BAB II
TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Pada penelitian yang dilakukan oleh Driantami *et al*. [8] memiliki tujuan untuk mengidentifikasikan risiko TI, menganalisis tingkat prioritas risiko TI, dan mitigasi risiko TI terhadap sistem penjualan Alphapos pada PT. Matahari Department Store Cabang Malang *Town Square*. Penelitian ini juga menggunakan metode berupa wawancara dan observasi dalam pengambilan datanya; yang dimana menggunakan metode penelitian kualitatif dalam pengolahan datanya dan dibantu dengan kerangka NIST 800-30; serta penentuan analisis *likelihood* (kemungkinan terjadinya risiko) pada sistem Alphapos dan perhitungan *cost-benefit analysis*. Penelitian ini menggunakan Standar ISO 31000: 2009, dan didapatkan hasil penelitian berupa penentuan peringkat risiko dengan 3 deskripsi *risk level*, seperti pencurian *password* otorisasi (tertinggi), koneksi yang tiba-tiba *offline*, dan *humar error*, sehingga dibutuhkan rekomendasi terhadap pengendalian menggunakan *analisis risk reduction, risk avoidance*, serta *cost-benefit analysis* untuk setiap risikonya.

Pada penelitian lainnya, yang dilakukan oleh Ahmad [11] bertujuan untuk melakukan analisis dalam penerapan Manajemen Risiko agar dapat mewujudkan *Good Governance* di Pemerintah Kabupaten Bandung Barat. Sehingga pada penelitian ini, penulis menggunakan metode berupa pengambilan data yang dilakukan dengan cara observasi, wawancara, dan dokumentasi dengan pengolahan datanya secara kualitatif deskriptif; serta melakukan pengujian validitas data seperti *credibility*, *transferability*, *dependability*, dan *confirmability*. Penelitian ini juga menggunakan standar ISO 31000:2009, sehingga memiliki hasil penelitian berupa kegiatan penerapan Manajemen Risiko di Pemerintahan Kab. Bandung Barat masih belum efektif, dikarenakan kurangnya faktor pemahaman, kesadaran dan pentingnya akan Manajemen Risiko, dan sumber daya yang masih kurang memadahi; maka dari itu dibutuhkan peningkatan evaluasi, mitigasi, dan pelaporan

manajemen risiko; serta diperlukan adanya perbaikan dalam kegiatan monitoring dan komunikasi.

Pada penelitian lainnya, yang dilakukan oleh Rilyani *et al*. [19] yang memiliki dua tujuan, yaitu melakukan tahapan dan proses terhadap analisis risiko TI yang berbasis *risk management* dengan standar ISO 31000, serta mengetahui tingkat pada risiko TI terhadap sistem i-Gracias saat ini dan perlakuan risiko yang diberikan. Metode pada penelitian ini menggunakan penelitian kualitatif dan kuantitatif dalam pengolahan datanya, sedangkan pengambilan datanya dilakukan dengan cara wawancara, observasi, maupun kuesioner. Penelitian ini juga menggunakan standar ISO 31000:2009 dan memperoleh hasil penelitian berupa penilaian *Risk Priority Number* (RPN) berdasarkan proses pengukuran pada tiap risiko yang telah dianalisis serta diidentifikasikan, sehingga organisasi mampu melakukan pencegahan, penanganan dan perbaikan sesuai tingkat prioritas risiko.

Pada penelitian yang dilakukan oleh Mahardika *et al*. [32] dengan bertempat di CV. XY memiliki tujuan untuk memperoleh analisis manajemen risiko dibagian IT dengan proses identifikasi risiko, pengukuran risiko, dan membentuk strategi dalam pengelolaan sumber daya yang tersedia. Dalam pemerolehan datanya, dilakukan dengan cara observasi dan wawancara terhadap pihak yang berwenang dan dilakukan pengolahan data dengan metode kualitatif. Penelitian ini menggunakan pedoman standar ISO 31000:2018 yang memperoleh hasil berupa analisis penentuan kemungkinan-kemungkinan risiko sesuai dengan perusahaan atas berbagai tingkatan.

Berikutnya adalah penelitian yang dilakukan oleh Candra *et al.* [33] memiliki beberapa tujuan, yaitu memberikan pemahaman terhadap pejabat atau karyawan DISKOMINFOPS Kab. INHIL dalam melakukan penerapan manajemen keamanan aset teknologi informasi, serta perancangan terhadap kerangka kerja yang berbasis pada keamanan aset teknologi informasi. Penelitian ini, menggunakan metode observasi, wawancara, dan kuesioner dalam pengambilan datanya, sedangkan dalam pengolahan datanya dilakukan dengan metode kualitatif dan kuantitatif. Penelitian ini dilakukan dengan berpedoman pada standar ISO 31000:2018 yang memperoleh hasil berupa identifikasi analisis sebanyak 45 risiko,

dengan tiga pengkategorian, yaitu: 14 risiko yang terendah, 16 risiko dengan level menengah, dan 15 dengan risiko tertinggi. Pada 15 risiko yang tertinggi diberikan perlakuan khusus dan untuk kegiatan keseluruhan pengelolaan risiko dilakukan pengujian UAT (*User Acceptance Test*) agar berjalan dengan fungsinya terhadap keamanan aset teknologi informasi.

Berdasarkan penjelasan diatas, berikut merupakan tabel perbandingan antar topik yang menjadi pedoman oleh penulis, dan dapat dilihat pada tabel 2.1.

Tabel 2. 1. Penelitian Terdahulu

No.	Penulis	Tahun	Objek	Standar	Tujuan	Metode	Hasil
1.	Driantami *et al.*	2018	PT. Matahari Department Store Cabang Malang *Town Square*	ISO 31000: 2009	Mengidentifikasi risiko TI, menganalisis tingkat prioritas risiko TI, dan mitigasi risiko TI terhadap sistem penjualan Alphapos.	1. Melakukan wawancara dan observasi untuk pengambilan data. 2. Penelitian kualitatif untuk pengolahan data yang dibantu kerangka NIST 800-30, serta penentuan *likelihood* pada sistem Alphapos dan perhi-tungan c*ost-benefit analysis.*	Analisis sistem Alphapos menghasilkan penentuan peringkat risiko dengan 3 deskripsi *risk level* dan rekomendasi terhadap pengendalian menggunakan *cost-benefit analysis* untuk setiap risiko.
2.	Ahmad	2019	Pemerintahan Kabupaten Bandung Barat	ISO 31000: 2009	Untuk melakukan analisis dalam penerapan Manajemen Risiko agar dapat mewujudkan *Good Governance* di Pemerintah Kab. Bandung Barat.	1. Melakukan observasi, wawancara, dokumentasi dalam pengambilan data. 2. Penelitian kualitatif deskriptif untuk pengolahan datanya dan pengujian validitas data (*Credibility, Transferability, Dependability, Confirmability*)	Dalam penerapan Manajemen Risiko di Pemerintahan Kab. Bandung Barat masih belum efektif, dikarenakan kurangnya faktor pemahaman, kesadaran dan pentingnya akan Manajemen Risiko, dan sumber daya yang kurang memadahi.

3.	Rilyani *et al.*	2015	Telkom University	ISO 31000: 2009	1. Melakukan tahapan dan proses terhadap analisis risiko TI yang berbasis risk management dengan standar ISO 31000 2. Mengetahui tingkat pada risiko TI sistem i-Gracias saat ini dan perlakuan risiko yang diberikan	1. Pengambilan data dengan observasi, wawancara dan kuesioner 2. Pengolahan data dengan melakukan penelitian kualitatif dan kuantitatif	Menghasilkan *Risk Priority Number* (RPN) berdasarkan dari hasil proses pengukuran pada tiap risiko yang telah dianalisis serta diidentifikasikan, sehingga organisasi mampu melakukan pencegahan, penanganan dan perbaikan sesuai tingkat prioritas risiko.
4.	Mahardika *et al.*	2019	CV.XY	ISO 31000: 2018	Melakukan analisis manajemen risiko dengan proses identifikasi risiko, pengukuran risiko, dan membentuk strategi dalam pengelolaan sumber daya yang tersedia.	1. Melakukan observasi, dan wawancara dalam proses pengambilan datanya 2. Pengolahan data dilakukan dengan metode kualitatif.	Memperoleh analisis berupa penentuan kemungkinan risiko sesuai perusahaan dengan berbagai tingkatan

5.	Candra *et al.*	2019	DISKOMINFOPS Kab. Indragiri Hilir	ISO 31000: 2018	1. Memberikan pemahaman akan pentingnya keamanan terhadap aset teknologi informasi. 2. Memberikan perancangan terhadap kerangka kerja dalam proses pengelolaan risiko keamanan aset teknologi informasi	1. Dalam pengambilan datanya, dilakukan kegiatan observasi, wawancara dan kuesioner. 2. Pengolahan data dilakukan dengan metode kualitatif dan kuantitatif.	1. Memperoleh analisis berupa hasil identifikasi risiko sebanyak 45, dengan 14 risiko level yang rendah; 16 hasil risiko level menengah; dan 15 risiko level yang tinggi. 2. Melakukan perlakuan khusus terhadap 15 risiko dengan level tertinggi dan pengujian UAT (*User Acceptance Test*) akan keamanan aset teknologi informasi pada DISKOMINFOPS Kab. Indragiri Hilir.

2.2. Dasar Teori

2.2.1. Keamanan Informasi

Dengan adanya berbagai macam informasi yang bersifat krusial, keamanan informasi merupakan tindakan yang tepat dalam organisasi untuk menjaga informasi tersebut dari risiko yang akan muncul. Keamanan informasi sendiri, tidak hanya berkaitan dengan bidang teknologi dan sumber daya manusianya saja, namun dapat berkaitan dengan bidang manajemen, seperti sistem yang berlaku dalam manajemen tersebut; kebijakan dalam organisasi; dan perilaku dari manusia dalam kegiatan manajemen [20].

Secara umum keamanan informasi memiliki 3 aspek atau unsur penting, yaitu kerahasiaan (*confidentiality*); keutuhan (*integrity*) dan ketersediaan (*availability*). Kerahasiaan memiliki arti yaitu informasi yang diakses harus berdasarkan pada pihak yang berwenang atau bersangkutan dan bersifat aman dari pihak luar (tidak berwenang). Kemudian keutuhan dapat diartikan bahwa dalam informasi harus bersifat utuh atau tidak mengalami pengurangan yang dilakukan secara sengaja. Sedangkan ketersediaan berarti informasi yang diperoleh tersebut, harus dapat diakses dimanapun dan kapanpun [21]. Dengan adanya hal ini, tentu kegiatan kontrol dalam pengamanan informasi dapat ditingkatkan dengan pengambilan keputusan serta mengurangi potensi risiko-risiko yang akan muncul.

2.2.2. Aset Informasi dan Teknologi

Pada sebuah instansi/organisasi tentu memiliki aset atau alat pendukung dalam menjalankan bisnisnya masing-masing. Aset-aset ini dapat berupa aset yang berwujud dan tidak berwujud yang digunakan sebagai bentuk untuk melakukan serta mendukung proses kegiatan informasi. Setiap aset juga memiliki kategori, yang meliputi [22]:

a. Aset utama dapat diartikan sebagai bentuk informasi atau proses pada sebuah instansi/organisasi dalam kegiatan untuk membentuk perancangan, perencanaan, dan pengelolaan keberlangsungan bisnis sesuai dengan konteks untuk memperoleh keamanan informasi. Aset utama dapat berupa:

1. Informasi; dan
2. Kegiatan organisasi, proses bisnis, dan sub-proses bisnis

b. Aset pendukung merupakan semua hal/barang yang dapat mendukung proses dalam kinerja aset utama agar dapat dilaksanakan sesuai perencanaan. Aset pendukung sangat berkaitan erat dengan aset utama, yang apabila tidak dapat bekerja secara semaksimal mungkin, tentu akan memperoleh kegagalan dalam proses kegiatan aset utama. Aset pendukung dapat berupa:
    1. Personel (manusia);
    2. Jaringan;
    3. Perangkat keras;
    4. Perangkat lunak;
    5. Tempat; dan
    6. Struktur dalam organisasi.

2.2.3. Manajemen Risiko

Manajemen risiko sangat melekat dengan definisi dasarnya berupa risiko yang memiliki arti ketidakjelasan atau ketidakpastian dalam sebuah kejadian yang dimana mampu menghalangi serta berdampak negatif bagi sebuah organisasi dalam mencapai tujuannya [23]. Selain itu dalam Kamus Besar Bahasa Indonesia sendiri, menjelaskan bahwa risiko merupakan tindakan yang bersifat membahayakan dan dapat menyebabkan kerugian [24]. Risiko yang bersifat berbahaya ini, dapat berupa pelaksanaan tugas maupun kondisi tempat kerja pada tingkat yang dapat ditoleransi yang berkaitan dengan kerugian akan Sumber Daya Manusia (SDM) bahkan ekonomi dalam organisasi [25].

Manajemen risiko merupakan sebuah proses kegiatan terkoordinasi berupa pengelolaan risiko yang mencakup identifikasi, evaluasi, serta pengendalian risiko yang dapat meningkatkan aktivitas dan keberlangsungan sebuah organisasi atau perusahaan [26]. Dalam penerapannya, manajemen risiko dapat menganalisis kejadian apa yang akan terjadi serta konsekuensi apa yang akan muncul, sebelum memutuskan sebuah kegiatan dan waktu yang tepat dalam mengurangi resiko ke

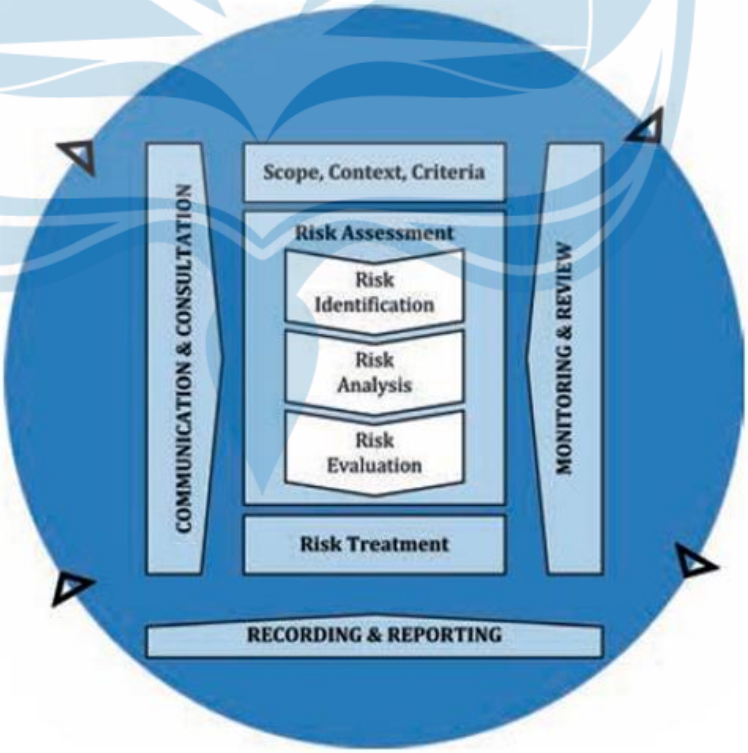
level yang dapat dipastikan atau diterima [27]. Manajemen risiko memiliki tujuan utama dalam memberikan pandangan mengenai hal yang akan terjadi sehingga organisasi mampu menyusun rencana dalam upaya pencegahan dan penilaian terhadap risiko. Hal ini dapat dilihat dari 5 tahapan utama dalam manajemen risiko, yaitu: (1) penetapan konteks, (2) pengidentifikasian risiko/bahaya yang muncul, (3) penganalisisan risiko, (4) penilaian dan pengevaluasian risiko, (5) serta pencegahan akan risiko [26].

2.2.4. ISO 31000: 2018

Standar ISO 31000 diterbitkan oleh *The International Organization for Standardization* pada tanggal 13 November 2009, yang digunakan oleh seluruh jenis organisasi atau perusahaan dalam menghadapi berbagai risiko, yang berkaitan dengan aktivitas pada organisasi tersebut [8]. ISO 31000 memiliki 2 tahapan dalam proses pengerjaan manajemen risikonya, berupa *risk assessment* dan *risk treatment*. *Risk assessment* adalah sebuah proses dalam penentuan risiko yang dapat mengganggu aktivitas organisasi dalam mencapai tujuan bisnisnya (*business goals*). Dalam tahapan risk assessment ini, terdapat 3 proses utama yaitu *risk identification* yang merupakan sebuah proses dalam pengidentifikasian kemungkinan risiko yang akan terjadi; kemudian *risk analyst* berarti proses dalam penentuan risiko yang dapat menghambat tujuan bisnis; serta *risk evaluation* merupakan proses evaluasi pada setiap kemungkinan risiko yang terjadi berdasarkan tingkat kerentanan dan kriteria yang telah dibuat. Sedangkan *risk treatment* merupakan upaya dalam proses penyeleksian terhadap kemungkinan risiko sebelumnya, sehingga dampak dan kemungkinan risiko tersebut dapat berkurang atau bahkan dapat bertambah [28]. Proses tersebut dapat ditunjukkan pada gambar 2.1.

Dalam ISO 31000 terdapat prinsip; kerangka; dan proses pada manajemen risiko yang dapat digunakan untuk menjamin usaha berupa penerapan manajemen risiko yang tepat dan efektif. Pada bagian prinsip, terdiri dari (1) perlindungan dan penambahan nilai; (2) bagian terpadu pada proses organisasi; (3) bagian dalam pengambilan keputusan; (4) penanganan berupa hal yang ketidakpastian;

(5) memiliki sifat yang terukur, sistematis dan tepat waktu; (6) berlandaskan pada informasi yang terbaik; (7) harus disesuaikan dengan organisasi; (8) harus mempertimbangkan faktor kebudayaan dan kemanusiaan; (9) bersifat inklusif serta transparan; (10) bersifat dinamis, berulang, dan responsif terhadap perubahan yang ada; dan (11) yang pastinya harus mampu membangun peningkatan mutu organisasi. Di bagian kerangka sendiri, memiliki komponen dasar, seperti (1) komitmen dan mandat; (2) desain terhadap kerangka manajemen risiko; (3) penerapan dalam manajemen risiko; (4) kegiatan dalam *review* dan *monitoring* pada kerangka; serta (5) peningkatan dengan kerangka kerja yang dilakukan secara berkala. Sedangkan pada bagian proses terdapat beberapa tahap, seperti (1) kegiatan konsultasi dan komunikasi; (2) penetapan konteks; (3) penilaian terhadap risiko, berupa identifikasi, analisis dan evaluasi; (4) penindakan yang tepat terhadap risiko; (5) peninjauan dan pengawasan; serta (6) pencatatan terhadap proses manajemen risiko [11].



Gambar 2. 1. *Risk Management - Guidelines* [29]