua persyaratan dalam klausa 4 – 10 mereka karena pada klausa 1 – 3 berisi informasi secara general mengenai ISO 22301 sehingga yang digunakan sebagai bahan uji analisis dan penelitian yaitu klausa 4 – 10 saja[27]. Berikut ini tabel 2.3 yang menjelaskan klausa dari ISO 22301 :

**Tabel 2. 3 Klausa ISO 22301**[32]

| Klausa | Penjelasan |
|---|---|
| Klausa 1 "*Scope*" | Ruang lingkup ISO 22301 menetapkan bahwa :<br>1. Tujuan dari standar yang digunakan<br>2. Merancang strukturasi organisasi<br>3. Bagian dari standar yang berisi persyaratan harus dipatuhi oleh organisasi agar organisasi disertifikasi "sesuai" dengan yang diharapkan.<br>ISO 22301 dirancang untuk dapat diterapkan pada semua jenis organisasi. Terlepas dari ukuran, kompleksTIas, sektor industri, tujuan atau tingkat kematangannya, setiap organisasi dapat menerapkan dan memelihara BCMS yang sesuai dengan ISO 22301. |
| Klausa 2 "*Normative References*" | Dalam standar ISO, bagian referensi normatif mencantumkan standar lain yang berisi informasi tambahan yang relevan untuk menentukan apakah organisasi mematuhi standar yang dimaksud atau tidak. ISO 22301 hanya memiliki satu dokumen adalah lister ISO 22300 mengenai keamanan dan ketahanan. |
| Klausa 3 " *Term and Definitions*" | Istilah lain yang dijelaskan pada bagian "Prinsip Utama dan Terminologi" di atas, istilah terpenting yang digunakan dalam ISO 22301 adalah : |

| Klausa | Penjelasan |
|---|---|
| | 1. *Business Continuity*<br>Kemampuan organisasi untuk melanjutkan pengiriman produk atau layanan pada tingkat yang telah ditentukan sebelumnya yang dapat dTIerima setelah adanya gangguan yang terjadi pada proses bisnis perusahaan atau organisasi.<br>2. *Business Continuity Management*<br>Proses manajemen holistik yang mengidentifikasi potensi ancaman terhadap organisasi dan dampak ancaman tersebut, jika disadari, dapat menyebabkan operasi bisnis, dan menyediakan kerangka kerja untuk membangun ketahanan organisasi dengan kemampuan respons yang efektif yang melindungi kepentingan pihak yang berkepentingan utama, reputasi , merek, dan aktivitas penciptaan nilai.<br>3. *Business Continuity Plan*<br>Prosedur terdokumentasi yang memandu organisasi untuk merespons, memulihkan, melanjutkan, dan memulihkan dirinya sendiri ke tingkat operasi yang telah ditentukan sebelumnya setelah terjadi gangguan pada proses bisnis perusahaan atau organisasi.<br>4. *Business Impact Analysis*<br>Proses menganalisis aktivitas dan dampak gangguan bisnis selama berjalannya proses bisnis perusahaan atau organisasi.<br>5. *Crisis Management Team*<br>Sekelompok fungsi individu yang bertanggung jawab untuk mengarahkan pengembangan dan pelaksanaan rencana respons dan kelangsungan operasional, dan gangguan operasional selama proses pemulihan, baik sebelum dan sesudah kejadian gangguan.<br>6. *Disruption*<br>Peristiwa yang diantisipasi atau tidak diantisipasi yang menyebabkan penyimpangan negatif yang tidak direncanakan dari penyampaian produk atau jasa diharapkan sesuai dengan tujuan organisasi. |
| Klausa 4<br>"*Context Of The Organization*" | Tujuan BCMS adalah untuk memungkinkan organisasi merespons insiden yang mengganggu secara efektif dan melanjutkan pengiriman produk dan layanan utama pada tingkat yang telah ditentukan sebelumnya, sehingga operasi normal dapat dijalankan kembali. |

| Klausa | Penjelasan |
|---|---|
| | A. Konteks Internal<br>Berikut ini adalah contoh area yang harus dipertimbangkan saat menilai masalah internal yang mungkin terkait dengan BCMS :<br>1. Kematangan<br>Apakah Anda seorang pemula yang gesit dengan kanvas kosong untuk dikerjakan, atau institusi berusia 30+ tahun dengan proses dan rencana darurat yang mapan?<br>2. Budaya Organisasi<br>Apakah organisasi Anda santai tentang bagaimana, kapan, dan dimana orang bekerja, atau sangat diatur?<br>3. Ketergantungan<br>Apa ketergantungan internal yang diperlukan untuk merespons secara efektif insiden yang mengganggu pada Layanan TI, daya, peralatan?<br>4. Pengelolaan<br>Apakah ada saluran dan proses komunikasi yang jelas dari pengambil keputusan utama organisasi hingga ke seluruh organisasi?<br>5. Ukuran Sumber Daya<br>Apakah Anda bekerja dengan sumber daya, personel, dan peralatan dalam jumlah terbatas?<br>6. Kematangan Sumber Daya<br>Apakah sumber daya yang tersedia seperti karyawan atau kontraktor sudah berpengetahuan, terlatih, dapat diandalkan, dan konsisten, atau apakah personel tidak berpengalaman dan terus berubah?<br>7. Konsistensi<br>Apakah memiliki proses yang seragam di seluruh organisasi, atau banyak praktik operasi yang berbeda dengan sedikit konsistensi?<br>8. Peralatan<br>Apakah Anda memerlukan peralatan khusus?<br>B. Konteks Eksternal<br>Berikut ini adalah contoh area yang dapat dipertimbangkan saat menilai masalah eksternal yang mungkin terkait dengan BCMS :<br>1. Tuan Rumah<br>Apakah Anda memerlukan persetujuan untuk |

| Klausa | Penjelasan |
|---|---|
| | meningkatkan keamanan fisik?<br>2. Pemasok<br>Apakah pemasok Anda dapat menyediakan pemasok tepat waktu?<br>3. Regulator/Badan Penegak<br>Apakah ada persyaratan peraturan atau undang-undang yang perlu Anda pertimbangkan saat mengembangkan BCMS Anda? Apakah Anda perlu memberi tahu mereka bahwa Anda telah melibatkan BCP Anda?<br>4. Ekonomi/Politik<br>Apakah fluktuasi mata uang berdampak pada organisasi Anda?<br>5. Ketergantungan<br>Ketergantungan eksternal apa yang Anda perlukan untuk merespons secara efektif insiden yang mengganggu (Layanan TI, Suplai, Listrik, Peralatan?)<br>6. Pertimbangan Lingkungan<br>Apakah ada masalah lingkungan yang mungkin berdampak pada BCMS Anda?<br>7. Pelanggan<br>Apa dampak pemanggilan BCMS Anda terhadap pelanggan Anda? Apakah Anda perlu memberi tahu mereka bahwa Anda telah memanggil BCP Anda?<br>8. Pemegang saham<br>Apakah mereka sangat memperhatikan kemampuan organisasi Anda untuk menanggapi insiden yang mengganggu?<br>C. Pihak yang Tertarik<br>Pihak yang berkepentingan adalah siapa saja yang dapat dipengaruhi oleh permintaan BCP Anda. Pihak-pihak yang berkepentingan akan menjadi jelas melalui proses melakukan analisis mendalam terhadap isu-isu internal dan eksternal. Kemungkinan termasuk pemegang saham, tuan tanah, regulator, pelanggan, karyawan, pemasok, dan dapat meluas ke masyarakat umum dan lingkungan, tergantung pada sifat bisnis Anda. Anda tidak harus mencoba untuk memahami atau memuaskan setiap kebutuhan mereka, tetapi Anda harus menentukan mana dari setiap kebutuhan mereka, tetapi Anda harus |

| Klausa | Penjelasan |
|---|---|
| | menentukan kebutuhan dan harapan mereka yang relevan dengan BCMS Anda.<br>D. Hukum dan Peraturan<br>Identifikasi dan ikuti perkembangan terbaru dengan persyaratan hukum dan peraturan yang terkait dengan kelangsungan produk dan layanan, aktivitas, dan sumber daya Anda saat menerapkan dan memelihara BCMS Anda.<br>- Dokumen<br>Dokumentasikan persyaratan kepatuhan hukum, peraturan, dan lainnya serta pendekatan Anda untuk memenuhi persyaratan tersebut. |
| Klausa 5<br>"*Leadership*" | Kepemimpinan dalam konteks ini berarti keterlibatan aktif dalam menetapkan arah BCMS, mempromosikan pelaksanaannya, menyoroti pentingnya dan memastikan sumber daya yang tepat tersedia.<br>1. Memastikan bahwa kebijakan kelangsungan bisnis dan tujuan kelangsungan bisnis ditetapkan dan selaras dengan arah strategis organisasi<br>2. Memastikan integrasi persyaratan BCMS ke dalam praktik bisnis organisasi<br>3. Memastikan bahwa BCMS memiliki sumber daya yang memadai<br>4. Mengkomunikasikan pentingnya kelangsungan bisnis dan sesuai dengan persyaratan BCMS<br>5. Memastikan BCMS mencapai hasil yang diinginkan<br>6. Mengarahkan dan mendukung orang-orang untuk berkontribusi pada efektivitas BCMS<br>7. Mempromosikan perbaikan terus-menerus<br>8. Mendukung peran manajerial lainnya untuk menunjukkan kepemimpinan dan komitmen mereka.<br>ISO 22301 sangat mementingkan keterlibatan aktif oleh manajemen puncak di BCMS, berdasarkan asumsi bahwa keterlibatan manajemen puncak sangat penting dalam memastikan penerapan, pemeliharaan, dan peningkatan berkelanjutan yang efektif dari BCMS yang efektif oleh kelompok karyawan yang lebih luas. |
| Klausa 6<br>"*Planning*" | Ketika merencanakan BCMS-nya, sebuah organisasi perlu mempertimbangkan risiko dan peluang yang diidentifikasi saat menentukan konteks organisasi dan ruang lingkup |

| Klausa | Penjelasan |
|---|---|
| | BCMS. Organisasi perlu menentukan risiko dan peluang mana yang perlu ditangani :<br>1. Memberikan jaminan bahwa BCMS dapat mencapai hasil yang diinginkan<br>2. Mencegah atau mengurangi efek yang tidak diinginkan<br>3. Mencapai peningkatan berkelanjutan<br><br>A. Mengatasi Risiko dan Peluang<br>Organisasi harus menetapkan metodologi untuk menilai risiko dan peluang yang berdampak pada kemampuan BCMS untuk mencapai hasil yang diinginkan dan menentukan tindakan yang diperlukan untuk mengatasi risiko dan peluang. Sebuah organisasi harus :<br>1. Identifikasi tindakan untuk mengatasi risiko dan peluang<br>2. Melaksanakan tindakan mengidentifikasi<br>3. Evaluasi keefektifan tindakan ini<br>B. Tujuan Kontinuitas Bisnis (dan perencanaan untuk mencapainya)<br>Objek kelangsungan bisnis perlu ditetapkan pada fungsi dan tingkat yang relevan dalam suatu organisasi, tujuan dapat berada di tingkat organisasi atau departemen. Tujuan harus :<br>1. Konsisten dengan kebijakan kelangsungan bisnis<br>2. Terukur<br>3. Memperhitungkan persyaratan yang berlaku<br>4. Dikomunikasikan<br>5. Dipantau dan diperbarui sebagaimana mestinya<br>Tujuan harus dikomunikasikan kepada orang-orang yang relevan dalam organisasi, dipantau dan diperbarui sesuai kebutuhan.<br>C. Mencapai Tujuan<br>Sebuah organisasi harus menetapkan rencana untuk mencapai tujuannya, rencana tersebut harus mempertimbangkan :<br>1. Apa yang perlu dilakukan<br>2. Sumber daya yang dibutuhkan<br>3. Siapa yang bertanggung jawab<br>4. Tanggal penyelesaian |

| Klausa | Penjelasan |
|---|---|
| | 5. Cara mengevaluasi hasil<br>D. Ubah ke BCMS<br>Ada kemungkinan bahwa dari waktu ke waktu proses organisasi, kegiatan, produk, dan layanan akan berubah. Akibatnya Anda perlu melakukan perubahan pada BCMS Anda, perubahan harus dilakukan secara terencana dan harus mempertimbangkan :<br>1. Tujuan perubahan dan konsekuensi potensialnya<br>2. IntegrTIas BCMS<br>3. Ketersediaan sumber daya<br>4. Re-alokasi tanggung jawab dan wewenang. |
| Klausa 7<br>"*Support*" | Klausul 7 menyangkut dirinya dengan sumber daya. Ini berlaku untuk orang, infrastruktur dan lingkungan sebanyak sumber daya fisik, material, peralatan, dll. Ada juga fokus baru pada pengetahuan sebagai sumber daya yang signifikan dalam organisasi Anda. Saat merencanakan tujuan kesinambungan bisnis Anda, pertimbangan utama adalah kapasitas dan kapabilitas sumber daya Anda saat ini serta yang mungkin Anda perlukan dari pemasok atau mitra eksternal.<br>A. Kompetensi<br>Penerapan BCMS yang efektif sangat bergantung pada pengetahuan dan keterampilan karyawan, pemasok, dan kontraktor Anda. Untuk memastikan dasar pengetahuan dan keterampilan yang sesuai, Anda perlu :<br>1. Mentukan pengetahuan dan keterampilan yang dibutuhkan<br>2. Tentukan siapa yang perlu memiliki pengetahuan dan keterampilan<br>3. Verifikasi bahwa orang yang tepat memiliki pengetahuan dan keterampilan yang tepat.<br>Auditor Anda akan mengharapkan Anda memiliki dokumen yang merinci persyaratan pengetahuan dan keterampilan Anda. Jika yakin persyaratannya terpenuhi, ini perlu didukung dengan catatan seperti sertifikat pelatihan, catatan kehadiran kursus atau penilaian kompetensi internal.<br>B. Kesadaran<br>Selain memastikan kompetensi khusus personal kunci dalam kaitannya dengan kelangsungan bisnis, kelompok |

| Klausa | Penjelasan |
|---|---|
| | karyawan, pemasok, dan kontraktor yang lebih luas perlu mengetahui elemen dasar BCMS Anda. Hal ini penting untuk membangun budaya yang mendukung dalam organisasi. Semua staf, pemasok, dan kontraktor harus mengetahui hal-hal berikut :<br>1. Bahwa memiliki BCMS dan mengapa Anda memilikinya<br>2. Bahwa memiliki Kebijakan Kelanjutan Bisnis dan elemen tertentu mana yang relevan dengannya<br>3. Bagaimana mereka dapat berkontribusi pada organisasi dalam menanggapi situasi yang merugikan dan mempertahankan kesinambungan produk atau layanan pada tingkat yang telah ditentukan sebelumnya<br>4. Kebijakan, prosedur mana yang relevan dengannya dan apa konsekuensinya jika tidak mematuhinya<br>C. Komunikasi<br>Agar proses di BCMS Anda bekerja secara efektif, Anda perlu memastikan bahwa Anda memiliki aktivitas komunikasi yang direncanakan dan dikelola dengan baik. Suatu organisasi harus menetapkan :<br>1. Apa yang perlu dikomunikasikan<br>2. Kapan perlu dikomunikasikan<br>3. Kepada siapa hal itu perlu dikomunikasikan<br>4. Apa saja proses komunikasi?<br>5. Siapa yang bertanggung jawab atas komunikasi |
| Klausa 8<br>“*Operation*” | Setelah menyelesaikan semua aktivitas perencanaan dan penilaian risiko yang dipersyaratkan oleh standar, sekarang melanjutkan ke tahap implementasi dan operasi. Di sinilah proses dan tindakan yang diidentifikasi untuk mengatasi risiko dan peluang diimplementasikan dan dikendalikan. Untuk menerapkan proses yang efektif, praktik berikut ini sangat penting :<br>1. Proses diciptakan dengan mengadaptasi atau memformalkan aktivitas "Bisnis seperti Biasa" organisasi<br>2. Identifikasi sistematis risiko kelangsungan bisnis yang relevan untuk setiap produk dan layanan<br>3. Definisi dan komunikasi yang jelas tentang rangkaian aktivitas yang diperlukan untuk mengelola risiko |

| Klausa | Penjelasan |
|---|---|
| | kelangsungan bisnis terkait<br>4. Pembagian tanggung jawab yang jelas untuk melaksanakan kegiatan terkait<br>5. Alokasi sumber daya yang memadai untuk memastikan bahwa aktivitas terkait dapat berlangsung saat dan saat diperlukan<br>6. Penilaian rutin atas konsistensi setiap proses yang diikuti dan efektivitasnya dalam mengelola risiko kelangsungan bisnis |
| Klausa 9 "*Performance Evaluation*" | A. Pemantauan, Pengukuran, Analisis dan Evaluasi<br>Sebuah organisasi perlu mengevaluasi kinerja dan efektivitas BCMS untuk memastikan dapat mencapai hasil yang diinginkan. Perlu ditentukan apa yang perlu dipantau dan diukur, metode pemantauan dan pengukuran dan bagaimana hasilnya akan dievaluasi. Ketika kegiatan pemantauan dan pengukuran harus direncanakan, personel yang melakukan kegiatan pemantauan dan pengukuran harus diidentifikasi dan dipilih dengan mempertimbangkan kompetensi dan ketidakberpihakan. Bukti yang tepat dari kegiatan pemantauan dan pengukuran serta hasil kegiatan pemantauan dan pengukuran harus disimpan.<br>B. Audit Internal<br>Tujuan dari audit internal adalah untuk memastikan bahwa BCMS telah diterapkan secara efektif dan untuk mengidentifikasi setiap kelemahan dan peluang untuk perbaikan. Audit internal harus memeriksa :<br>1. Apakah BCMS memenuhi kebutuhan organisasi<br>2. Sesuai dengan persyaratan ISO 22301<br>3. Seberapa konsisten proses dan prosedur diterapkan<br>4. Apakah proses dan prosedur mencapai hasil yang diinginkan<br>C. Audit Program<br>Sebuah organisasi harus melakukan Audit internal pada interval yang direncanakan. Program Audit harus<br>1. Mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya<br>2. Tentukan kriteria dan ruang lingkup untuk setiap Audit<br>3. Pilih Auditor dan lakukan Audit untuk memastikan |

| Klausa | Penjelasan |
|---|---|
| | objektivitas dan ketidakberpihakan proses Audit<br>4. Memastikan hasil Audit dilaporkan kepada manajer terkait<br>5. Menyimpan bukti terdokumentasi dari pelaksanaan program Audit dan hasil Audit<br>6. Pastikan bahwa setiap tindakan korektif yang diperlukan diambil tanpa penundaan untuk mengatasi ketidaksesuaian dan penyebabnya.<br>D. Ulasan Manajemen<br>Manajemen puncak harus meninjau BCMS organisasi pada interval yang direncanakan untuk menilai kecukupan, kesesuaian, dan efektivitasnya yang berkelanjutan dalam memenuhi kebutuhan organisasi.<br>Masukan dan keluaran pertemuan tinjauan manajemen harus memenuhi persyaratan klausul 9. Output harus mencakup keputusan yang terkait dengan peluang peningkatan berkelanjutan dan setiap perubahan yang diperlukan untuk meningkatkan efisiensi dan efektivitas BCMS. Organisasi harus menyimpan informasi terdokumentasi sebagai bukti hasil tinjauan manajemen dan mengkomunikasikan hasilnya kepada pihak berkepentingan yang relevan. |
| Klausa 10<br>"*Improvement*" | Tujuan utama penerapan BCMS adalah untuk memastikan organisasi dapat merespons insiden yang mengganggu secara tepat waktu, dan untuk melanjutkan pengiriman produk dan layanan utamanya pada tingkat yang telah ditentukan sebelumnya hingga kembali ke operasi normal dapat terpengaruh. Analisis akar penyebab yaitu organisasi harus menyelidiki ketidaksesuaian untuk :<br>1. Tetapkan jika ketidaksesuaian ada di tempat lain<br>2. Identifikasi akar penyebab ketidaksesuaian<br>3. Identifikasi tindakan korektif yang diperlukan untuk mencegah terulangnya ketidaksesuaian<br>4. Identifikasi setiap perubahan pada BCMS yang diperlukan.<br>Setiap tindakan korektif yang diidentifikasi untuk mengatasi ketidaksesuaian harus dilaksanakan tanpa penundaan yang tidak semestinya. Tindakan korektif yang diterapkan harus ditinjau ulang untuk menentukan efektivitasnya. |

Penelitian menggunakan perbandingan standarisasi dan kerangka kerja BCP untuk mendapatkan hasil yang akurat dan efektif bagi obyek penelitian. Kerangka kerja sebagai pembanding yaitu pembanding yaitu ISO 27001. Perbedaan dari standarisasi ISO 27001 dan ISO 22301 yaitu seperti pada tabel 2.4 dibawah ini :

**Tabel 2. 4 Perbedaan ISO22301 dan ISO 27001**

| Indikator | ISO 27001 | ISO 22301 |
|---|---|---|
| Alur Proses | Kerangka perlindungan *Information Security Management Systems* (ISMS) pada proses bisnis. | Merencanakan, meninjau, memelihara dan memperbaiki sistem manajemen untuk melindungi dan mengurangi kemungkinan terjadinya insiden yang mengganggu proses bisnis serta memperbaikinya jika insiden terjadi menggunakan PDCA *Life Cycle*. |
| Kekurangan | Terlalu general untuk penelitian yang akan dilakukan dan tidak memiliki alur analisis khususnya seperti *life cycle*. | - (Tidak Ada) |

### 2.2.7 Metode Penelitian Kualitatif

Metode penelitian kualitatif melibatkan pengumpulan data pengalaman pribadi, introspeksi, wawancara, observasi, interaksi dan teks visual yang signifikan bagi kehidupan masyarakat. Metode penelitian kualitatif berawal dari ilmu-ilmu sosial untuk memungkinkan para peneliti untuk belajar berorientasi sosial dan budaya fenomena. Saat ini, penggunaan metode dan analisis kualitatif diperluas hampir ke setiap bidang dan area penelitian. Metode umumnya mencakup data sumber dengan observasi responden, wawancara dan kuesioner, dokumen dan kesan dan persepsi peneliti. Definisi yang baik diberikan oleh Denzin dan Lincoln (1994) bahwa

penelitian kualitatif berfokus pada interpretasi fenomena dalam pengaturan alami mereka untuk masuk akal istilah makna yang dibawa orang ke pengaturan ini.

Data kualitatif adalah kumpulan data yang diperoleh dari wawancara, catatan lapangan, pengamatan dan analisis dokumen. Informasi yang dikumpulkan ini harus terorganisir dan ditafsirkan dengan benar untuk mengekstrak temuan kunci untuk penelitian. Prosedur umum dalam analisis data kualitatif menurut Creswell (1998) yaitu sebagai berikut :

1. Organisasi data menjadi beberapa bentuk yaitu database, kalimat, kata
2. Membaca dengan teliti kumpulan data untuk mendapatkan gambaran atau ikhtisar lengkap tentang apa yang dikandungnya secara keseluruhan. Selama proses, seorang peneliti harus mencatat membuat catatan pendek atau ringkasan dari poin - poin kunci yang menyarankan kemungkinan kategori atau interpretasi
3. Identifikasi kategori atau tema umum dan klasifikasikan hal ini akan membantu peneliti untuk melihat pola atau makna dari data yang diperoleh
4. Integrasikan dan rangkum data untuk audiens. Langkah ini juga mungkin termasuk hipotesis yang menyatakan hubungan di antara kategori-kategori Itu ditentukan oleh peneliti. Rangkuman data dapat diwakili oleh tabel, gambar atau diagram matriks.

Pendekatan kualitatif berfokus pada proses dan pemahaman berdasarkan deskripsi yang kaya dari tubuh pengetahuan. Data mengambil bentuk komunikasi dari responden Itu sendiri, ekstrak dari dokumen penelitian, sumber daya multimedia sumber daya multimedia seperti rekaman audio dan video ini juga mendukung temuan sebuah studi[33].

### 2.2.7 Metode *Failure and Effect Analysis* (FMEA)

*Failure Mode and Effects Analysis* atau FMEA adalah metodologi yang bertujuan untuk memungkinkan organisasi mengantisipasi kegagalan selama tahap desain dengan mengidentifikasi semua kemungkinan kegagalan dalam proses desain atau manufaktur. Dikembangkan pada 1950-an, FMEA adalah salah satu metode peningkatan keandalan terstruktur paling awal. Sampai saat ini masih menjadi metode yang sangat efektif untuk menurunkan kemungkinan kegagalan. FMEA adalah pendekatan terstruktur untuk menemukan potensi kegagalan yang mungkin ada dalam desain produk atau proses. Mode kegagalan adalah cara di mana suatu proses bisa gagal adalah cara kegagalan ini dapat menyebabkan pemborosan, cacat, atau hasil yang berbahaya bagi pelanggan. Mode Kegagalan dan Analisis Efek dirancang untuk mengidentifikasi, memprioritaskan, dan membatasi mode kegagalan ini. Berikut ini waktu yang tepat untuk menggunakan metode FMEA yaitu :

1. Ketika merancang produk, proses, atau layanan baru
2. Ketika berencana melakukan proses yang ada dengan cara yang berbeda
3. Ketika memiliki sasaran peningkatan kualitas untuk proses tertentu
4. Ketika perlu memahami dan meningkatkan kegagalan suatu proses

Selain Itu, disarankan untuk melakukan FMEA sesekali sepanjang masa proses. Kualitas dan keandalan harus secara konsisten diperiksa dan ditingkatkan untuk hasil yang optimal.

FMEA dilakukan dalam tujuh langkah, dengan aktivitas utama di setiap langkah. Langkah - langkah dipisahkan untuk memastikan bahwa hanya anggota tim yang sesuai untuk setiap langkah yang harus hadir. Pendekatan FMEA yang digunakan oleh *QualTIy-One* telah dikembangkan untuk menghindari perangkap umum yang

membuat analisis menjadi lambat dan tidak efektif. Model *QuaIity-One* memungkinkan untuk memprioritaskan aktivitas dan penggunaan waktu tim yang efisien.

Analisis FMEA dapat dilakukan dengan memutuskan kapan harus mengambil tindakan pada FMEA secara historis ditentukan oleh ambang RPN. *Quality-One* tidak merekomendasikan penggunaan ambang RPN untuk menetapkan target tindakan. Target tersebut diyakini dapat mengubah perilaku tim secara negatif karena tim memilih angka terendah untuk mendapatkan di bawah ambang batas dan bukan risiko aktual, yang memerlukan mitigasi. Setelah selesai, Tindakan memindahkan risiko dari posisinya saat ini di Matriks Kritisitas FMEA *Quality-One* ke posisi risiko yang lebih rendah. Metode FMEA dilakukan dengan memberikan nilai dampak *(Severity),* kemungkinan *(Occurance),* dan deteksi *(Detection)* kemudian menghasilkan nilai RPN sebagai penentu tingkat kritis layanan TI[34].

1. *Severity* atau nilai dampak

   Penilaian ini dapat diukur melalui intensitas terjadinya dampak risiko dan gangguan yang menghambat proses bisnis organisasi. Berikut ini tabel 2.5 nilai yang dapat diberikan untuk mengukur tingkat intensitas dampak terjadinya gangguan[34] :

**Tabel 2. 5 Nilai Dampak (*Severity)*[34]**

| TINGKAT | DAMPAK YANG TERJADI | NILAI |
|---|---|---|
| Akibat Berbahaya | Manajemen atau karyawan terluka | 10 |
| Akibat Serius | Kegiatan yang tidak sesuai peraturan yang berlaku | 9 |
| Akibat Ekstrim | Ketidaklayakan produk atau jasa | 8 |
| Akibat Major | Ketidakpuasan pelanggan secara ekstirm | 7 |
| Akibat Signifikan | Kerusakan produk secara keseluruhan | 6 |
| Akibat Moderat | Kinerja yang menurun dan terjadi banyak keluhan | 5 |

| | | |
|---|---|---|
| Akibat Minor | Mengalami kerugian dalam jumlah sedikTI | 4 |
| Akibat Ringan | Mengalami gangguan kecil yang mudah untuk diatasi tanpa menimbulkan gangguan lain | 3 |
| Akibat Sangat Ringan | Mengalami gangguan kecil pada kinerja yang tidak disadari | 2 |
| Tidak Ada Akibat | Tidak disadari dan tidak memberikan dampak pada kinerja | 1 |

2. *Occurance* atau nilai kemungkinan

Penilaian yang megukur intensTIas kemungkinan terjadinya gangguan dari dampak risiko dari layanan TI perusahaan. Berikut ini tabel 2.6 nilai yang dapat diberikan untuk mengukur tingkat intensTIas kemungkinan terjadinya gangguan [34] :

**Tabel 2. 6 Nilai Kemungkinan (*Occurance)***[34]

| TINGKAT | KEMUNGKINAN YANG TERJADI | NILAI |
|---|---|---|
| *Very High* | Lebih dari satu kali setiap hari | 10 |
| Tidak dapat menghindari kegagalan | | |
| *Very High* | Satu kali setiap 3 – 4 hari | 9 |
| Selalu terjadi kegagalam | | |
| *High* | Satu kali dalam 1 minggu | 8 |
| Berulang kali terjadi kegalalan | | |
| *High* | Satu kali dalam setiap 1 bulan | 7 |
| Sering terjadi kegagalan | | |
| *Moderately High* | Satu kali setiap 3 bulan | 6 |
| Saat waktu tertentu kegagalan terjadi | | |
| *Moderate* | Satu kali setiap 6 bulan | 5 |
| Sesekali waktu terjadi kegagalan | | |
| *Moderate Low* | Satu kali dalam 1 tahun | 4 |
| Jarang terjadi kegagalan | | |
| *Low* | Satu kali dalam 1 – 3 tahun | 3 |
| IntensTIas gagal | | |

| TINGKAT | KEMUNGKINAN YANG TERJADI | NILAI |
|---|---|---|
| relative kecil | | |
| *Very Low* | Satu kali dalam 3 – 6 tahum | 2 |
| IntensTIas gagal relative kecil dan sangat jarang terjadi | | |
| *Remote* | Satu kali dalam 6 – 50 tahun | 1 |
| Tidak pernah terjadi kegagalan | | |

3. *Detection* atau nilai deteksi

Penilaian terhadap kemampuan mengendalikan atau penanganan control yang terjadi pada saat gangguan terjadi menghambat proses bisnis organisasi. Nilai ini memberikan gambaran dari kemampuan organisasi melakukan pengendalian dampak risiko dari gangguan yang terjadi. Berikut tabel 2.7 nilai dari deteksi[34] :

**Tabel 2. 7 Nilai Deteksi (*Detection*)[29]**

| TINGKAT | DETEKSI | NILAI |
|---|---|---|
| Hampir tidak ada kemungkinan | Tidak ada metode penaggulangan risiko | 10 |
| Sangat kecil | Tidak memiliki waktu yang cukup pada metode deteksi | 9 |
| Kecil | Metode deteksi tidak dapat mendeteksi ketepatan waktu | 8 |
| Sangat Rendah | Metode deteksi tidak dapat diandalkan ketika mendeteksi ketepatan waktu | 7 |
| Rendah | Efektivitas yang rendah pada metode deteksi yang dignunakan | 6 |
| Sedang | Tingkat efektivitas yang rata – rata pada metode deteksi | 5 |
| Cukup Tinggi | Kemungkinan cukup tinggi pada metode deteksi untuk menganalisis kegagalan | 4 |
| Tinggi | Kemungkinan tinggi untuk menganalisis kegagalan | 3 |
| Sangat Tinggi | Sangat efektif pemanfaatan metode deteksi dengan waktu yang tepat ketika digunakan | 2 |
| Hampir Pasti | Metode deteksi hampir pasti untuk mengukur waktu ketika | 1 |

| | | |
|---|---|---|
| | diimplementasikan | |

Hasil perhItungan dari nilai dampak, kemungkinan, dan deteksi maka *output* yang didapatkan yaitu mengkalikan ketiga variabel menjadi nilai *Risk Priority Number (RPN).* Rumus dari perhItungan RPN yaitu[34] :

**RPN = *Severity (S)* x *Occurance (O)* x *Detection (D)***

Hasil RPN yang sudah didapatkan kemudian digunakan untuk menentukan tingkat risiko berdasarkan metode FMEA. Berikut ini tabel 2.8 level risiko pada FMEA[34] :

**Tabel 2. 8 Level Risiko**

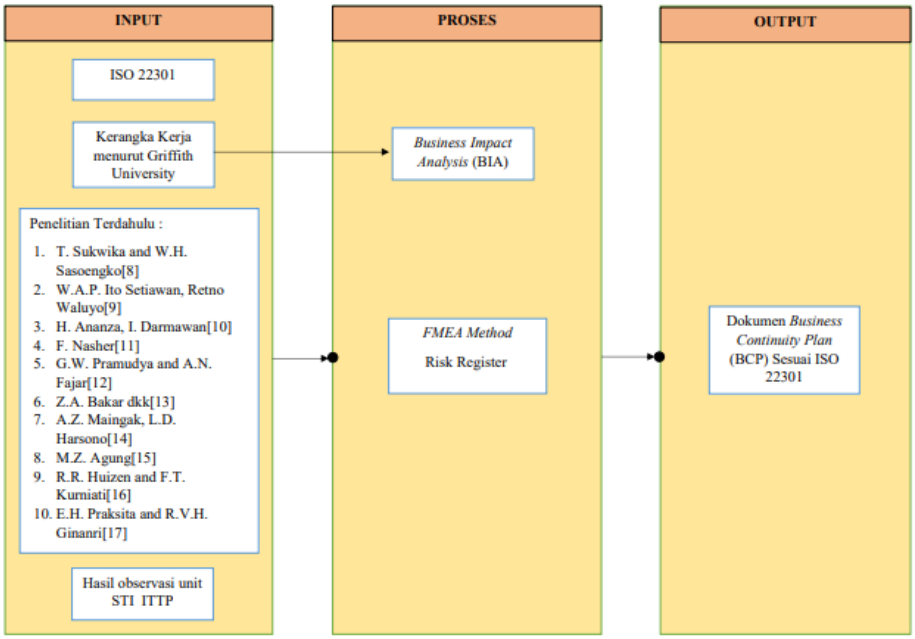
| Level Risiko | Skala Nilai RPN |
|---|---|
| Very High | >200 |
| High | <200 |
| Medium | <120 |
| Low | <80 |
| Very Low | >20 |

Komponen layanan TI yang sudah dilakukan analisis berdasarkan metode FMEA dan memiliki nilai RPN digunakan untuk menentukan level risiko dan skala prioritas yang dapat dilakukan agar organisasi dapat melakukan strategi dan mitigasi penanganan dampak risiko untuk menjaga stabilitas proses bisnis organisasi. Skala prioritas yang harus diperhatikan oleh organisasi yaitu komponen layanan TI yang memiliki nilai RPN tertinggi.

### 2.2.12 Kerangka Pemikiran

Berdasarkan studi literatur penelitian sebelumnya seperti berikut [8][9][12][17] berkaitan dengan penelitian yang akan disusun dari standarisasi yang digunakan menggunakan standar ISO 22301 untuk menilai, menganalisis dan menyusun dokumen BCP. Objek penelitian yang dianalisis dan ditinjau keamanan layanan sistem informasinya

berdasarkan studi literatur [15][16] yaitu sama di organisasi pendidikan dan studi literatur lainnya menggunakan objek perusahaan dan pemerintahan. Selain Itu, sebagai pembanding standarisasi penelitian yang akan dilakukan dengan mempelajari studi literatur seperti berikut [10][11][13][14]16] dengan menggunakan standar ISO 27001 dan metode analisis selain FMEA yaitu OCTAVE[12], SPSS[13], CMMI[14]. Penelitian yang akan dilakukan setelah mempelajari studi literatur [8][16] terkait dengan menggunakan metode *Failure Mode and Effect Analysis* (FMEA) yang menghasilkan RPN. Berikut ini gambar 2.3 kerangka pemikiran untuk menyusun dokumen BCP menggunakan standar ISO 22301.




**Gambar 2. 3 Kerangka Pemikiran**