BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan perkembangan teknologi informasi (TI) yang sangat pesat, banyak hal yang menjadi lebih mudah dalam berbagai aspek aktivitas. Teknologi informasi banyak digunakan oleh organisasi atau lembaga untuk meningkatkan kemampuan dalam menyalurkan, mengelola, dan mendistribusikan informasi sehingga kebutuhan informasi dapat dicapai (Ratnawati, 2020). Informasi merupakan salah satu aset penting yang harus dilindungi oleh organisasi karena informasi merupakan kebutuhan utama dalam pelaksanaan semua kegiatan yang membantu perkembangan organisasi. Pengolahan data yang baik akan menghasilkan informasi yang berguna, oleh karena itu harus sebanding dengan proses pengelolaan data (Handayani, 2016). Seiring dengan laju perkembangan zaman, informasi menjadi kunci utama dalam proses bisnis sehingga pertukaran informasi sudah menjadi keharusan terutama bagi organisasi atau lembaga yang menggunakan *Komputer Based Information System* (CBIS) atau dikenal dengan Sistem Informasi berbasis Komputer (Mila Khoiroh, 2018).

Kebutuhan manusia semakin kompleks seiring dengan kemajuan teknologi informasi. Perusahaan atau organisasi yang menawarkan berbagai kemudahan dan keuntungan juga mengalami perkembangan tersebut. Teknologi informasi sangat penting untuk sistem informasi karena tidak hanya digunakan untuk membuat laporan keuangan, tetapi telah menjadi bagian integral dari semua bisnis Perusahaan atau organisasi. Perusahaan dapat menjamin aan dan keamanan data melalui penggunaan sistem informasi yang baik.

Optimized using
trial version
www.balesio.com

Hal ini secara tidak langsung dapat meningkatkan kinerja pegawai dan meningkatkan kinerja perusahaan atau organisasi secara keseluruhan (Novitasari dkk, 2023).

Dengan semakin besarnya peranan TI, sangat penting untuk memiliki informasi yang akurat dan tepat, maka investasi dibidang TI juga semakin meningkat. Selain memberikan keuntungan, penggunaan TI juga dapat menimbulkan risiko yang beragam seperti kehilangan data yang disebabkan oleh adanya virus, kerusakan diakibatkan oleh bencana alam maupun kesalahan yang disebabkan oleh penipuan ataupun alasan yang disengaja. Banyaknya aktivitas proses bisnis yang dilakukan, membuat TI sangat rentan terhadap keamanan informasi (Desy et al., 2014). Oleh karena itu, dalam menghadapi pertumbuhan suatu organisasi atau lembaga dibutuhkan kebijakan yang tepat untuk dapat melindungi aset informasi dan memperhatikan keamanan informasi yang dimiliki. Hal tersebut dilakukan agar investasi TI yang telah digunakan tidak menimbulkan ancaman yang dapat merugikan organisasi.

Keamanan informasi merupakan salah satu cara untuk mempertahankan informasi dari gangguan atau kerusakan (Miloslavskaya, 2014). Keamanan informasi akan mengacu pada proses dan metodologi yang dibentuk dan diterapkan dengan tujuan melindungi informasi atau data cetak dari gangguan yang dapat menimbulkan kerugian bagi organisasi. Keamanan informasi tidak bisa disandarkan hanya pada teknologi informasi, namun perlu adanya pengetahuan dan pemahaman mengenai permasalahan yang mungkin muncul apabila terjadi serangan. Pengelolaan keamanan informasi merupakan tanggung jawab

si untuk mengindari risiko yang merugikan. Oleh karena itu, organisasi enghindari kesalahan dalam pengelolaan keamanan informasi seperti

Optimized using
trial version
www.balesio.com

tidak membuat struktur tata kelola keamanan informasi yang tepat yang merupakan aspek penting bagi organisasi (Solms, 2004). Berdasarkan pada survey yang dilakukan terhadap 1.271 manajer sistem informasi di AS dalam majalah *Information Week*, hanya 22% responden yang mengatakan bahwa masalah keamanan sistem informasi sangat penting, dan kebanyakan dari mereka memprioritaskan strategi pemotongan biaya dan peningkatan persaingan meskipun faktanya memperbaiki sistem setelah adanya ancaman jauh lebih banyak. Meskipun masalah keamanan sering kali dilihat sebagai sesuatu yang tidak dapat diukur secara langsung dengan mata uang (*intangible),* namun masalah celah keamanan terhadap sistem informasi sebetulnya dapat diukur secara real (*tangible)* seperti kerugian yang ditimbulkan dari sebuah sistem apabila sistem tidak dapat dioperasikan selama beberapa jam (Budiarto, 2017).

Risiko adalah sesuatu yang menimbulkan ketidakpastian tentang apakah suatu kejadian akan terjadi pada saat tertentu dan apakah kejadian tersebut akan mengakibatkan kerugian yang tidak dapat memengaruhi operasi organisasi atau kerugian yang dapat memengaruhinya (Soputan, 2014). Kerugian yang ditimbulkan akibat adanya risiko adalah bentuk ketidakpastian yang seharusnya dipahami dan dikelola dengan baik agar tidak mengganggu tujuan organisasi. Pengelolaan risiko merupakan komponen tata kelola dan *strategy* yang dapat memberikan nilai, oleh karena itu perusahaan atau organisasi juga harus menerapkan manajemen risiko untuk mengatasi kerugian atau kerusakan yang mungkin muncul. Karena jenis risikonya belum diketahui secara pasti, risiko akan menjadi tantangan yang harus dihadapi di masa mendatang. Namun, dengan alikan risiko terhadap ketidakpastian, kita dapat mengurangi atau alkan dampak risiko yang terus-menerus. Oleh karena itu, manajemen

Optimized using
trial version
www.balesio.com

risiko harus diterapkan saat menjalankan proses bisnis, baik primer maupun sekunder (Kusumawati, 2016).

Penerapan manajemen risiko yang berhubungan dengan manajemen keamanan TI merupakan salah satu cara untuk melindungi keamanan informasi. Manajemen risiko merupakan proses mengidentifikasi risiko, menilai risiko, dan mengambil tindakan untuk mengurangi risiko sampai batas yang dapat diterima (Stoneburner, 2002). Manajemen risiko juga dikenal sebagai suatu kemampuan yang dimiliki oleh seorang manajer untuk menata kemungkinan variabilitas pendapatan dengan menekan sekecil mungkin tingkat kerugian yang diakibatkan oleh keputusan yang akan diambil (Wibowo et al., 2018). Manajemen risiko tidak terbatas pada TI, tetapi juga mencakup proses bisnis yang dapat membantu manajemen dalam memenuhi tugas untuk melindungi aset organisasi.

Diperlukan insentif bagi manajer sektor publik untuk merubah karena manajer cenderung menghindari risiko, yang mengakibatkan manajemen tidak efektif. Manajer yang mengetahui risiko akan menemukan ancaman dalam organisasi sejak awal dan mempertimbangkan konsekuensi dari ancaman tersebut bersama dengan tanggung jawab yang diberikan. Dalam organisasi di mana kesadaran akan risiko tinggi, manajemen risiko telah menjadi sangat kuat sehingga hampir tidak terlihat karena semua karyawan secara implisit mengelola risiko tersebut (Damayanti et al., 2023).

Manajemen risiko merupakan suatu proses untuk mengantisipasi terhadap risiko yang mungkin muncul agar tidak menimbulkan kerugian untuk organisasi (Pratiwi dan Kurniawan, 2018). Menurut Budiarto (2017) manajemen risiko adalah

an ilmiah untuk menangani semua jenis risiko dengan mengantisipasi ngambil tindakan untuk meminimalkan kerugian. Manajemen risiko

Optimized using
trial version
www.balesio.com

merupakan serangkaian metodologi dan prosedur yang digunakan untuk mengelola ancaman/risiko dengan cara mengidentifikasi risiko, menilai risiko, dan mengambil langkah-langkah untuk mengurangi risiko ke tingkat yang dapat diterima. Manajemen risiko yang baik adalah yang memiliki fokus pada identifikasi dan cara mengatasi risiko yang berfungsi untuk meningkatkan kemungkinan sukses, dan mengurangi kemungkinan kegagalan. Menurut Marginingsih (2017) manajemen risiko merupakan bagian penting dari strategi yang harus dilakukan agar organisasi mampu melindungi aset dan mampu mencapai keberhasilan tujuan baik jangka pendek maupun jangka panjang serta bisa mempersiapkan organisasi untuk menghadapi kondisi tertentu yang dapat menyebabkan kerugian.

BKAD (Badan Keuangan dan Aset Daerah) Kabupaten Maros merupakan salah satu OPD yang sudah lama terbentuk yang sebelumnya bernama Badan Pengelolaan Keuangan dan Pendapatan Daerah (BPKPD) sesuai dengan Peraturan Daerah (PERDA) Kabupaten Maros No. 3 Tahun 2019 tentang Perubahan Atas Peraturan Daerah (PERDA) Kabupaten Maros No. 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah melakukan penyusunan kedudukan, sturktur organisasi, tugas, tanggung jawab, dan tata kerja dari perangkat daerah. BKAD merupakan unsur pelaksana fungsi penunjang urusan pemerintahan yang menjadi kewenangan daerah di bidang keuangan daerah sesuai dengan Peraturan Bupati No. 7 Tahun 2016 tentang Pembentukan dan Susunan dari Perangkat Daerah menyusun kedudukan, susunan organisasi, tugas, fungsi dan tata kerja dari perangkat daerah Kabupaten Maros (Maros, 2022). Pengelolaan keuangan daerah adalah salah satu tanggung jawab BKAD

en Maros, yang mencakup kewenangan pengawasan pengelolaan

n daerah, asas-asas umum dan susunan Anggaran Pendapatan dan

Belanja Daerah (APBD), penyusunan Rancangan Anggaran Pendapatan dan Belanja Daerah (RAPBD), penetapan Anggaran Pendapatan dan Belanja Daerah (APBD), pelaksanaan Anggaran Pendapatan dan Belanja Daerah (APBD), perubahan Anggaran Pendapatan dan Belanja Daerah (APBD), pengelolaan kas, penatausahaan keuangan, akuntansi keuangan, dan pertanggungjawaban Anggaran Pendapatan dan Belanja Daerah. Termasuk pula pengawasan dan pembinaan.

Berdasarkan Permendagri Nomor 70 Tahun 2019, Sistem Informasi Pemerintahan Daerah (SIPD) adalah sistem informasi yang saling terhubung yang mengelola Informasi Pembangunan Daerah, Informasi Keuangan Daerah, dan Informasi Pemerintahan Daerah lainnya. Sistem ini digunakan selama operasi pembangunan daerah. SIPD ini dirancang untuk membuat layanan informasi Pemerintahan Daerah yang terhubung dan terintegrasi secara elektronik, seperti yang disebutkan dalam Pasal 4 ayat (2).

Badan Keuangan dan Aset Daerah mulai menerapkan Sistem Informasi Pemerintahan Daerah (SIPD RI) pada tahun 2024. Dalam penerapan SIPD RI tentu saja mempunyai beberapa permasalahan dan hambatan yang dapat mengganggu proses penerapan pada BKAD seperti kehilangan data, penyalahgunaan hak akses, kerusakan akibat bencana alam, jaringan terputus akibat pemadaman listrik dan lain sebagainya. Hal ini tentunya dapat menyebabkan rusaknya aset penting yang dimiliki dan menjadi masalah bagi BKAD. Adanya kemungkinan munculnya permasalahan tersebut menjadi dasar pentingnya melakukan analisis risiko terkait penerapan teknologi informasi di atau organisasi lain. Dengan mengetahui risiko potensial yang terjadi embantu BKAD untuk membuat dan menentukan langkah-langkah yang

Optimized using
trial version
www.balesio.com

tepat untuk menangani setiap risiko yang muncul sehingga BKAD mampu menghindari dan meminimalisir dampak yang merugikan (Permatasari, 2024).

Untuk mengetahui dan mengidentifikasi risiko yang mungkin terjadi pada keamanan teknologi informasi pada sebuah organisasi, diperlukan adanya prosedur evaluasi yang memungkinkan munculnya potensi *risk* serta menghambat proses organisasi yang berjalan sehingga menimbulkan kerugian bagi organisasi. Untuk melakukan analisis *risk management* untuk masalah yang terdapat pada BKAD, maka peneliti akan gunakan standar IEC/ISO 31010:2019 yang bertujuan memberikan control pada setiap risiko.

Standar IEC/ISO 31010:2019 adalah standar *risk management* yang ditetapkan oleh Organisasi Internasional untuk Standardisasi (ISO) dan Komisi Elektroteknik Internasional (IEC). Standar ini memberikan panduan untuk memilih dan menerapkan teknik penilaian risiko dalam berbagai situasi. Standar IEC/ISO 31010:2019 memiliki beberapa manfaat, di antaranya: membantu pengambilan keputusan dalam kondisi ketidakpastian, memberikan informasi tentang risiko tertentu, sebagai bagian dari proses manajemen risiko, menggambarkan manfaat dan kekurangan metode pengelolaan risiko, serta memudahkan pengambilan keputusan manajemen. Standar IEC/ISO 31010:2019 merupakan standar yang digunakan guna melakukan tindakan pengelolaan *risk management*. Pada penelitian ini, tahapan awal manajemen risiko adalah konsultasi dan komunikasi dengan cara wawancara dengan tujuan memperoleh informasi dan menciptakan *planning* yang sesuai dengan target.

Penelitian yang dilakukan oleh Malau dkk (2023) bertujuan untuk ıtifikasi risiko, menganalisis manajemen keamanan sistem informasi, dan ‹an kemungkinan risiko pada SIKS-NG (Sistem Informasi Kesejahteraan

Optimized using
trial version
www.balesio.com

Sosial - Next Generation) di Kota Batam menggunakan IEC/ISO 31010:2019. Hasilnya menunjukkan bahwa pada saat Dinas Sosial di Kota Batam menerapkan SIKS-NG (Sistem Informasi Kesejahteraan Sosial - Next Generation) terhadap pemrosesan rencana BANSOS, ada enam belas potensi bahaya yang muncul. Dari enam belas kemungkinan *risk* tersebut, terdiri dari 3 risiko tinggi, 8 risiko medium, dan 5 risiko rendah. Penelitian tersebut menunjukkan bahwa Standar IEC/ISO 31010: 2019 berfungsi dengan baik sebagai *framework risk management* untuk sistem aplikasi yang digunakan di lembaga pemerintah. Selain itu, penelitian ini memberikan rekomendasi tentang cara memperbaiki risiko yang terdapat pada aplikasi SIKS-NG dan bagaimana mendokumentasi *risk management*. Saran-saran ini akan mempermudah Dinas Sosial di Kota Batam dalam pengelolaan *risk* yang kemungkinan akan terjadi pada sistem tersebut, terutama selama proses perencanaan BANSOS.

Penelitian yang dilakukan oleh Maria dkk (2023) pada Dinas Kependudukan dan Pencatatan Sipil di Kabupaten Semarang, dalam aktivitas manajemen analisis risiko untuk aplikasi SMARD dilakukan sesuai dengan standar IEC/ISO 31010:2019. Petugas operator Desa dan Kelurahan menggunakan Sistem Informasi Administrasi Kependudukan Desa dan Kelurahan (SMARD) untuk menyimpan laporan administratif terkait layanan. Ini termasuk pembuatan akta kematian, akta kelahiran, dan kartu keluarga, kemudian diproses melalui petugas GISA Disdukcapil. Jika data pendukung memenuhi syarat ketentuan, pelaporan akan diverifikasi. Menurut IEC/ISO 31010:2019, aktivitas *risk management* mencakup langkah-langkah *communication and consultation, setting, identification, analysis, evaluation*, dan *risk treatment*. Standar digunakan sebab telah terbukti berhasil dalam proses *risk management*

Optimized using
trial version
www.balesio.com

yang berkaitan dengan teknologi informasi dan sistem informasi di lembaga pemerintah. Penelitian tersebut menunjukkan bahwa terdapat dua puluh kemungkinan risiko terkait dengan penerapan Sistem Informasi Administrasi Kependudukan Desa dan Kelurahan (SMARD) Disdukcapil; diantaranya empat kemungkinan *risk* pada tingkat tinggi, delapan kemungkinan *risk* pada tingkat sedang, dan delapan kemungkinan *risk* pada tingkat rendah. Hasil penelitian tersebut menunjukkan bahwa Standar IEC/ISO 31010: 2019 dapat diimplementasikan dengan baik dalam manajemen *risk analysis* sistem informasi di lembaga pemerintah. Hasil dari penelitian tersebut didokumentasikan, dan rekomendasi untuk *risk treatment* yang mungkin muncul ketika SMARD diterapkan pada layanan publik di tempat tersebut.

Penelitian yang dilakukan oleh Maulana dkk (2024) bertujuan untuk menemukan risiko dan langkah-langkah untuk mengendalikannya pada Biro Administrasi Akademik dan Kemahasiswaan Universitas Muhammadiyah di Kabupaten Sorong. Penelitian ini lebih menekankan proses penilaian risiko dengan menggunakan ISO 31010:2019. Ada 17 risiko yang telah diidentifikasi selama proses identifikasi risiko hingga evaluasi risiko. Dari tujuh belas risiko tersebut, dua termasuk risiko tinggi dengan nilai level risiko dua puluh lima pada risiko A1 dan dua puluh pada risiko A5. Lebih jauh lagi, *risk* A3, A7, A11, dan A9 mempunyai peringkat tingkat risiko empat, yang menjadikannya risiko sedang. Untuk mengevaluasi *risk* terhadap dua risiko tertinggi tersebut, kode risiko A1 dikurangi dengan membeli CCTV dan memasangkannya di ruang BAAK. Dengan mengganti jenis kertas pada cetakan ijazah dan mengganti printer dengan printer uai dan memenuhi persyaratan pencetakan ijazah, maka kode *risk* A5 kurang.

Optimized using
trial version
www.balesio.com

Berdasarkan latar belakang yang telah disebutkan, untuk mengidentifikasi risiko yang mungkin terjadi pada penerapan SIPD RI (Sistem Informasi Pemerintahan Daerah), maka penulis tertarik untuk melakukan penelitian dengan judul "Analisis *Risk Management* dalam Penerapan Sistem Informasi Pemerintahan Daerah (SIPD RI) di Kabupaten Maros Menggunakan IEC/ISO 31010:2019 (Studi Kasus pada Badan Keuangan dan Aset Daerah Kabupaten Maros)".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka permasalahan dari penelitian ini adalah bagaimana melakukan Analisis Risk Management dalam penerapan Sistem Informasi Pemerintahan Daerah (SIPD RI) di Badan Keuangan dan Aset Daerah Kabupaten Maros menggunakan IEC/ISO 31010:2019?

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengetahui Analisis Risk Management dalam penerapan Sistem Informasi Pemerintahan Daerah (SIPD RI) di Badan Keuangan dan Aset Daerah Kabupaten Maros menggunakan IEC/ISO 31010:2019.

1.4 Kegunaan Penelitian

Kegunaan dalam penelitian ini antara lain sebagai berikut.

1.4.1 Kegunaan Teoretis

Dalam penelitian ini diharapkan mampu memberikan suatu informasi yang mendalam terkait Risk Management dalam penerapan Sistem Informasi Pemerintahan Daerah (SIPD RI), khususnya pada sektor pemerintahan, serta ‹an pemahaman terkait perlakuan risiko menggunakan sistem informasi

Optimized using
trial version
www.balesio.com

tersebut. Selain itu, penelitian ini juga diharapkan dapat dijadikan pedoman bagi penelitian selanjutnya.

1.4.2 Kegunaan Praktis

Dalam penelitian ini diharapkan dapat memberikan panduan praktis bagi para pengguna Sistem Informasi Pemerintahan Daerah (SIPD RI), terkhusus pada sektor pemerintahan, tentang bagaimana *Risk Management* dalam penerapannya.

1.5 Ruang Lingkup

Lingkup penelitian terkait dengan *Risk Management* dalam penerapan SIPD RI (Sistem Informasi Pemerintahan Daerah) di Kabupaten Maros. Objek penelitian terbatas hanya pada pegawai atau staff yang terlibat dalam penggunaan Sistem Informasi tersebut.

1.6 Sistematika Penulisan

Sistematika penulisan penelitian ini terdiri dari lima (5) bab, yang disebutkan di bawah ini.

Bab I Pendahuluan. Bab ini membahas latar belakang penelitian dan rumusan masalah penelitian, tujuan dari suatu penelitian, kegunaan teoritis dan praktis penelitian, ruang lingkup dari penelitian, dan metode penulisan.

Bab II Tinjauan Pustaka. Bab ini membahas landasan teori yang digunakan oleh peneliti agar penelitian dapat dilakukan terarah pada fokus penelitian.

Bab III Metode Penelitian. Bab ini membahas terkait dengan penjelasan yang mendetail mengenai prosedur maupun analisis yang dipergunakan dalam penelitian nantinya.

Optimized using
trial version
www.balesio.com

Bab IV Hasil Penelitian. Bab ini berisi data yang diperoleh dan hasil penelitian yang dilakukan menggunakan metode yang dibahas pada Bab III sebelumnya.

Bab V Penutup. Bab ini berisi hasil penelitian, kendala penelitian, dan saran untuk penelitian selanjutnya.

Optimized using
trial version
www.balesio.com

BAB II

TINJAUAN PUSTAKA

2.1 Standar IEC/ISO 31010:2019 – Teknik Penilaian Risiko

Risiko merupakan sesuatu hal yang menghalangi organisasi atau perusahaan dalam mencapai tujuannya. Hal ini tergantung pada jenis risiko yang muncul dalam situasi tertentu, faktor yang menjadi hambatan dapat berupa faktor yang berasal dari dalam ataupun dari luar. Ketika ada *risk*, fokus manajemen akan terganggu untuk mencapai tujuan organisasi. Oleh karena itu, tindakan manajemen risiko harus dilakukan sehingga manajemen tidak tersesat ketika risiko timbul dalam organisasi yang mereka kelola. Manajemen risiko bertujuan untuk mengurangi dampak risiko pada lingkungan, manusia, teknologi, dan organisasi. Tahap penilaian risiko adalah langkah penting dalam proses *risk management*, yang mencakup *identification, analysis, evaluation,* dan *risk treatment*. Dalam penelitian ini, aktivitas manajemen risiko dilakukan sesuai dengan standar dari IEC/ISO 31010:2019 *Risk Management* sebagai Teknik Penilaian Risiko. Standar ini mendukung ISO 31000 dan menjelaskan bagaimana menggunakan teknik penilaian risiko berdasarkan prinsip *risk management*. Standar IEC/ISO 31010:2019 merupakan pengembangan paling baru dari Standar IEC/ISO 31010 tahun 2009. Selain berfungsi untuk standar tambahan untuk ISO 310000, standar tersebut terdapat juga kelebihan, yakni menawarkan teknik maupun penjelasan untuk menilai *risk* yang terinci serta menyeluruh jika dibandingkan dengan versi

Optimized using
trial version
www.balesio.com

ıya. Tak hanya itu, standar ini dapat membantu manajemen memahami dan kekurangan dari berbagai metode pengelolaan risiko, sehingga ɛbih mudah membuat keputusan.

2.1.1 Komunikasi dan Konsultasi

Komunikasi dan konsultasi adalah langkah pertama dalam proses *risk management*. Komunikasi dan konsultasi dilakukan guna menentukan konteks yang akurat. Pada tahap tersebut, peserta yang diwawancarai termasuk Kepala Badan sebagai administrator SKPD (Satuan Kerja Perangkat Daerah) dan beberapa staf dari Badan Keuangan dan Aset Daerah. Tujuan dari wawancara ini adalah untuk memastikan bahwa proses manajemen risiko untuk aplikasi SIPD diakui dan didukung.

2.1.2 Penetapan Konteks

Sebelum memulai pengelolaan risiko, penting untuk menentukan suatu konteks. Hal ini merupakan prosedur yang digunakan untuk menetapkan standar berdasarkan keadaan internal dan eksternal dari suatu organisasi. Analisis risiko dalam penerapan Sistem Informasi Pemerintahan Daerah termasuk dalam ruang lingkup penelitian ini. Kriteria *likelihood* dan *impact* penggunaan SIPD perlu dilakukan sebelum memulai kegiatan pengelolaan risiko. Kriteria *likelihood* berguna untuk mengukur tingkat risiko yang sering muncul dalam SIPD. Sedangkan kriteria *impact* menunjukkan bagaimana penerapan SIPD berdampak pada risiko yang ada pada kegiatan dalam SIPD. Kerugian yang terjadi akibat risiko tersebut dikategorikan menjadi 3 tingkat kategori, yakni risiko rendah (*low risk*), risiko sedang (*moderate risk*), dan risiko tinggi (*high risk*). Kerugian berkisar antara 0 sampai dengan 1.000.000.000.

2.1.3 Analisis Risiko

nalisis risiko yang berkaitan dengan penerapan Sistem Informasi ahan Daerah (SIPD) akan dilakukan di tahap ini. Berdasarkan Standar 31010:2019, analisis risiko merupakan salah satu tahap penilaian risiko

Optimized using
trial version
www.balesio.com

(*risk assessment*) yang akan digunakan dalam tahapan ini. Tahap identifikasi risiko, kemudian analisis risiko, lalu evaluasi risiko, dan tahap perlakuan risiko (*risk treatment*) adalah tiga tahap tindakan yang dilakukan dalam penilaian risiko.

2.1.4 Perlakuan Risiko (*Risk Treatment*)

Pada tahapan ini, saran atau rekomendasi diberikan terkait cara menangani risiko yang mungkin muncul selama implementasi SIPD. Diharapkan bahwa *risk treatment* yang disarankan akan meminimalisir dampak dan kemungkinan *risk* yang berpotensi terjadi. Perilaku risiko dapat berarti mencegah, memindahkan risiko ke pihak ketiga, maupun menerima risiko sebab dampak negatifnya tidak signifikan untuk organisasi. Rekomendasi perlakuan risiko akan disusun didasarkan pada tingkat risiko dari paling tinggi ke paling rendah.

2.2 Konsep Dasar Sistem Informasi

2.2.1 Pengertian Sistem

Sistem adalah suatu susunan komponen yang saling terhubung atau terpadu yang digunakan untuk mencapai suatu tujuan tertentu (Kadir, 2014). Sistem adalah suatu kelompok atau kumpulan variabel, faktor, atau komponen yang saling berhubungan, saling bergantung, terorganisasi, dan berinteraksi satu sama lain (Sutabri, 2012).

Sistem adalah susunan komponen-komponen yang saling terkait yang bekerja bersama sebagai satu kesatuan untuk mencapai suatu tujuan yang utama (Sutarman, 2012). Sistem adalah suatu tatanan (integrasi) yang terdiri dari beberapa komponen fungsional (dengan unit-unit fungsional dan tugas yang unik)

ng terhubung dan bekerja bersama untuk menyelesaikan suatu proses

Fatansyah, 2015).

Optimized using
trial version
www.balesio.com

Penulis dapat membuat kesimpulan dari berbagai definisi di atas bahwa sistem terdiri dari kumpulan elemen, kumpulan variabel yang terorganisasi, dan komponen fungsional yang berinteraksi satu sama lain untuk memenuhi tujuan yang akan dicapai.

2.2.2 Pengertian Informasi

Informasi ialah sekumpulan data yang telah diproses dan diolah untuk menghasilkan pengetahuan yang akan lebih bermanfaat dalam menyelesaikan suatu tugas. Jika data menawarkan lebih banyak manfaat daripada sekadar melihatnya, maka data tersebut dianggap bermanfaat (Ferdian, 2017).

Terdapat beberap definisi dari informasi, yakni: Dalam karyanya, "Analisis dan Desain Sistem Informasi Pendekatan Terstruktur", H. M. Yogianto menyatakan definisi informasi yakni: “Informasi adalah data yang telah diubah ke dalam format yang menyampaikan makna kepada penerima dan memiliki nilai nyata dan praktis untuk pilihan saat ini atau masa mendatang.” Dalam bukunya yang berjudul Kerangka Dasar Sistem Informasi Manajemen, Gordon B. Davis menyatakan definisi informasi yakni: “Informasi adalah data yang telah diubah menjadi format konkret dan berguna atau menjadi wawasan yang dapat dipahami untuk pengambilan keputusan saat ini atau di masa mendatang.”

2.2.3 Pengertian Sistem Informasi

Sistem informasi merupakan sistem buatan yang terdiri dari kumpulan komponen terintegrasi berbasis komputer dan manual yang dirancang untuk mendukung pengambilan keputusan manajemen dan menyederhanakan operasi

si dengan memberi manajer akses ke informasi yang dapat mereka untuk merencanakan dan mengawasi kegiatan organisasi. Karena sistem

Optimized using
trial version
www.balesio.com

informasi dapat mendukung rencana strategis perusahaan dan memberikan informasi penting kepada manajemen, fungsinya sangat krusial bagi keberhasilan organisasi (Stahl, 2018). Sistem informasi sebagian besar digunakan untuk mengubah data menjadi informasi yang dapat digunakan untuk membuat keputusan.

Dalam perkembangan suatu organisasi, sistem informasi sangatlah penting. Selain itu, sistem informasi yang baik diperlukan karena perubahan dalam bisnis, teknologi, kebijakan pemerintah, prosedur, dan kebutuhan informasi yang meningkat.

2.3 Sistem Informasi Pemerintahan Daerah (SIPD RI)

Berdasarkan Permendagri Nomor 70 Tahun 2019, Sistem Informasi Pemerintahan Daerah (SIPD) adalah sistem informasi yang saling terhubung yang mengelola Informasi Pembangunan Daerah, Informasi Keuangan Daerah, dan Informasi Pemerintahan Daerah lainnya. Sistem ini digunakan selama operasi pembangunan daerah. SIPD dirancang sebagai layanan informasi dalam Pemerintahan Daerah yang terhubung serta terintegrasi secara elektronik, seperti yang disebutkan dalam Pasal 4 ayat (2). Adapun ruang lingkup SIPD menurut Permendagri Nomor 70 Tahun 2019 antara lain:

1. Informasi Pembangunan Daerah

   Informasi Pembangunan Daerah memungkinkan analisis dan profil pembangunan daerah serta data dan informasi perencanaan pembangunan daerah. Informasi Pembangunan Daerah diselenggarakan an dikelola oleh BAPPEDA (Badan Perencanaan Pembangunan,

Optimized using
trial version
www.balesio.com

Penelitian dan Pengembangan Daerah). Informasi Pembangunan Daerah memuat tentang:

a. Data Perencanaan Pembangunan Daerah;
b. Analisis dan Profil Pembangunan Daerah; dan
c. Informasi Perencanaan Pembangunan Daerah.

Informasi Pembangunan Daerah mampu memfasilitasi penyusunan dokumen perencanaan pembangunan daerah dan dokumen perangkat daerah yang mencakup:

a. Rencana Pembangunan Jangka Panjang Daerah (RPJPD);
b. Rencana Pembangunan Jangka Menengah Daerah (RPJMD);
c. Rencana Kerja Pemerintah Daerah (RKPD);
d. Rencana Strategis Perangkat Daerah (RENSTRA PD); dan
e. Rencana Kerja Perangkat Daerah (RENJA PD).

Adanya dokumen-dokumen yang disebutkan diatas membuat analisis dan profil pelaksanaan pembangunan daerah dapat diakses dengan mudah, serta bisa dipergunakan sebagai referensi ketika dokumen anggaran daerah dibuat seperti Kebijakan Umum APBD (KUA), Prioritas dan Plafon Anggaran Sementara (PPAS) dan rancangan APBD sampai menjadi APBD. Selain itu, juga terdapat Informasi Perencanaan Pembangunan Daerah yang dapat meliputi:

a. Demografi;
b. Kondisi geografis daerah;
c. Ekonomi & keuangan daerah

Potensi sumber daya daerah;

Aspek pelayanan umum;

Optimized using
trial version
www.balesio.com

f. Aspek daya saing daerah; dan

g. Aspek kesejahteraan masyarakat.

2. Informasi Keuangan Daerah

Sistem Informasi Keuangan Daerah memungkinkan pengelolaan data dan informasi, serta penyusunan, pemantauan, maupun evaluasi dokumen pengelolaan keuangan daerah yang dilakukan secara elektronik dengan lebih produktif dan efisien sambil mempertahankan prinsip transparansi dan akuntabilitas. Informasi Keuangan Daerah dikelola oleh BPKAD (Badan Pengelolaan Keuangan dan Aset Daerah). Proses pengelolaan keuangan daerah yang dimaksud meliputi:

a. Perencanaan Anggaran Daerah;

b. Pelaksanaan & Penatausahaan Keuangan Daerah;

c. Akuntansi & Pelaporan Keuangan Daerah;

d. Pertanggung Jawaban Pelaksanaan Keuangan Daerah;

e. Pertanggung Jawaban Barang Milik Daerah; dan

f. Informasi Keuangan Daerah lainnya.

3. Informasi Pemerintahan Daerah Lainnya

Informasi Pemerintahan Daerah Lainnya memungkinkan untuk mengelola data dan informasi umum lainnya tentang penyelenggaraan pemerintahan. Data umum tersebut dapat disajikan dalam bentuk PERDA (Peraturan Daerah), EPPD (Evaluasi Penyelenggaraan Pemerintahan Daerah), atau Laporan Penyelenggaraan Pemerintahan Daerah (LPPD) satu tahun. Perangkat daerah mengelola informasi pemerintahan daerah innya berdasarkan peran atau bidang tanggung jawabnya masing-asing.

Optimized using
trial version
www.balesio.com

Sistem Informasi Pemerintah Daerah (SIPD) dibuat untuk memenuhi UU No. 23 Tahun 2014 tentang pemerintahan daerah dan PP No. 12 Tahun 2019 tentang pengelolaan keuangan daerah, yang diperkuat oleh Permendagri No. 70 Tahun 2019 tentang Sistem Informasi Pemerintah Daerah. Sasaran dari SIPD adalah bertujuan mengubah pelaksanaan pemerintahan menjadi lebih kreatif, fleksibel, responsif, dan akuntabel. Aplikasi SIPD membantu proses perencanaan dan pelaksanaan pemerintahan daerah menjadi lebih efisien, mendorong kerja sama dan keterlibatan semua pihak dalam proses perencanaan, sistem yang terintegrasi memudahkan penyediaan informasi kepada masyarakat dan pimpinan, dan diharapkan dapat terintegrasi dengan sistem pengadaan barang dan jasa LKPP (Lembaga Kebijakan Pengadaan Barang Jasa Pemerintah).

2.4 Risiko

2.4.1 Definisi Risiko

Risiko merupakan dampak negatif bersih dari penerapan kerentanan dengan mempertimbangkan probabilitas dan dampak yang dihasilkan (Stoneburner et al., 2002). Dalam penelitian yang dilakukan oleh Soputan dkk (2014), risiko adalah sesuatu yang menyebabkan suatu kejadian tertutup selama waktu tertentu, yang dapat menyebabkan kerugian, baik yang tidak signifikan maupun yang dapat mempengaruhi proses dalam suatu perusahaan atau organisasi. Pada umumnya, risiko sebagai dampak negatif seperti kehilangan, [illegible]an lain sebagainya. Kerugian yang timbul akibat risiko merupakan bentuk [illegible]astian yang seharusnya dipahami dan dikelola secara efektif oleh

Optimized using
trial version
www.balesio.com

organisasi yang merupakan bagian dari strategi sehingga hal tersebut dapat menjadi nilai tambah dan mendukung pencapaian misi suatu organisasi.

2.4.2 Konsep Risiko

Risiko adalah situasi atau peristiwa yang tidak pasti yang dapat berdampak positif atau negatif apabila terjadi. Risiko muncul secara bertahap dan dapat mempengaruhi tujuan suatu organisasi. Konsep risiko dapat menentukan tingkat risiko/*level of risk* (Leonard et al., 2020). Tingkat risiko dapat dikategorikan dengan cara berikut berdasarkan faktor yang digunakan: *impact* dan *probability*.

1. *Low Risk* (*Low Probability Low Impact*), maksudnya adalah bila dibandingkan dengan risiko lain yang teridentifikasi, risiko ini mempunyai pengaruh paling kecil, sehingga dapat diabaikan karena tidak mempunyai kaitan dengan tujuan.
2. *Moderate Risk* (*Low Probability High Impact*), maksudnya adalah risiko yang memiliki tingkat pengaruh sedang dan hanya memerlukan pemantauan alih-alih diabaikan.
3. *Moderate Risk* (*High Probability Low Impact*), maksudnya adalah risiko yang memiliki tingkat pengaruh sedang, di mana risiko tersebut tidak bisa diabaikan, tetapi perlu dilakukan monitoring.
4. *High Risk* (*High Probability High Impact*), maksudnya adalah risiko yang memiliki tingkat pengaruh terbesar di antara risiko lainnya. Risiko ini memiliki dampak signifikan terhadap suatu tujuan dan berbahaya jika diabaikan; oleh karena itu, risiko ini perlu ditangani segera untuk mencegah kerugian dan kerusakan.

Optimized using
trial version
www.balesio.com

2.4.3 Klasifikasi Risiko

Risiko dapat klasifikasikan dengan beberapa cara yang berbeda. Berikut ini adalah gambaran berbagai pendekatan untuk mengklasifikasikan risiko (Frame, 2003).

1. Pure (or Insurable) Risk

   Pure risk atau risiko murni merupakan risiko mengenai kemungkinan terjadinya kerusakan maupun bentuk kerugian. Pendekatan ini terfokus secara eksklusif terhadap munculnya kejadian terburuk. Risiko murni biasanya disebut dengan risiko yang dapat diasuransikan karena pendekatan ini bertujuan untuk melindungi dari konsekuensi kerusakan dan kerugian.

2. Business Risk

   Dalam *business risk*, terdapat peluang keuntungan dan kerugian maksudnya ketika ada peluang untuk mendapatkan sebuah keuntungan, harus diimbangi dengan kemungkinan munculnya kerugian, hal tersebut menjadi energi bagi pelaku bisnis. Ciri utama pelaku bisnis adalah pengambil risiko. Mereka menyadari bahwa tidak ada sesuatu yang besar terjadi apabila bersikap hati-hati, yaitu dengan menghindari risiko karena semakin besar risiko yang diambil maka semakin besar prospek untung dan rugi.

3. Project Risk

   Suatu proyek tidak lepas dari adanya risiko. Risiko yang terjadi pada proyek berkaitan erat dengan estimasi, baik estimasi mengenai waktu maupun biaya. Proyek akan menghadapi masalah yang signifikan jika

Optimized using
trial version
www.balesio.com

tugas tidak dinilai secara akurat, estimasi biaya tidak akurat, atau kebutuhan sumber daya tidak ditentukan dengan tepat.

4. Operational Risk

   Risiko operasional berhubungan dengan pelaksanaan seperti mengelola kantor, mengoperasikan fasilitas komputer dan lain sebagainya. Risiko akan muncul ketika operasional melakukan kelalaian yang dapat merusak reputasi dan menyebabkan kerugian bisnis. Oleh karena itu, risiko operasional dianggap sebagai risiko yang muncul akibat kegagalan manusia, proses, bahkan teknologi. Risiko operasional sulit diantisipasi karena ketidakpastiannya.

5. Technical Risk

   Saat pertama menerapkan manajemen risiko, biasanya organisasi berfokus pada risiko mengenai anggaran, jadwal, atau target organisasi. Hal tersebut merupakan situasi yang sering terjadi apabila organisasi menerapkan teknologi tinggi, padahal tidak menutup kemungkinan bahwa terjadinya gangguan teknis yang tidak terlihat. Oleh karena itu, risiko teknis seharusnya juga dipertimbangkan terutama bagi organisasi yang menerapkan teknologi canggih.

6. Political Risk

   Risiko politik mengacu pada situasi saat pengambilan keputusan. Dalam suatu organisasi, risiko politik mengacu pada masalah yang dapat dipicu oleh politik kantor, contohnya sebelum melakukan investasi pembuatan kantor, pengusaha harus menyesuaikan antara investasi tersebut dengan kebijakan yang ada di pemerintahan setempat.

Optimized using
trial version
www.balesio.com

2.4.4 Jenis-jenis Risiko

Secara umum risiko dapat dihadapi oleh seseorang atau organisasi di mana terdapat kemungkinan yang dapat merugikan. Menurut (Suganda, 2015) terdapat beberapa jenis risiko yang mungkin terjadi sebagai berikut.

1. Risiko Murni, didefinisikan sebagai risiko yang muncul tanpa unsur kesengajaan dan berpotensi menimbulkan kerugian jika terjadi. Misalnya, bahaya yang ditimbulkan oleh pencurian, penggelapan, kebakaran, dan sebagainya.
2. Risiko Spekulatif, didefinisikan sebagai risiko yang sengaja diciptakan oleh individu yang bersangkutan dengan tujuan menciptakan ketidakpastian untuk menghasilkan uang. Misalnya, risiko perjudian.
3. Risiko Khusus, maksudnya adalah risiko yang berasal dari suatu peristiwa atau kejadian dan biasanya diketahui penyebabnya. Contohnya risiko pesawat jatuh.
4. Risiko Dinamis, maksudnya adalah risiko yang muncul sebagai hasil dari perkembangan dan kemajuan manusia dalam ilmu pengetahuan dan teknologi.
5. Risiko fundamental adalah risiko yang berpotensi melukai banyak orang dan sumbernya tidak dapat diidentifikasi. Contohnya tsunami dan banjir.

2.5 Manajemen Risiko

2.5.1 Definisi Manajemen Risiko

Mengidentifikasi risiko, menilai risiko, dan mengambil tindakan untuk ngi risiko ke tingkat yang dapat diterima merupakan definisi dari en risiko (Stoneburner et al., 2002). Dengan menjaga proses bisnis yang misi atau tujuan bisnis organisasi, manajemen risiko membantu manajer

Optimized using
trial version
www.balesio.com

bisnis menyeimbangkan biaya keuangan dan operasional dari tindakan pencegahan dan meningkatkan kemampuan misi organisasi (Yustanti et al., 2018). Manajemen risiko tidak terbatas hanya pada teknologi informasi, namun ini merupakan sebuah proses bisnis yang dapat membantu manajemen dalam memenuhi tugas untuk melindungi asset organisasi. Manajemen risiko pada suatu program bertujuan untuk mengurangi risiko yang mungkin muncul dengan melaksanakan tugas atau tanggung jawab tertentu dengan standar yang memuaskan dan mendapatkan persetujuan manajemen puncak.

Manajer suatu organisasi harus mampu memastikan bahwa organisasi memiliki kemampuan yang dibutuhkan dalam pencapaian tujuan. Oleh sebab itu, organisasi perlu menentukan kemampuan keamanan teknologi informasi dalam menyediakan dukungan dalam menghadapi ancaman dunia nyata. Karena sebagian besar bisnis memiliki dana terbatas untuk keamanan TI, pengeluaran untuk itu harus dipertimbangkan secara cermat seperti pilihan manajemen lainnya. Manajemen dapat menemukan pengendalian keamanan yang tepat untuk mencapai tujuan organisasi dengan bantuan teknik manajemen risiko yang efektif (Stoneburner et al., 2002).

2.5.2 Tahapan Manajemen Risiko

Dalam manajemen risiko terdiri dari tiga proses berbeda, yaitu penilaian risiko, mitigasi risiko, dan evaluasi dan penilaian. Berikut adalah penjelasan tentang proses pada manajemen risiko (Stoneburner et al., 2002).

1. Penilaian Risiko

Salah satu proses pertama dalam pendekatan manajemen risiko adalah penilaian risiko. Proses ini biasanya digunakan oleh organisasi

Optimized using
trial version
www.balesio.com

untuk menentukan tingkat *threat* dan *risk* yang mungkin terkait dalam teknologi informasi. Hasil penilaian risiko dapat membantu organisasi menemukan cara terbaik untuk mengurangi atau mengeliminasi risiko selama proses pengurangan risiko.

2. Mitigasi Risiko

   Mitigasi risiko adalah tahap kedua dari manajemen risiko. Ini mencakup menentukan prioritas, menilai, dan menerapkan metode pengurangan risiko yang tepat yang disarankan oleh proses penilaian risiko. Manajemen senior, manajer fungsional dan bisnis bertanggung jawab untuk menggunakan strategi yang paling murah atau terendah dan menerapkan pengendalian yang sesuai karena biasanya sulit atau hampir mustahil untuk menghilangkan semua risiko pada tahap ini.

3. Evaluasi dan Penilaian

   Di sebagian besar organisasi, aplikasi perangkat lunak akan diperbarui atau diganti dengan versi yang lebih baru, koneksi akan terus diperluas dan diperbarui, dan komponen akan dimodifikasi. Selain itu, peraturan keamanan mungkin akan berubah seiring waktu, begitu pula perubahan personel. Risiko baru akan muncul sebagai akibat dari perubahan ini, dan *risk* yang sebelumnya telah berkurang dapat muncul kembali. Oleh karena itu, proses *risk management* bersifat berkelanjutan dan dinamis. Prosedur ini menekankan pada praktik terbaik, perlunya penilaian dan evaluasi risiko berkelanjutan, dan elemen-elemen yang akan berkontribusi pada keberhasilan program *risk management*.

Optimized using
trial version
www.balesio.com

2.5.3 Penanganan Risiko

Manajemen risiko merupakan salah satu cara yang dapat dilakukan untuk menganalisis risiko yang mungkin muncul pada organisasi. Setelah melakukan penilaian risiko, langkah selanjutnya adalah mengambil langkah untuk melakukan penanganan risiko. Terdapat empat pilihan dalam penanganan risiko yang mungkin muncul sebagai berikut (Desy et al., 2014).

1. Terima (*Take*)

   Apabila organisasi tidak dapat menghindari risiko yang muncul (risiko cukup besar) yang mengakibatkan organisasi mengalami dampak yang dapat mengganggu dan merusak secara alamiah, maka tindakan yang perlu diambil terkait risiko tersebut adalah *take* atau terima. Contoh risikonya seperti bencana alam, gempa bumi, banjir, badai, dan lain sebagainya.

2. Kurangi (*Treat*)

   Apabila organisasi memiliki kemampuan untuk mengurangi risiko, maka tindakan yang harus diambil terhadap risiko tersebut adalah *treat* atau mengurangi risiko tersebut dengan cara melakukan kontrol dan mitigasi terhadap risiko sehingga akibatnya dapat diminimalkan.

3. Hindari (*Terminate*)

   Apabila risiko yang mungkin muncul dirasa terlalu besar bagi Organisasi seperti dalam rangka membuat suatu produk maka tindakan yang harus diambil adalah terminante atau hindari. Penanganan ini dilakukan apabila risiko yang ditimbulkan dapat merugikan dan engganggu proses bisnis organisasi.

Optimized using
trial version
www.balesio.com

4. Alihkan (*Transfer*)

Apabila risiko yang akan muncul dinilai akan lebih baik jika dibandingkan kepada pihak yang sesuai dengan bidang ahlinya, maka tindakan yang harus diambil adalah *transfer* atau alihkan, contohnya risiko mengenai asuransi.

2.6 Penelitian Terdahulu

No.	Nama Peneliti	Judul Penelitian	Hasil Penelitian
1.	Ericson Malau (2023)	Penerapan IEC/ISO 31010:2019 untuk *Risk Management* pada SIKS-NG (Sistem Informasi Kesejahteraan Sosial - Next Generation)	Hasil penelitian menunjukkan bahwa pada saat Dinas Sosial di Kota Batam menerapkan SIKS-NG (Sistem Informasi Kesejahteraan Sosial - Next Generation) terhadap pemrosesan rencana BANSOS, ada enam belas potensi bahaya yang muncul. Dari enam belas kemungkinan *risk* tersebut, terdiri dari 3 risiko tinggi, 8 risiko medium, dan 5 risiko rendah. Penelitian tersebut menunjukkan bahwa Standar IEC/ISO 31010: 2019 berfungsi dengan baik sebagai *framework risk management* untuk sistem aplikasi yang digunakan di lembaga pemerintah.
2.	Kamila Yumna Indira dan Evi Maria (2023)	Penerapan IEC/ISO 31010:2019 dalam Manajemen Risiko Aplikasi SMARD DISDUKCAPIL di Kabupaten Semarang	Hasil penelitian menunjukkan bahwa terdapat dua puluh kemungkinan risiko terkait dengan penerapan Sistem Informasi Administrasi Kependudukan Desa dan Kelurahan (SMARD) Disdukcapil; diantaranya empat kemungkinan *risk* pada tingkat tinggi, delapan kemungkinan *risk* pada tingkat sedang, dan delapan kemungkinan *risk* pada tingkat rendah. Hasil penelitian tersebut menunjukkan bahwa Standar IEC/ISO 31010: 2019 dapat diimplementasikan dengan baik dalam manajemen *risk*

Optimized using
trial version
www.balesio.com

			analysis sistem informasi di lembaga pemerintah. Hasil dari penelitian tersebut didokumentasikan, dan rekomendasi untuk *risk treatment* yang mungkin muncul ketika SMARD diterapkan pada layanan publik di tempat tersebut.
3.	Mirga Maulana Rachmadhani (2024)	Analisis *Risk Management* Aset pada Biro Administrasi Akademik dan Kemahasiswaan Universitas Muhammadiyah Sorong	Hasil penelitian ini menunjukkan bahwa ada 17 risiko yang telah diidentifikasi selama proses identifikasi risiko hingga evaluasi risiko. Dari tujuh belas risiko tersebut, dua termasuk risiko tinggi dengan nilai level risiko dua puluh lima pada risiko A1 dan dua puluh pada risiko A5. Lebih jauh lagi, *risk* A3, A7, A11, dan A9 mempunyai peringkat tingkat risiko empat, yang menjadikannya risiko sedang. Untuk mengevaluasi *risk* terhadap dua risiko tertinggi tersebut, kode risiko A1 dikurangi dengan membeli CCTV dan memasangkannya di ruang BAAK. Dengan mengganti jenis kertas pada cetakan ijazah dan mengganti printer dengan printer yang sesuai dan memenuhi persyaratan pencetakan ijazah, maka kode *risk* A5 dapat berkurang.
4.	Melanie Mardolna dan Evi Maria (2022)	Analisis *Risk Management* pada Penerapan Sistem Informasi Pembangunan Daerah (SIPD) Menggunakan IEC/ISO 31010:2019 di Kabupaten Rote Ndao	Hasil penelitian ini menunjukkan bahwa dari 17 kemungkinan *risk* yang terdapat dalam *fiture* atau menu perencanaan pemba-ngunan daerah aplikasi SIPD, terdiri dari 3 yang teridentifikasi memiliki tingkat *high risk*, yaitu: kebocoran data, kegagalan transaksi *finance*, dan penyalahgunaan atau peretasan akun pada *database system*. Dua risiko pada level sedang terdiri dari penyalahgunaan akun atau hak akses, pemba-

Optimized using
trial version
www.balesio.com

			talan dalam pengajuan proposal, kesalahan sistem *database*, kegagalan verifikasi proposal, ketidakmampuan pengguna untuk pemahaman fungsi-fungsi dari menu aplikasi SIPD, kesalahan dalam penginputan harga pada akun belanja, kesalahan dalam penginputan ganda pada data kegiatan perencanaan Pembangunan daerah, kesa-lahan input data pendapatan, dan kesalahan dalam pengin-putan data belanja. Dua risiko pada level rendah terdiri dari ketidakakuratan data dan informasi serta kurangnya informasi yang relevan.
5.	Ni Komang Septia Noriska	*Risk Register*: Implikasi Penerapan Manajemen Risiko pada CV. Elang Borneo Sejahtera	Hasil penelitian ini menemukan bahwa organisasi atau bisnis yang dapat memasukkan manajemen risiko ke dalam *Risk Register* memiliki keunggulan yang kompetitif. Dengan lebih tanggap terhadap peluang dan tantangan, pelaku bisnis dapat mengurangi dampak negatif dan bahkan mengubah risiko menjadi peluang untuk tumbuh.

Tabel 2.1 Penelitian Terdahulu

Optimized using
trial version
www.balesio.com