BAB II
TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Studi sebelumnya mengenai analisis risiko pada sistem informasi menggunakan ISO 31000: 2009 pernah dilakukan oleh Rahmawati dan Wijaya [7]. Objek penelitian yang digunakan adalah *IT Operation System* (iTop) yang merupakan sebuah sistem yang digunakan PT. ABCD dalam membantu menerima *customer incident.* Sistem ini digunakan PT.ABCD agar dapat mengetahui kualitas layanan pada *customer*. Studi ini dilakukan dengan harapan dapat meminimalisir peluang risiko-risiko yang mungkin terjadi pada sistem iTop.Pada tahap pertama yang dilakukan penelitian ini dilakukan proses identifikasi aset yang berkaitan dengan sistem iTop seperti *software, hardware* dan data dengan melakukan proses *interview* dengan *IT Operation Support* & *Biz Deputy Head* pada PT. ABCD. Kemudian, pada tahapan selanjutnya yaitu mengidentifikasi kemungkinan potensi risiko – risiko yang mungkin terjadi pada aset sistem iTop baik secara fisik maupun logic. Setelah melakukan mengidentifikasi kemungkinan risiko – risiko, dilakukannya penilaian risiko menggunakan metode ISO 31000: 2009 dengan mengklasifikasi risiko beserta tingkatannya. Berdasarkan hasil analisis risiko yang telah dilakukan, terdapat 21 kemungkinan risiko yang terdiri dari 8 kemungkinan risiko tingkat sedang (*medium)* dan 17 kemungkinan risiko tingkat rendah (*low*). setelah melakukan analisis risiko, peneliti memberikan usulan saran perlakuan risiko (*risk treatment*) yang diharapkan dapat mengurangi, meminimalisir, dan mencegah kemungkinan risiko yang mungkin terjadi.

Penelitian selanjutnya mengenai analisis risiko teknologi informasi pada Lembaga Penerbangan dan Antariksa (Lapan) menggunakan ISO 31000: 2009 yang dilakukan oleh Nice dan Imbar dengan objek penelitian *website Space Weather Information and Forecast Services* (SWIFTS) dengan menggunakan ISO 31000:2009 [8]. SWIFTS adalah *website* yang digunakan LAPAN dalam menunjang kinerja sistem, mendukung berjalannya proses bisnis, dan menyampaikan informasi kepada masyarakat. Penelitian ini dilakukan dengan

harapan dapat meminimalisir peluang risiko-risiko yang mungkin terjadi pada *website* SWIFTS. Pada tahap pertama yang dilakukan penelitian ini dilakukan proses identifikasi aset untuk mengetahui kemungkinan risiko yang mungkin terjadi pada aset-aset SWIFTS dengan melakukan observasi dan wawancara dengan pihakpihak yang terkait langsung. Kemudian pada tahap selanjutnya dilakukan identifikasi kemungkinan risiko yang mungkin akan terjadi pada website SWIFTS dari faktor Alam/Lingkungan, Manusia, Sistem dan Infrakstruktur. Berdasarkan hasil identifikasi dampak risiko yang dilakukan, terdapat 7 kemungkinan risiko yang mungkin akan terjadi pada *website* SWIFTS yang terdiri dari 2 risiko tingkat rendah (*low*), 2 tingkat menengah (*moderate*), dan 3 tingkat tinggi (*high*). Peneliti menyarankan untuk mengimplementasikan usulan *risk treatment* dengan harapan agar setiap risiko-risiko yang mungkin terjadi dapat terhindar.

Penelitian selanjutnya mengenai analisis manajemen risiko sistem informasi menggunakan ISO 31000 pernah dilakukan oleh Fernando dengan objek penelitian *Automotive Management System* (AMS) [9]. AMS merupakan sebuah sistem yang yang digunakan Perusahaan Agung Toyota untuk meningkatkan kinerja perusahaan dan membantu dalam melakukan pengelolaan data penjualan seperti data kredit tunai, data faktur kendaraan, data leasing, data pemesanan kendaraan hingga data laporan penjualan. Penelitian ini dilakukan dengan harapan dapat meminimalisir peluang risiko-risiko yang mungkin terjadi pada AMS. Pada tahap pertama pada penelitian ini dikakukannya pengumpulan data dengan mengidentifikasi aset yang berkaitan dengan AMS dengan cara melakukan observasi dan *interview*. Tahap selanjutnya yaitu melakukan analisis risiko dan evaluasi risiko dengan menggunakan metode ISO 31000: 2009. Setelah dilakukan analisis risiko dan evaluasi risiko, diketahui terdapat 9 risiko yang mungkin terjadi yang terdiri dari 1 risiko tingkat tinggi (*high*), 4 risiko tingkat sedang (*medium*), dan 4 risiko tingkat rendah (*low*). Peneliti memberikan saran kepada perusahaan untuk melakukan *monitoring* dan *review* secara terus menerus agar dapat mencapai sasaran dalam implementasi manajemen risiko.

Pengestu dan Wijaya melakukan analisis manajemen risiko pada perpustakaan XYZ menggunakan ISO 31000: 2018 dengan objek penelitian aplikasi SINTESA [10]. SINTESA merupakan sebuah sistem informasi *support system* yang digunakan untuk membantu perpustakaan XYZ dalam melakukan mencatat buku yang dipinjam , daftar ketersediaan buku, total stok buku, waktu jatuh tempo buku dan daftar peminjam buku. Penelitian ini dilakukan dengan harapan dapat meminimalisir peluang risiko-risiko yang mungkin terjadi pada SINTESA. Pada tahap awal penelitian ini dilakukannya identifikasi aset yang berkaitan dengan

aplikasi SINTESA seperti *software, hardware* hingga data. Dalam proses ini dilakukan juga *interview* dengan Kepala Bagian Perpustakaan dan Staff TI-PD yang bertanggung jawab dalam pemeliharaan SINTESA. Setelah melakukan identifikasi aset, kemudian masuk ke tahap identifikasi risiko agar dapat mengetahui kemungkinan risiko – risiko dengan melakukan pengelompokan berdasar faktor alam/lingkungan, manusia , dan sistem dan infrastruktur. Berdasarkan analisis risiko diketahui bahwa terdapat 18 kemungkinan risiko yang terdiri dari 2 risiko tinggat tinggi (*high*), 7 risiko tingkat menengah (*medium*), dan 8 risiko tingkat rendah (*low*). Peneliti memberikan saran dan berharap dari penelitian ini dapat digunakan perpustakaan XYZ dalam Menyusun kebijakan agar dapat meminimalisir peluang risiko – risiko yang mungkin akan terjadi.

Penelitian selanjutnya mengenai analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pernah dilakukan oleh Miftahatun dengan objek penelitian pada website Ecofo [11]. Ecofo merupakan sebuah website yang digunakan sebagai pengelolaan data tiket oleh Kesatuan Pemangkuan Hutan (KPH) Banyumas timur yang merupakan perusahaan umum dibawah naungan Badan Usaha Milik Negara (BUMN). Pada tahap awal penelitian ini peneliti melakukan pengumpulan data dengan mengidentifikasi aset yang berkaitan dengan Efoco dengan cara melakukan wawancara, observasi dan dokumentasi. Tahapan selanjutnya yaitu melakukan penilaian risiko (identifikasi risiko, analisis risiko, evaluasi risiko). Berdasarkan penilaian risiko yang dilakukan, teridentifikasi 24 kemungkinan risiko dimana terdapat 3 risiko tingkat tinggi (*high*), 10 risiko tingkat sedang (*medium*), dan 11 risiko tingkat rendah (*low*) yang dapat dijadikan acuan pencegahan, penanganan dan pemeliharaan terhadap aset teknologi informasi di KPH Banyumas Timur.

Sesuai paparan penelitian terdahulu yang telah dijelaskan sebelumnya, peneliti telah merangkum kedalam tabel yang dapat dilihat pada tabel 2.1 yang berisi tentang ringkasan pada penelitian ini dengan tujuan sebagai pembanding dengan penelitian-penelitian terdahulu.

Tabel 2.1 Perbandingan Penelitian Sebelumnya

No	Penulis	Tahun	Domain	Tujuan	Metode	Alat	Hasil
1	Rahmawati & Wijaya [7].	2019	Manajemen risiko pada teknologi informasi manajemen	Melakukan dokumentasi berbagai macam kemungkinan risiko serta mengelompokan risiko-risiko tersebut dalam aplikasi iTop terhadap perusahaan	Penelitian ini menggunakan metode pengumpulan data wawancara.	ISO 31000: 2009	Terdapat 21 kemungkinan risiko yang terdiri dari 8 kemungkinan risiko tingkat sedang (*medium)* dan 17 kemungkinan risiko tingkat rendah (*low*). setelah melakukan analisis risiko, peneliti memberikan usulan saran perlakuan risiko (*risk treatment*)
2	Nice & Imbar [8].	2017	Manajemen risiko teknologi informasi operasional	Melakukan tahapan proses analisis risiko TI pada website SWIFTS menggunakan standar dan kerangka kerja ISO 31000 serta melakukan dokumentasi *level* risiko dan *risk treatment*	Penelitian ini menggunakan metode pengumpulan data observasi dan wawancara.	ISO 31000: 2009	Terdapat 7 kemungkinan risiko yang mungkin akan terjadi pada *website* SWIFTS yang terdiri dari 2 risiko tingkat rendah (*low*), 2 tingkat menengah (*moderate*), dan 3 tingkat tinggi (*high*).

3	Fernando [9].	2020	Manajemen risiko pada sistem operasional manajemen	mengukur tingkat risiko teknologi informasi yang ada pada Sistem Informasi AMS.	Penelitian ini menggunakan metode pengumpulan data observasi, wawancara dan kuesioner.	ISO 31000: 2009	Terdapat 9 risiko yang mungkin terjadi yang terdiri dari 1 risiko tingkat tinggi (*high*), 4 risiko tingkat sedang (*medium*), dan 4 risiko tingkat rendah (*low*)
4	Pangestu & Wijaya [10].	2020	Manajemen risiko pada sistem informasi perpustakaan	Mengetahu celah - celah atau kemungkinan - kemungkinan risiko yang mungkin terjadi pada sistem dan memberikan *risk treatment* dari kemungkinan - kemungkinan risiko yang mungkin terjadi.	Penelitian ini menggunakan metode pengumpulan data wawancara.	ISO 31000: 2018	Terdapat 18 kemungkinan risiko yang terdiri dari 2 risiko tinggat tinggi (*high*), 7 risiko tingkat menengah (*medium*), dan 8 risiko tingkat rendah (*low*). peneliti memberikan usulan saran perlakuan risiko (*risk treatment*).

5	Miftahatun [11].	2020	Manajemen		Penelitian ini	ISO 31000: 2009	Berdasarkan hasil teridentifikasi 24 kemungkinan risiko yang terdiri dari 3 risiko
			risiko sistem informasi operasional	Melaksanakan tahapan proses analisis manajemen risiko pada sistem informasi Efoco menggunakan standar ISO 31000	menggunakan metode pengumpulan data berupa wawancara, observasi dan dokumentasi.		tingkat tinggi (*high*), 10 risiko tingkat sedang (*medium*), dan 11 risiko tingkat rendah (*low*). Peneliti memberikan usulan saran perlakuan risiko.

2.2. Dasar Teori

2.2.1. Sistem Informasi

Sistem informasi (*information system*) dapat dipahami sebagai kumpulan komponen yang saling berkaitan yang mengumpulkan, memproses, menyimpan dan menyebarkan infromasi pada suatu organisasi dalam rangka mendukung sebuah pengambilan keputusan . Sistem informasi digunakan untuk membantu organisasi dalam menganalisis masalah, mennguraikan hal rumit hingga menciptakan sebuah *output* baru [12] . Sistem informasi juga dapat didefinisikan sebagai gabungan dari 4 komponen utama yang terdiri dari *software, hardware*, fasilitas, dan Sumber Daya Manusia (SDM) yang berpengalaman [13]. Sistem informasi didefinisikan sebagai suatu sistem pada suatu organisasi yang merupakan gabungan dari manusia, insfratuktur, teknologi, sarana, metode – metode dan pengendalian yang difokuskan untuk memperoleh jalur komunikasi yang penting, menangani jenis transaksi khusus, menyampaikan peringatan pengelolaan terhadap keadaan- keadaan tertentu baik internal maupun eksternal yang bernilai dan menyediakan informasi sebagai landasan pengambilan keputusan yang baik [14] .

2.2.2. Manajemen Risiko

Pengertian manajemen risiko tidak terlepas dari kata risiko yang dapat artikan sebagai suatu akibat yang merugikan atau membahayakan yang terjadi karena suatu perbuatan atau tindakan [15] . Risiko juga dapat didefinisikan sebagai ketidakpastian akan suatu peristiwa yang dapat menyebabkan kerugian baik kecil maupun besar yang dapat mempengaruhi suatu organisasi [16] . Secara umum risiko merupakan sebuah peristiwa yang dapat menyebabkan dampak negatif bagi suatu organisasi. Oleh karena itu diperlukannya sebuah pengelolaan risiko agar dapat meminimalisir dampak negatif yang ditimbulkan oleh risiko – risiko tersebut.

Manajemen risiko merupakan sebuah serangkaian aktifitas dalam proses identifikasi risiko, pengukuran risiko, hingga pembentukan strategi untuk dapat mengelola risiko dengan sumber daya yang tersedia. Tujuan dari manajemen risiko itu sendiri yaitu agar dapat mengelola risiko denagan baik untuk mendapatkan hasil

yang maksimal. Untuk mendapatkan hasil yang maksimal, manajemen risiko harus tersusun secara struktur dalam suatu standar atau kerangka kerja yang baik [8].

2.2.2.1. Prinsip – Prinsip Manajemen Risiko

Prinsip manajemen risiko merupakan sebuah suatu landasan yang membantu kita dalam merancang implementasi, mengawas *framework*, dan proses manajemen risiko. Prinsip manajemen risiko dapat dikatakan baik jika menerapkan prinsip – prinsip berikut ini [17] :

1. Manajemen risiko dapat menciptakan dan melindungi nilai
2. Manjemen risiko meningkatkan kinerja dan membantu perusahaan dalam mencapai sasarannya.
3. Manajemen risiko merupakan fragmen dari proses dan tata kelola organisasi.
4. Manajemen risiko yaitu bagian dari proses pengambilan keputusan.
5. Manajemen risiko secara spesifik mampu untuk menangani aspek ketidakpastian.
6. Manajemen risiko merupakan serangkaian langkah yang sistematik, tersutruktur dan tepat waktu.
7. Manajemen risiko berladasan pada data dan informasi terbaik yang tersedia.
8. Manajemen risiko unik berdasarkan kebutuhan penggunanya (*tailored*).
9. Manajemen risiko memperhitungkan aspek manusia dan budaya.
10. Manajemen risiko bersifat transparan dan inklusif.
11. Manajemen risiko bersifat dimanis, berulang dan tanggap akan perubahan.
12. Manajemen risiko berupaya dalam meyediakan perbaikan dan peningkatan organisasi secara berlanjut.

2.2.2.2. Kerangka Kerja Manajemen Risiko

Manajemen risiko harus disusun kedalam suatu kerangka kerja manajemen risiko agar mendapat hasil yang baik. Kerangka kerja ini nantinya akan menjadi standar dan penataan yang melingkupi seluruh aktivitas manajemen risiko pada berbagai macam kegiatan organisasi. Kerangka kerja manajemen risiko akan

menjadi landasan organisasi dalam mengelola risiko serta menjadi landasan dalam mengambil keputusan. Kerangka kerja ini tidak dimaksudkan sebagai sebuah sistem pengelolaan, tetapi lebih ditunjukkan untuk membantu organisasi dalam mengintregrasikan manajemen risiko ke dalam kesuluruhan sistem manajemen organisasi [18]. Kerangka kerja mengelola risiko ditunjukkan pada gambar 2.1.

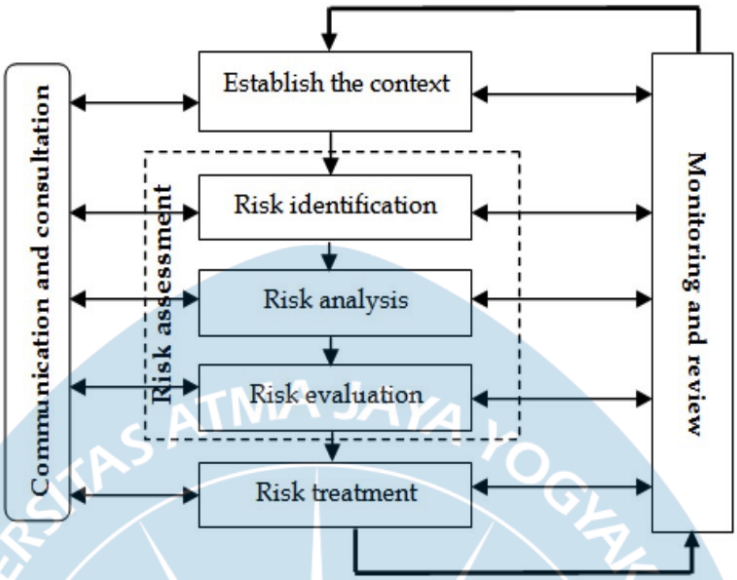
Gambar 2.1. Kerangka Kerja Mengelola Risiko [19].

Kerangka kerja manajemen risiko pada organisasi terdiri dari 5 kompenen yaitu [18] :

1. Mandat dan komitmen
2. Perencanaan kerangka kerja manajemen risiko
3. Penerapan manajemen risiko
4. *Monitoring* dan *review* kerangka kerja
5. Perbaikan kerangka kerja secara berkelanjutan

2.2.2.3. Proses Manajemen Risiko

Proses manajemen risiko merupakan tahapan yang dilakukan untuk mengelola risiko. Pada proses ini terdapat lima aktivitas yaitu (lihat gambar 2.2):



Gambar 2.2. Proses Pengelolaan Risiko *[20].*

1. Komunikasi dan konsultasi (*Communication and consultation*)

   Komunikasi dan konsultasi merupakan suatu aktivitas yang penting dalam manajemen risiko karena harus dilakukan terus – menerus dan berulang. Hal ini penting karena diperlukannya sebuah kesepakatan dari berbagai pihak dalam pengambilan keputusan untuk implementasi kerangka kerja dan manajemen risiko. Selain itu juga agar komunikasi dan konsultasi berjalan dengan efektif dan memperoleh hasil yang maksimal, diperlukan penyatuan visi organisasi ke depan, memberitahukan segala sesuatu mengenai teknik manajemen risiko, dan menyediakan implementasinya [17].

2. Menentukan konteks (*Establish the context*)

   Menentukan konteks merupakan sebuah aktivitas yang bertujuan untuk menetapkan batasan atau skala internal maupun eksternal agar dapat digunakan dalam mengelola risiko dan menentukan kriteria risiko dan lingkup kerja untuk proses berikutnya. Dalam menetapkan konteks meliputi beberapa faktor seperti tujuan strategi, organisasi, lingkup, skala aktivitas organisasi atau bagian dimana manajemen risiko diterapkan. Dalam implementasinya manajemen risiko, perlu dipertimbangkan berdasarkan tanggung jawab, sumber daya, dokumentasi proses dan kewenangan [17].

3. Penilaian risiko (*Risk assessment*)

Penilaian risiko (*Risk Assesment)* pada ISO 31000 dapat didefinisikan sebagai keseluruhan proses yang meliputi identifikasi risiko, analisis risiko dan evaluasi risiko. Pada proses identifikasi risiko, terdapat kategori/kriteria penilaian risiko yakni [21] (lihat tabel 2.2.):

Tabel 2.2. Kategori/Kriteria Penilaian Risiko

Penilaian Risiko	Kategori Risiko	Deskripsi Risiko
3	Tinggi	Ancaman memilki peluang dan pengaruh namun pengendalian yang ada tidak efektif untuk mencegah ancaman
2	Sedang	Ancaman memilki peluang dan pengaruh namun pengendalian yang ada mampu untuk menghambat ancaman
1	Rendah	Ancaman tidak memilki peluang dan pengaruh namun pengendalian yang ada mampu untuk menghalangi ancaman

4. Perlakuan risiko (*Risk treatment*)

Setiap risiko memiliki perlakuan risiko yang berbeda – beda. Oleh karena itu diperlukannya pemeriksaan ulang yang baik terhadap hasil analisis risiko dengan tujuan agar memberikan perlakuan risiko yang tepat sehingga dapat meminimalisir dampak risiko. Secara umum perlakuan risiko memiliki 4 perlakuan yaitu [17]:

a. Menghindari risiko (*risk avoidance*)
b. Mentransfer risiko (*risk sharing/transfer*)

c. Mitigasi (*mitigation*)
d. Menerima risiko (*risk acceptance*)

5. Pemantauan dan peninjauan berkala (*Monitoring and review) Monitoring and review*

Merupakan sebuah proses manajemen risiko yang bertujuan untuk memastikan keseluruhan proses manajemen risiko berjalan dengan baik. Proses ini terdiri dari dua aktivitas yaitu *Monitoring* yang merupakan pengamatan rutin terhadap kinerja manajemen risiko dan *review* yang merupakan kontrol berkala atas kondisi saat ini dengan fokus tertentu.

2.2.3. ISO 31000

ISO 31000 *Risk Management – Guideline on Priciples and implementation of risk management* merupakan salah satu standar manajemen risiko yang dikembangkan oleh *Internartional Standard Organization* (ISO). ISO 31000 yang dirilis pada tanggal 13 November 2009 dan diperbaharui pada februari 2018 merupakan standar manajemen risiko yang universal, yang artinya ISO 31000 dapat digunakan untuk kegunaan yang lebih spesifik atau khusus sehingga dapat diimplementasikan pada segala jenis industri dan organisasi di dunia. Hal yang paling membedakan antara standar ISO 31000 dengan standar manajemen risiko yang lainnya yaitu pada sudut pandang ISO 31000 dimana standar ini memiliki prinsip – prinsip lebih luas dan terperinci dibandingkan standar manajemen risiko lainnya. Standar ISO 31000 memiliki proses manajemen risiko yang umum yang terdapat pada standar manajemen risiko lainnya seperti, identifikasi risiko, penilaian risiko, perlakuan terhadap risiko, dan implementasinya [17].