BAB II
LANDASAN TEORI

Pada landasan teori membahas mengenai dasar-dasar teori dari jurnal ilmiah yang signifikan sesuai permasalahan pada penelitian ini. Landasan teori ini bertujuan sebagai pedoman untuk mendukung penelitian. Berikut merupakan landasan teori dari penelitian ini, yaitu

2.1 Dasar Teori

Pada bagian ini berisi rangkuman dari dasar teori yang digunakan dalam penelitian. Berikut dasar teori yang digunakan.

2.1.1 Risiko

Menurut Kouns dan Minoli (2010) risiko merupakan sesuatu kejadian yang berpotensi menyebabkan kerusakan yang disebabkan oleh ancaman, kerentanan, atau peristiwa (berbahaya atau tidak berbahaya) yang mempengaruhi kumpulan aset TI yang dimiliki oleh organisasi. Sedangkan menurut Darmawi (2016) mendeskripsikan risiko merupakan kemungkinan terjadinya akibat buruk (kerugian) dari adanya kejadian yang tidak diinginkan sehingga dapat mengancam organisasi karena dapat mengakibatkan kerugian. Dari beberapa definisi risiko yang dijelaskan diatas dapat disimpulkan bahwa risiko mengandung unsur:

1. Kemungkinan peristiwa yang terjadi
2. Dampak atau hasil (jika itu terjadi risiko memiliki hasil atau akibat)
3. Probabilitas peristiwa (risiko selalu dalam bentuk probabilitas yang dapat diukur).

Menurut Darmawi (2016), terdapat 2 jenis-jenis risiko yang perlu diketahui yaitu sebagai berikut:

a. *Pure Risk* (risiko murni) merupakan ketidakpastian terjadinya suatu bentuk kerugian. Apabila risiko murni terjadi akan menyebabkan kerugian. Sebaliknya

jika risiko murni tidak terjadi maka tidak akan menimbulkan sebuah kerugian dan keuntungan

b. *Speculative Risk* (risiko spekulatif) merupakan risiko yang dapat menyebabkan kemungkinan kerugian, tetapi kemungkinan kerugian terdapat kemungkinan untung

   Jadi, ada beberapa pengertian diatas risiko merupakan hal yang pasti ada dalam setiap aktivitas yang dilakukan serta berpeluang memiliki dampak negatif terhadap tujuan yang akan dicapai.

Menurut Harsanto dan Hidayat (2018) ada beberapa hal yang menjadi penyebab terjadinya risiko adalah:

1. Risiko *internal* adalah risiko yang terjadi akibat dari dalam organisasi itu sendiri.
2. Risiko *eksternal* adalah risiko yang dapat terjadi akibat faktor luar organisasi.
3. Risiko keuangan adalah risiko yang dapat terjadi akibat dari faktor ekonomi dan keuangan seperti perubahan harga, suku bunga dan lain-lain.
4. Risiko operasional adalah risiko yang terjadi dikarenakan tidak beroperasinya sistem internal yang ada pada sebuah organisasi maupun adanya kesalahan dari manusia dan faktor eksternal yaitu bencana alam dan lain-lain.

2.1.2 Manajemen Risiko

Menurut Darmawi (2016) risiko merupakan suatu usaha untuk mengetahui, menganalisis, serta mengendalikan risiko dalam setiap kegiatan perusahaan dengan tujuan memperoleh efektivitas dan efisiensi yang lebih tinggi. Sedangkan menurut Stoneburner, Goguen, Feringa (2002) manajemen risiko adalah proses mengidentifikasi risiko, menilai risiko dan mengambil langkah-langkah untuk mengurangi risiko ke tingkat yang dapat diterima. Proses utama dari manajemen risiko ada tiga hal yaitu penilaian risiko, mitigasi risiko dan evaluasi serta melakukan penilaian kontrol risiko.

1. Penilaian risiko merupakan kegiatan mengidentifikasi dan mengevaluasi dari risiko yang ada dan efek yang ditimbulkan dalam organisasi, serta merekomendasi agar dapat mengurangi risiko yang terjadi.
2. Mitigasi risiko merupakan tahapan dalam menentukan prioritas, serta menerapkan dan mempertahankan level risiko yang sesuai rekomendasi dalam tahapan penilaian risiko.
3. Evaluasi kontrol merupakan proses evaluasi yang selalu dilakukan pada tahapan manajemen risiko untuk mengukur dan melihat keberhasilan dalam menerapkan sebuah manajemen risiko.

Adapun tujuan dari diterapkannya manajemen risiko yaitu sebagai berikut:

1. Untuk memungkinkan organisasi mencapai misinya dengan mengamankan sistem sistem TI yang menyimpan, memproses, atau mengirimkan informasi organisasi dengan lebih baik
2. Memungkinkan manajemen membuat keputusan manajemen risiko yang terinformasi dengan baik untuk menjustifikasi pengeluaran yang merupakan bagian dari anggaran
3. Membantu manajemen dalam mengesahkan atau mengakreditasi sistem TI berdasarkan dokumen pendukung yang dihasilkan dari kinerja manajemen risiko

2.1.3 Risiko Teknologi Informasi

Menurut Stoneburner, Goguen, Feringa (2002) organisasi menggunakan sistem teknologi informasi untuk memproses informasi dalam mendukung visi dan misi mereka dengan untuk menjadi lebih baik. Risiko merupakan dampak negatif karena adanya kerentanan yang terjadi dengan mempertimbangkan adanya kemungkinan dan dampak kejadian. Teknologi Informasi merupakan risiko terhadap suatu aset berharga dalam sebuah organisasi yang apabila terancam akan menimbulkan kerugian dan dapat mengganggu jalannya proses bisnis dan aktivitas operasional dalam organisasi. Risiko teknologi informasi adalah risiko terhadap aset perusahaan yang disebabkan oleh

pengamalan teknologi informasi, risiko teknologi informasi ini yaitu komponen dari keseluruhan risiko perusahaan. Risiko teknologi informasi bisa berdampak pada operasional perusahaan dan menciptakan tantangan dalam mencapai suatu tujuan dan pencapaian strategis (ISACA, 2009).

Risiko Kehilangan Informasi dan ketahanan dalam penggunaan teknologi dibagi menjadi enam kategori menurut (Harsanto dan Hidayat, 2018) yaitu

1. Keamanan

   Modifikasi atau penggunaan informasi oleh orang yang tidak memiliki hak, contohnya kejahatan dalam dunia maya, kebocoran orang dalam dan terorisme dalam dunia maya dan lain sebagainya.

2. Ketersediaan

   Risiko tidak bisa mengakses data setelah adanya kegagalan sistem, yang disebabkan adanya kesalahan manusia, kurangnya penggunaan arsitektur dan perubahan konfigurasi.

3. Daya pulih

   Risiko tidak mendapatkan informasi secara tepat waktu yang disebabkan oleh kegagalan pada perangkat lunak, perangkat keras, dan ancaman eksternal seperti bencana alam.

4. Performa

   Risiko informasi tidak tersaji saat dibutuhkan, yang disebabkan oleh arsitektur terdesentralisasi, permohonan yang meningkat dan disiplin teknologi informasi yang bermacam.

5. Daya skala

   Adanya risiko sulit dalam menanggulangi berbagai aplikasi baru dan anggaran bisnis dengan efektif karena pertumbuhan bisnis, parameter kemacetan, dan fungsi arsitektur semangkin tinggi.

6. Ketaatan

   Risiko manajemen dalam penerapan informasinya tidak menaati adanya persyaratan peraturan seperti peraturan pemerintah, pedoman peraturan perusahaan, dan kebijakan internal.

2.1.4 Keamanan Informasi

Menurut (ISO/IEC 17799:2005) keamanan informasi adalah perlindungan informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalkan risiko bisnis, dan memaksimalkan pengembalian investasi dan peluang bisnis. Keamanan informasi dicapai dengan menerapkan rangkaian kontrol yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi, dan fungsi perangkat lunak dan perangkat keras. Sedangkan menurut Kouns dan Minoli (2010) Keamanan informasi didefinisikan sebagai perangkat mekanisme, teknik, dan tindakan, dan proses administratif yang digunakan untuk melindungi aset TI dari akses yang tidak sah, alokasi, manipulasi, modifikasi, kehilangan, penggunaan, pengungkapan data dan informasi yang tidak disengaja tertanam dalam aset tersebut

Keamanan sistem informasi mencakup perlindungan dari aspek-aspek berikut (Kouns dan Minoli, 2010)

1. *Confidentiality* (Kerahasiaan) adalah perlindungan terhadap akses yang tidak sah, aproriasi, atau penggunaan aset
2. *Integrity* (Integritas) adalah perlindungan terhadap manipulasi, modifikasi, atau kehilangan aset yang tidak sah
3. *Availabilit*y (Ketersediaan) adalah perlindungan terhadap pemblokiran, pembatasan, atau pengurangan manfaat dari aset.

Gambar 2.1 Aspek Keamanan Informasi
(Sumber: preferreditgroup.com)

Dalam Ketiga aspek tersebut sangat rentan terhadap serangan dan ancaman sumber informasi melalui akses fisik atau jaringan sehingga harus dipenuhi agar keamanan informasi tetap terjaga. Maka dari itu diperlukan manajemen risiko keamanan informasi agar dapat mengurangi dan memitigasi adanya risiko (Astuti, 2022).

2.1.5 Aset Informasi

Menurut IBISA (2011) aset merupakan informasi dari organisasi yang berharga dan penting sehingga harus dilindungi dari berbagai ancaman penyalahgunaan. Sedangkan menurut O'Brien (2009), aset informasi berupa kombinasi terorganisir dari *software*, *hardware*, *people*, data dan *network* yang saling berhubungan. Pengertian *hardware*, *software*, *people*, data, dan *network* menurut Rainer, Prince dan Cegielski (2013) yaitu:

1. *Hardware* terdiri dari perangkat seperti prosesor, monitor, keyboard, dan printer. Hardware atau perangkat keras adalah suatu perangkat yang dapat menerima, memproses program, dan menampilkan data dan informasi.
2. *Software* adalah program atau kumpulan program yang memungkinkan hardware untuk memproses dan mengelola data.
3. Data memuat sekumpulan fakta dari suatu hal yang diperoleh dari pengamatan sumber tertentu, dapat berupa angka, huruf, angka, suara, dan gambar.
4. *Network* adalah sistem koneksi (kabel atau nirkabel) yang menghubungkan perangkat komputer yang berbeda untuk berbagi sumber daya.

5. *People* merupakan individu atau pengguna yang menggunakan hardware dan software, berinteraksi, dan memanfaatkan hasil keluaran dari perangkat tersebut.

2.1.6 Metode NIST SP 800-30 Revisi 1

National Institute of Standard and Technology (NIST) *Special Publication* (SP) 800-30 Revisi 1 merupakan panduan untuk melakukan penilaian risiko sistem informasi dan organisasi dalam mengidentifikasi faktor risiko secara spesifik yang dapat dipantau secara berkelanjutan. Penilaian risiko merupakan salah satu aktivitas utama yang menjadi dasar dan mengawali proses manajemen risiko, di mana organisasi dapat memanfaatkan penilaian risiko untuk menentukan potensi ancaman maupun risiko yang dapat terjadi terhadap aset teknologi informasi pada organisasi. tujuan dalam penilaian risiko yaitu menentukan level ancaman yang dapat menyebabkan kerugian terhadap adanya potensi risiko yang terkait dengan sistem informasi (Permatasari, 2019). Hasil yang diperoleh dari adanya penilaian risiko yaitu dapat membantu organisasi agar dapat mengetahui dan melihat adanya risiko yang terdapat pada sistem serta mengidentifikasi kontrol yang tepat agar dapat memitigasi serta mengurangi risiko yang ada.

Terdapat Proses dalam Penilaian risiko dengan menerapkan metode NIST SP 800-30 Revisi 1 yaitu

1. Mempersiapkan Penelitian
    a. Identifikasi Tujuan

       Mengidentifikasi tujuan penilaian risiko dalam hal informasi yang dihasilkan untuk memastikan bahwa penilaian menghasilkan informasi yang tepat dan mendukung keputusan
    b. Identifikasi Ruang Lingkup

       Mengidentifikasi ruang lingkup penilaian risiko dalam hal penerapan organisasi, kerangka waktu yang didukung, dan pertimbangan arsitektur atau teknologi

c. Identifikasi asumsi dan kendala

Mengidentifikasi asumsi dan kendala spesifik dimana penilaian risiko dilakukan

d. Identifikasi sumber informasi

Mengidentifikasi *Integrated Library System* untuk mengetahui sumber-sumber informasi ancaman, kerentanan, serta dampak yang digunakan dalam penilaian risiko

e. Identifikasi model risiko dan pendekatan analisis

Mengidetifikasi model risiko dan pendekatan analitik yang digunakan dalam penilaian risiko

2. Melakukan penilaian

a. Identifikasi sumber ancaman

Identifikasi dan gambaran sumber ancaman yang menjadi perhatian, termasuk kapabilitas, niat, dan karakteristik penargetan untuk ancaman permusuhan dan berbagai efek untuk ancaman non-permusuhan. Identifikasi potensi peristiwa ancaman, relevansi peristiwa, dan sumber yang dapat memicu peristiwa tersebut

b. Identifikasi kerentanan dan kondisi predisposisi

Identifikasi kerentanan dan kondisi predisposisi yang mempengaruhi kemungkinan kejadian ancaman yang menimbulkan dampak negatif

c. Penentuan kemungkinan

Menentukan kemungkinan bahwa peristiwa ancaman menimbulkan dampak yang merugikan, dengan mempertimbangkan:

1) Karakteristik sumber ancaman yang dapat memulai peristiwa tersebut
2) Kerentanan atau kondisi predisposisi yang diidentifikasi
3) Kerentanan organisasi yang mencerminkan upaya perlindungan atau penanggulangan yang direncanakan atau diimplementasikan untuk menghambat peristiwa tersebut

d. Penentuan dampak

Menentukan dampak buruk dari peristiwa ancaman yang menjadi perhatian dengan mempertimbangkan:

1) Karakteristik sumber ancaman yang dapat memulai peristiwa tersebut
2) Kerentanan atau kondisi predisposisi yang diidentifikasi
3) Kerentanan organisasi yang mencerminkan upaya perlindungan atau penanggulangan yang direncanakan atau diimplementasikan untuk menghambat peristiwa tersebut

e. Penentuan risiko

Menentukan risiko bagi organisasi dari peristiwa ancaman yang menjadi pertimbangan dengan mempertimbangkan:

1) Dampak yang akan dihasilkan dari peristiwa tersebut
2) Kemungkinan terjadinya peristiwa

2.1.7 ISO/IEC 27001:2013

ISO/IEC merupakan singkatan dari *The International Organization for standardization*) *and The International Electrotechnical Commission*) 27001:2013 yaitu salah satu versi yang dikeluarkan oleh ISO/IEC 27001 dan diterbitkan pada tahun 2013. Standar ISO/IEC 27001:2013 ini merupakan edisi kedua pengganti edisi pertama (ISO/IEC 27001:2005) yang telah dilakukan perbaikan secara teknis. Standar ISO/IEC:2013 digunakan oleh pihak internal organisasi maupun pihak eksternal organisasi untuk melakukan penilaian risiko. Penggunaan dari ISO/IEC 27001:2013 dalam penilaian risiko dapat disesuaikan dengan kebutuhan yang diperlukan oleh organisasi untuk mencapai sasaran terhadap keamanan sistem informasi. Standar ISO/IEC 27001:2013 ini memiliki fungsi sebagai petunjuk untuk melakukan kontrol terhadap pengelolaan, penerapan serta untuk meningkatkan manajemen keamanan informasi. ISO/IEC 27001:2013 mempunyai pengendalian keamanan informasi yaitu terdiri dari 14 klausal dan 114 kontrol (*International Organization for Standardization*

27001:2013). Penerapan kontrol tersebut dipilih sesuai dengan ancaman yang relevan terhadap sistem informasi. Adapun 14 klausul ISO/IEC 27001:2013 yang dapat dilihat pada Tabel 2.1.

Tabel 2. 1 Klausul ISO/IEC 27001:2013

A.5	Kebijakan Keamanan informasi
A.6	Organisasi Keamanan Informasi
A.7	Keamanan Sumber Daya Manusia
A.8	Manajemen Aset
A.9	Kontrol Akses
A.10	Kriptografi
A.11	Keamanan Fisik dan Lingkungan
A.12	Keamanan Operasi
A.13	Keamanan Komunikasi
A.14	Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi
A.15	Hubungan Pemasok
A.16	Manajemen Insiden Keamanan Informasi
A.17	Aspek Keamanan Informasi Manajemen Kontinuitas Bisnis
A.18	Kepatuhan

(**Sumber**: ISO/IEC 27001:2013)

2.1.8 *Integrated Library System* (INLISLITE)

Menurut Liya Dachliyani (Bugis, 2019) INLISLITE merupakan sistem informasi yang terintegrasi dalam pengelolaan perpustakaan, yang mengotomatisasi kegiatan dan fungsi perpustakaan dalam melakukan kegiatan pengembangan koleksi, pengolahan bahan pustaka, melengkapi koleksi fisik, pelayanan perpustakaan hingga menghasilkan laporan.

INLISLITE merupakan Sistem Informasi perpustakaan yang dikembangkan pada tahun 2011 oleh Perpustakaan Nasional Republik Indonesia (Perpusnas). Nama INLIS berasal dari istilah *Integrated Library System*, yang digunakan untuk kegiatan keperluan rutin dalam pengelolaan informasi perpustakan di internal Perpusnas. Dikembangkan sebagai perangkat untuk dapat mengelola perpustakaan secara otomatisasi, sekaligus pengembangan perpustakaan berbasis digital serta mengelola dan layanan koleksi digital.

2.1.8.1 Fungsi dan Tugas Pokok INLISLITE

Terdapat 12 modul utama dalam inlislite yaitu back office, baca ditempat, buku tamu, keanggotaan online, layanan koleksi digital. online public access catalogue, artikel, pendaftaran anggota, statistik, survey, pengembalian mandiri, dan peminjaman mandiri. Berikut adalah penjelasan dari setiap modul pada *Integrated Library System* (Panduan Inlislite, 2016)

1. Modul *Back Office*

Modul *back office* berfungsi melakukan pengelolaan informasi perpustakaan antara lain data anggota, data buku, sirkulasi (Peminjaman dan pengembalian) dan lain sebagainya. Pustakawan dan petugas perpustakaan lainnya yang bertanggung jawab dapat menambah, memodifikasi, dan menghapus data menggunakan modul ini. sehingga penerima tugas diharuskan memiliki akun untuk dapat masuk kedalam sistem dengan memasukkan *username* dan *password*.

Terdapat beberapa fungsi yang ada pada modul *back office* antara lain:

a. Fungsi pengelolaan bahan pustaka

   Pengelolaan bahan pustaka dimasukkan kedalam sistem dengan menu akuisisi, katalog, laporan mengenai pengadaan dan pengolahan bahan pustaka.

b. Fungsi Pelayanan

   Fungsi pelayanan dipakai dalam meninjau aktivitas anggota di ruang pelayanan, seperti:

   1) Menu SSKCKR berfungsi memasukkan karya cetak dan karya rekam seperti buku, jurnal, laporan, surat kabar, skripsi dan lain lain.
   2) Menu keanggotaan berfungsi dalam melakukan pengolahan data anggota, seperti memasukkan data anggota, menambahkan foto anggota, melihat anggota yang sudah terdaftar, serta mencetak kartu anggota.

3) Menu sirkulasi (peminjaman dan pengembalian) berfungsi untuk memasukkan data koleksi yang akan dipinjam dan dikembalikan. Tersedia menu pendataan ulang dan monitoring koleksi yang masih dipinjamkan.
4) Menu loker berfungsi meminjamkan dan mengembalikan kunci loker sebagai tempat penyimpanan barang pemustaka.
5) Menu survey digunakan sebagai pembuat kuesioner online untuk mendapatkan umpan balik meliputi saran ataupun kritik dari pengguna.
6) Menu buku tamu berfungsi melihat data pengunjung yang datang ke perpustakaan.
7) Menu opac berfungsi dalam menampilkan data pencarian koleksi yang diinginkan pengguna.
8) Menu layanan koleksi digital berfungsi dalam menampilkan data pencarian katalog yang mempunyai konten secara digital digunakan sebagai tampilan kepada pemustaka.
9) Menu baca ditempat berfungsi mengetahui koleksi yang dibaca oleh pemustaka di ruang baca perpustakaan atau koleksi tersebut tidak dipinjam.

2. Modul baca ditempat

Modul baca ditempat adalah sarana pendukung layanan yang berfungsi dalam melakukan pencatatan koleksi buku yang dibaca oleh pemustaka pada ruang baca. Sehingga dengan begitu dapat dilihat tingkat kegunaannya.

3. Modul buku tamu

Modul buku tamu berfungsi untuk melakukan pencatatan kunjungan pemustaka yang datang ke perpustakaan. Data ini memungkinkan untuk memperoleh laporan informasi tentang kunjungan pengunjung dalam jangka waktu tertentu.

4. Modul Keanggotaan online

Modul keanggotaan online berfungsi sebagai sarana dalam melihat profil pribadi bagi para pemustaka. Dalam modul keanggotaan online ini para pemustaka dapat juga mengetahui aktivitasnya saat menggunakan layanan perpustakaan. Modul ini memungkinkan pengguna untuk mengubah kata sandi keanggotaan, memperbaharui data dan bahkan mengunggah karya ilmiah.

5. Modul Layanan koleksi digital

Fungsi modul layanan koleksi digital digunakan untuk melakukan penerbitan koleksi digital secara online. Dengan modul ini dapat secara otomatis mengklasifikasikan pencarian katalog yang mempunyai konten digital untuk ditampilkan.

6. Modul online public access catalogue (opac)

Modul opac berfungsi membantu pengguna menemukan koleksi yang mereka butuhkan melalui kata kunci dari koleksi pustaka yang akan dicari dimasukkan ke dalam modul opac.

7. Modul Artikel

Modul artikel berfungsi membantu pengguna perpustakaan dalam menemukan artikel yang dibutuhkan dengan memasukkan kata kunci dari judul artikel, peneliti dan subjek.

8. Modul pendaftaran anggota

Modul pendaftaran anggota berfungsi untuk melakukan pendaftaran anggota secara online dengan memasukkan identitas sesuai dengan syarat-syarat yang ditetapkan.

9. Modul Statistik

Modul informasi statistik berfungsi untuk menampilkan data grafik tentang pertumbuhan kunjungan, jumlah kunjungan dari anggota, pertumbuhan anggota, jumlah anggota, pertumbuhan koleksi, jumlah koleksi, pertumbuhan koleksi yang dipinjamkan, jumlah total koleksi yang dipinjamkan, dan pertumbuhan koleksi yang dibaca, jumlah total koleksi yang dibaca.

10. Modul Survey

Modul survey berfungsi memberikan umpan balik berkaitan dengan kepuasan pustakawan terhadap kebutuhan akan fasilitas dan layanan yang disediakan oleh pengelola perpustakaan.

11. Modul Peminjaman mandiri

Modul peminjaman mandiri berfungsi untuk meminjamkan koleksi dengan memasukkan nomor anggota yang sudah terdaftar atau dapat memindai barcode secara otomatis.

12. Modul pengembalian mandiri

Modul pengembalian berfungsi untuk melakukan pengembalian terhadap item koleksi yang dipinjam, dengan dapat memasukkan kode barcode item koleksi yang dipinjam

2.1.9 Dinas Perpustakaan dan Kearsipan Daerah Kabupaten Sambas

Dinas Perpustakaan dan Kearsipan Daerah Kabupaten Sambas merupakan penyelenggara kebijakan daerah yang berspesifik dibidang perpustakaan dan kearsipan. Berkomitmen dalam melaksanakan, memelihara, mendukung dan pengembangan sistem layanan perpustakaan. Yang telah dibentuk sesuai dengan Peraturan Bupati Sambas Nomor 50 Tahun 2016 tentang kedudukan, susunan

organisasi, tugas, fungsi dan tata kerja Dinas Perpustakaan dan Kearsipan Daerah Kabupaten Sambas.

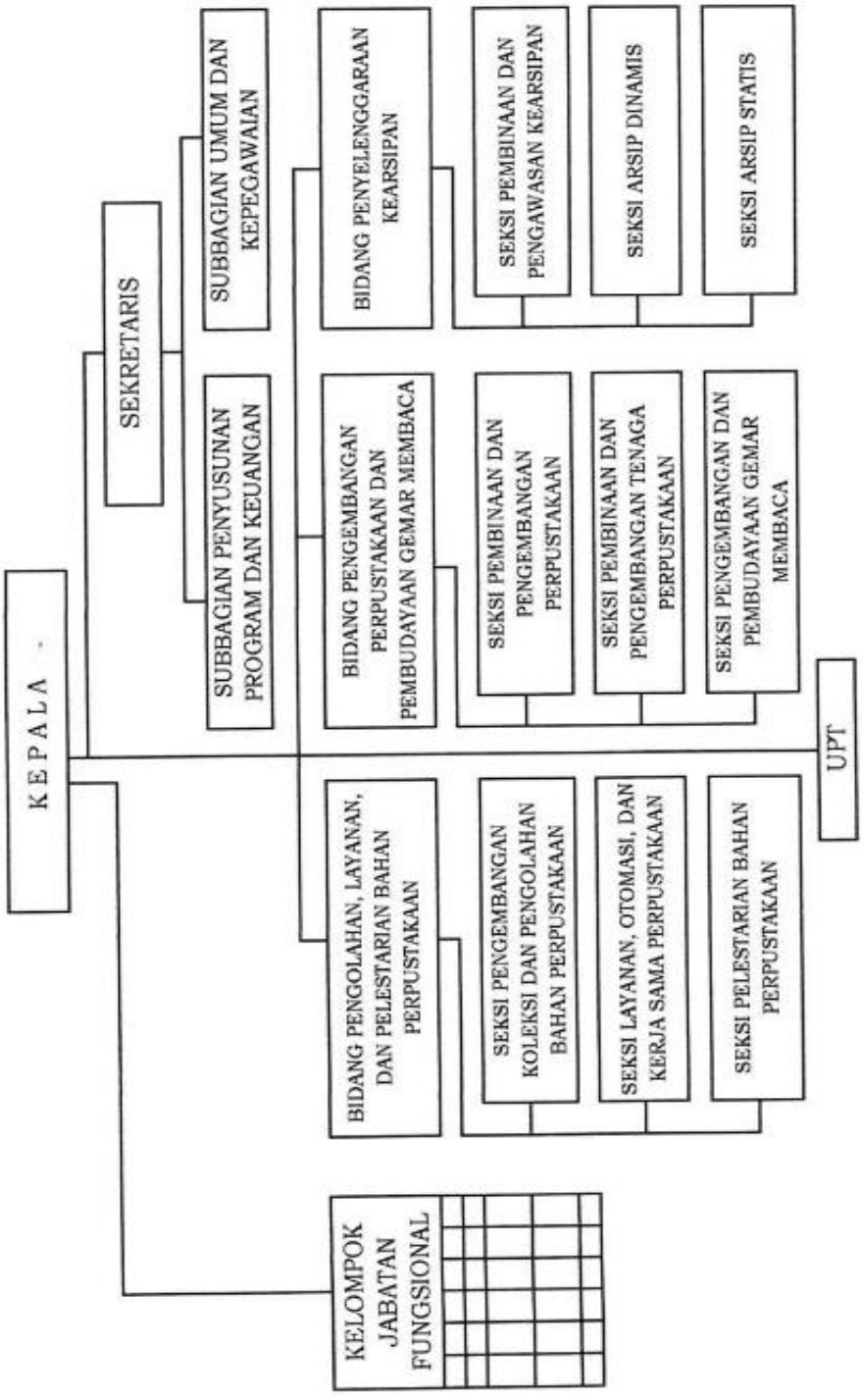
2.1.9.1 Visi dan Misi

Visi dari pada Dinas Perpustakaan dan Kearsipan Daerah Kabupaten Sambas yaitu "Terwujudnya Masyarakat Kabupaten Sambas yang Berakhlakul Karimah, Unggul dan Sejahtera". Dalam mendukung terwujudnya visi tersebut maka misi dari Dinas Perpustakaan dan Kearsipan Daerah Kabupaten Sambas

1. Meningkatkan kemampuan budi, daya dan karsa insani menuju pembangunan manusia seutuhnya
2. Meningkatkan upaya reformasi birokrasi dan tata kelola pemerintahan yang baik.

2.1.9.2 Struktur Organisasi

Dinas perpustakaan dan Kearsipan Daerah Kabupaten Sambas memiliki struktur organisasi. Terdapat Beberapa jabatan yang berada pada Dinas Perpustakaan dan Kearsipan Daerah Kabupaten Sambas yaitu sebagai berikut Kepala, Sekretaris, Kelompok jabatan fungsional, dan lain-lain yang secara lengkap dapat dilihat pada Gambar 2.2 Struktur Organisasi DPKD Kabupaten Sambas



Gambar 2. 2 Struktur Organisasi DPKD Kabupaten Sambas

2.2 Kajian Pustaka

Adapun Kajian Pustaka yang digunakan sebagai referensi atau memiliki kesamaan dengan penelitian ini dapat dilihat pada Tabel 2.2 berikut.

Tabel 2.2 Kajian Pustaka

No	Penelitian	Isi
1	Judul	Manajemen Risiko Sistem Informasi Rumah Sakit Menggunakan Framework NIST SP 800-30 (Studi Kasus: RSIA Eria Bunda Pekanbaru
	Nama Peneliti	Fuadi Khalish Muttaqi
	Tahun	2019
	Metode	NIST SP 800-30
	Hasil Penelitian	Melakukan identifikasi adanya kemungkinan risiko yang terjadi pada Sistem Informasi Rumah Sakit Dengan menerapkan metode NIST SP 800-30. Dengan melakukan identifikasi dan menilai risiko, dengan skala penelitian ini yaitu penilaian tingkat potensi risiko rendah, sedang, tinggi maka dengan adanya penilaian ini dapat memberikan pengetahuan dan rekomendasi kepada organisasi agar dapat membantu menurunkan risiko yang ada
	Persamaan Penelitian	- Mengidentifikasi dan menilai risiko keamanan pada sistem informasi dengan skala penilaian ancaman risiko dengan kategori Sangat tinggi, tinggi, sedang, rendah dan sangat rendah - Menggunakan metode yang sama yaitu NIST SP 800-30
	Perbedaan Penelitian	- Pada penelitian sebelumnya, dilakukan penelitian pada Sistem Informasi rumah sakit RSIA Eria Bunda Pekanbaru, sedangkan penelitian sekarang dilakukan pada *Integrated Library System* (INLISLITE) - Pada penelitian sebelumnya peneliti hanya melakukan penilaian risiko, sedangkan pada penelitian sekarang dilakukan penilaian risiko dan adanya rekomendasi kontrol keamanan dengan menerapkan Kontrol ISO 27001:2013 - Pada penelitian sebelumnya menggunakan pendekatan penelitian semi kuantitatif dan pada penentuan risiko tingkat dari impact yang dipetakan memilik 3 level risiko yaitu rendah, sedang dan tinggi sedangkan pada penelitian sekarang menggunakan pendekatan kualitatif dan memiliki tingkat level risiko yaitu sangat tinggi, tinggi, sedang, rendah, dan sangat rendah - Pada penelitian sebelumnya tidak terdapat hasil dari penentuan risiko apakah, risiko pada sistem tersebut dapat dikategorikan tinggi, sedang ataupun rendah sedangkan pada

		sekarang hasil berupa 3 risiko adversarial yang berada pada kategori Tinggi dan Sedang, 4 risiko accidental pada kategori Tinggi dan Sedang, 14 risiko structural pada kategori sangat tinggi, tinggi, sedang dan rendah, 3 risiko environmental pada kategori sedang dan rendah.
2	Judul	Analisis dan Penerapan Manajemen Risiko Aplikasi Pemantauan Serta Sistem Manajemen Keamanan Informasi SNI ISO 27001:2013
	Nama Peneliti	Topan Nurdiansyah M.Hendayun
	Tahun	2022
	Metode	ISO/IEC 27001:2013
	Hasil Penelitian	Melakukan identifikasi terhadap aset informasi, ancaman, kerentanan, risiko, dampak dan pemetaan klausul berdasarkan penilaian risiko. Lalu melakukan analisis maturity level, gap analisis, rekomendasi objektif kontrol dan keamanan informasi. Sehingga penelitian ini menghasilkan penilaian risiko, usulan pemetaan objektif kontrol dan kontrol berdasarkan SNI ISO/IEC 27001: 2013, Tingkat kematangan keamanan informasi pada aplikasi pemantauan terdapat tingkat tertinggi pada Klausul Manajemen aset dengan skor 3,25 pada level 3 dan nilai terendah pada Klausul Kesesuaian dengan skor 1,25 pada level 1. Hasil nilai rata-rata kontrol keamanan informasi pada aplikasi pemantauan sebesar 1,96. Dari, temuan dan rekomendasi.
	Persamaan Penelitian	- Menggunakan ISO 27001:2013 sebagai rekomendasi kontrol keamanan
	Perbedaan Penelitian	- Pada penelitian sebelumnya, dilakukan penelitian pada aplikasi pemantauan, sedangkan penelitian sekarang dilakukan pada *Integrated Library System* (INLISLITE) - Pada penelitian sebelumnya peneliti penilaian risiko menggunakan metode ISO/IEC 27001:2013 Sedangkan pada penelitian sekarang peneliti menggunakan NIST SP 800-30 sebagai metode penilaian risiko dan ISO/IEC 27001:2013 sebagai kontrol keamanan
3	Judul	Penggunaan Metode Octave-s dan ISO 27001:2013 Dalam Manajemen Risiko Keamanan Sistem Informasi Pada BKPSDM Kota Batu (Studi Kasus: Aplikasi E-Kinerja)
	Nama Peneliti	Dinda Riski Nurfadilah Widhy Hayuhardhika Nugraha Putra Aditya Rachmadi
	Tahun	2020
	Metode	OCTAVE-S dan ISO 27001:2013
	Hasil Penelitian	Dalam penelitian ini menggunakan metode OCTAVE-S mengidentifikasi ancaman risiko terkait TI dan melakukan penilaian, analisis, dan melaksanakan rencana strategis

		berdasarkan risiko tingkat keamanan yang dikombinasikan dengan ISO 27001:2013 untuk memberikan kontrol sehingga dapat menjadi pedoman BKPSDM agar dapat melakukan perbaikan terhadap sistem informasinya
	Persamaan Penelitian	- Melakukan penilaian risiko keamanan Sistem Informasi - Menggunakan Metode ISO 27001:2013 untuk memberikan rekomendasi kontrol terhadap keamanan ancaman yang ada
	Perbedaan Penelitian	- Pada penelitian sebelumnya menggunakan metode OCTAVE dalam melakukan penilaian risiko keamanan sistem informasi sedangkan pada penelitian ini menggunakan metode NIST SP 800-30 - Pada penelitian sebelumnya studi kasus penelitian dilakukan pada Sistem Informasi BKPSDM, Sedangkan pada penelitian sekarang dilakukan penelitian pada *Integrated Library System* (INLISLITE)
4	Judul	Penerapan Metode FMEA dan ISO 27001 Dalam Manajemen Risiko Keamanan Sistem Informasi pada Organisasi XYZ
	Nama Peneliti	Raden Budiarto
	Tahun	2017
	Metode	FMEA dan ISO 27001
	Hasil Penelitian	Pada penelitian ini menggunakan kerangka kerja FMEA untuk mengidentifikasi dan menilai Sistem Informasi pada organisasi xyz, serta juga menggunakan kerangka kerja ISO 27001 dengan memberikan daftar prioritas analisis risiko dan mengendalikan adanya risiko. yang berdampak positif dengan adanya penurunan tingkat kerawanan.
	Persamaan Penelitian	- Menggunakan Metode ISO 27001:2013 dalam pengendalian risiko
	Perbedaan Penelitian	- Pada penelitian sebelumnya menggunakan metode FMEA dalam melakukan penilaian risiko keamanan sistem informasi sedangkan pada penelitian ini menggunakan metode NIST SP 800-30 - Pada penelitian sebelumnya studi kasus penelitian dilakukan pada Sistem Informasi pada organisasi XYZ, Sedangkan pada penelitian sekarang dilakukan penelitian pada *Integrated Library System* (INLISLITE)