Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO/IEC 27001:2013

Sindi Aprianti[*1], Renny Puspita Sari[2], Ibnur Rusi[3]
[1,2,3]Program Studi Sistem Informasi, Universitas Tanjungpura,
Pontianak 78124, Kalimantan Barat, Indonesia
Email: [1]sindiaprnt12@student.untan.ac.id, [2]rennysari@sisfo.untan.ac.id,
[3]ibnurrusi@sisfo.untan.ac.id

Abstract. Simbada Security Risk Management Using NIST SP 800-30 Revision 1 Method and ISO/IEC 27001:2013 Control.
Sistem Informasi Manajemen Barang dan Aset Daerah (SIMBADA) is an application located at the Pontianak City Regional Finance Agency (BKD) Office to assist local governments in managing regional property, however, SIMBADA has problems with minimal risk management and is not too aware of the importance of information security on the system. Risk management is carried out using the NIST SP 800-30 Revision 1 method to conduct a risk assessment of SIMBADA management and provide mitigation recommendations based on ISO/IEC 27001: 2013 Control so that it can be a reference for minimizing risks that may occur. As a result, SIMBADA has 20 lists of risks that are at very high, high, medium, and low levels which will be given control recommendations for implementing information system security. There are 20 lists of risk threats and 54 mitigation recommendations that refer to ISO/IEC 27001:2013 Controls in 11 clauses, 21 objective controls, and 39 security controls that can be used.
Keywords: *risk management, information security, NIST SP 800-30 Revisi 1, Kontrol ISO/IEC 27001:2013*

Abstrak. *Sistem Informasi Manajemen Barang dan Aset Daerah (SIMBADA) merupakan aplikasi yang terdapat di Kantor Badan Keuangan Daerah (BKD) Kota Pontianak untuk membantu pemerintah daerah dalam mengatur barang milik daerah, namun SIMBADA memiliki permasalahan minimnya pengelolaan risiko serta belum terlalu menyadari pentingnya keamanan informasi terhadap sistem tersebut. Dengan ini dilakukannya manajemen risiko menggunakan metode NIST SP 800-30 Revisi 1 dengan tujuan untuk melakukan penilaian risiko atas pengelolaan SIMBADA dan memberikan rekomendasi mitigasi berdasarkan Kontrol ISO/IEC 27001:2013 sehingga dapat menjadi acuan untuk minimalisir risiko yang mungkin terjadi. Hasilnya SIMBADA memiliki 20 daftar risiko yang berada pada level sangat tinggi, tinggi, sedang, dan rendah yang akan diberikan rekomendasi kontrol untuk penerapan keamanan sistem informasi. Terdapat 20 daftar ancaman risiko dan 54 rekomendasi mitigasi yang mengacu pada Kontrol ISO/IEC 27001:2013 dalam 11 klausul, 21 kontrol objektif, dan 39 kontrol keamanan yang dapat digunakan.*
Kata Kunci: *manajemen risiko; keamanan informasi; NIST SP 800-30 Revisi 1; Kontrol ISO/IEC 27001:2013.*

1. Pendahuluan

Perkembangan teknologi saat ini mulai digunakan oleh berbagai sektor pemerintahan di Indonesia guna mencapai tujuan, visi dan misi organisasi atau perusahaan. Keamanan informasi dapat didefinisikan sebagai usaha untuk melakukan perlindungan terhadap aset informasi yang kita miliki [1]. Saat ini, masih terdapat organisasi atau perusahaan belum menyadari pentingnya keamanan informasi terkhusus pada SIMBADA yakni aset sistem informasi yang penting bagi Badan Keuangan Daerah (BKD) Kota Pontianak karena berkaitan dengan inventarisasi barang daerah. Terdapat beberapa permasalahan yang terjadi pada SIMBADA sehingga menghambat operasional pada BKD diantaranya kesalahan input data, gangguan tegangan listrik, dan *server*

down. Pemecahan masalah yang pernah dilakukan diantaranya yaitu memastikan data yang diinputkan sudah sesuai dan *maintenance* pada server yang ada. Atas permasalahan dan pemecahan solusi yang pernah dilakukan, maka perlu untuk melakukan optimalisasi solusi berupa penelitian guna mengorganisir pengelolaan aset dan manajemen risiko dari SIMBADA. Pentingnya akan penjagaan aset dan pengelolaan risiko sudah menjadi perhatian pada BKD Kota Pontianak, namun belum secara maksimal diimplementasikan, diantaranya pengelolaan pada SIMBADA. Kurang optimalnya fungsi dari SIMBADA ini dapat berdampak pada lambatnya perolehan informasi mengenai inventarisasi barang daerah serta kurangnya keakuratan data tersebut. Hal ini disebabkan karena keamanan informasi dapat menjamin keakuratan data, artinya ketika keamanan informasi menjadi prioritas perhatian maka data yang disajikan akan akurat, relevan, dan cepat untuk diproses, sehingga perlu untuk meningkatkan kesadaran dalam manajemen risiko keamanan informasi.

Penilaian dan pengurangan risiko merupakan rangkaian yang dilakukan dalam manajemen risiko keamanan informasi yaitu berdasarkan kebutuhan keamanan informasi ini yang terdiri dari tiga elemen yakni *confidentiality*, *integrity* dan *availability* [2]. Dalam melakukan manajemen risiko keamanan informasi sebagai panduan penelitian ini yaitu dengan menerapkan metode NIST SP 800-30 Rev 1 yang merupakan kerangka kerja manajemen risiko yang memberikan panduan dalam memahami langkah-langkah proses manajemen risiko. Sedangkan pengertian ISO/IEC 27001:2013 merupakan cara penerapan untuk mengontrol keamanan informasi sebagai proses dalam pemantauan risiko yang digunakan untuk menghasilkan rekomendasi mitigasi. Manajemen risiko atas SIMBADA diharapkan dapat mengurangi kemungkinan adanya risiko pada level sedang atau bahkan rendah, dengan cara memberikan rekomendasi dari kemungkinan sumber ancaman yang ada.

2. Tinjauan Pustaka

2.1 Manajemen Risiko

Risiko merupakan peluang timbulnya penyimpangan dari intensi yang dapat menyebabkan kerugian [3]. Risiko juga diartikan sebagai kemungkinan konsekuensi yang tidak diinginkan atau berpotensi membahayakan, seperti kehilangan, cedera, atau kebakaran [4], sedangkan manajemen risiko yakni kegiatan terkoordinasi yang dilakukan dengan tujuan mengelola dan mengendalikan organisasi menggunakan tahapan identifikasi, menentukan risiko, penilaian, dan pengambil tindakan untuk melakukan mitigasi [5]. Pada lingkup risiko dan manajemen risiko, terdapat istilah risiko teknologi informasi (TI) atau risiko TI. Risiko TI diartikan sebagai risiko terhadap aset perusahaan yang disebabkan oleh pengamalan teknologi informasi, risiko teknologi informasi ini yakni komponen dari keseluruhan risiko dalam perusahaan. Risiko TI bisa berdampak pada operasional perusahaan dan menciptakan tantangan dalam mencapai tujuan dan pencapaian strategis [6]. Manajemen risiko dapat diterapkan pada perusahaan dan juga sistem informasi. Salah satu bentuk manajemen risiko yang diterapkan pada sistem informasi yaitu pada penelitian [7] dan [8].

2.2 Keamanan Informasi

Informasi adalah data yang diatur untuk membuat lebih bermakna dan berguna, dan ditujukan untuk masyarakat umum. Keamanan informasi ialah pemeliharaan informasi dari ancaman terhadap berbagai serangan seperti peretas dan virus, memastikan kelangsungan organisasi perusahaan, mengurangi risiko bisnis, meningkatkan laba atas investasi serta peluang bisnis [9].

Informasi adalah suatu aset berharga dari sebuah organisasi atau perusahaan yang melakukan pememprosesan informasi dan hasilnya disimpan dan dibagikan. Keamanan sistem informasi mencakup perlindungan dari aspek-aspek berikut [10]:

1. *Confidentiality* (kerahasiaan) merupakan aspek yang mengamankan kerahasiaan data maupun informasi karena data atau informasi hanya dapat diakses bagi orang yang berhak;
2. *Integrity* (Integritas) merupakan aspek untuk memastikan suatu data tidak dimodifikasi tanpa persetujuan pihak yang berhak, untuk melindungi ketepatan dan integritas informasi; dan

3. *Availability* (Ketersediaan) merupakan aspek yang menyediakan data/informasi sesuai kebutuhan dan memungkinkan pengguna yang berhak untuk menggunakan informasi dan alat yang relevan.

2.3 Metode NIST SP 800-30 Revisi 1

NIST merupakan standar yang dikembangkan oleh *National Institute of Standards and Technology*. NIST SP 800-30 Revisi 1 memiliki keamanan informasi yang konsisten dan komprehensif untuk pembuatan kebijakan, model aset terstruktur, dan kemampuan produsen risiko yang berbeda untuk menerapkan informasi keamanan berkontribusi secara signifikan untuk melakukan penilaian risiko [11]. Proses penilaian risiko dilakukan dengan menerapkan metode NIST SP 800-30 Rev 1 yang memiliki 6 tahapan yaitu:

1. Identifikasi Sumber Ancaman: mengidentifikasi sumber ancaman yang ada pada Sistem Informasi Manajemen Barang dan Aset Daerah. Kemudian besar rentang efek setiap sumber ancaman ditentukan oleh organisasi;
2. Identifikasi Peristiwa Ancaman: hasil dari wawancara terhadap narasumber kemudian dilakukan identifikasi peristiwa ancaman untuk mencari tahu sejauh mana signifikannya peristiwa ancaman dengan Sistem Informasi Manajemen Barang dan Aset Daerah;
3. Identifikasi Kerentanan dan Kondisi Predisposisi: identifikasi kerentanan yang digunakan untuk menghasilkan daftar kerentanan sistem yang dapat dieksploitasi nanti. Kerentanan termasuk kelemahan yang terdapat pada perangkat lunak, perangkat keras, atau perangkat lain yang dapat menimbulkan ancaman;
4. Penentuan Kemungkinan: menentukan kemungkinan mengetahui besarnya kecenderungan yang akan terjadi. Organisasi menggunakan proses tiga langkah untuk menentukan probabilitas keseluruhan dari peristiwa ancaman. Pertama, organisasi menilai kemungkinan terjadinya peristiwa ancaman. Kedua, organisasi menilai kemungkinan bahwa peristiwa yang mengancam sebelumnya dapat berdampak negatif sistem. Ketiga, organisasi mengevaluasi probabilitas keseluruhan sebagai kombinasi dari kemungkinan inisiasi/peristiwa dan kemungkinan menghasilkan dampak negatif;
5. Penentuan Dampak: melakukan Identifikasi dampak negatif dari keberhasilan terjadinya ancaman. Harapan dari langkah ini yakni mengetahui dampak negatif yang akan diperoleh jika ancaman tersebut terjadi. Organisasi menggambarkan efek negatif yang berpotensi merusak sistem.
6. Penentuan Risiko: melakukan penilaian tingkat risiko pada sistem TI dengan mengkombinasikan tingkat dari penentuan kemungkinan dan penentuan dampak. Penentuan risiko juga menunjukkan tindakan yang harus diambil untuk setiap tingkat risiko. Penentuan tingkat risiko dapat dilihat pada Tabel 1 [11].

Tabel 1. Tingkat Risiko

Kemungkinan	Dampak				
	Sangat Rendah	**Rendah**	**Sedang**	**Tinggi**	**Sangat Tinggi**
Sangat Tinggi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Tinggi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sedang	Sangat Rendah	Rendah	Sedang	Sedang	Tinggi
Rendah	Sangat Rendah	Rendah	Rendah	Rendah	Sedang
Sangat Rendah	Sangat Rendah	Sangat Rendah	Sangat Rendah	Rendah	Rendah

2.4 Kontrol ISO 27001:2013

International Organization for Standarization dan *International Electrotechnical Commission* menerbitkan seri ISO/IEC 27001 sebagai standar keamanan informasi yang menggantikan BS-7799:2. ISO/IEC 27001 mencakup kualifikasi atau spesifikasi yang wajib dipenuhi saat membuat Sistem Manajemen Keamanan Informasi (SMKI). Standar ini tidak bergantung pada produk TI dan memerlukan pemanfaatan metode manajemen berbasis risiko,

dengan kontrol keamanan terpilih yang melindungi informasi dari bermacam risiko dan memberikan tingkat keamanan kepada pemangku kepentingan [12].

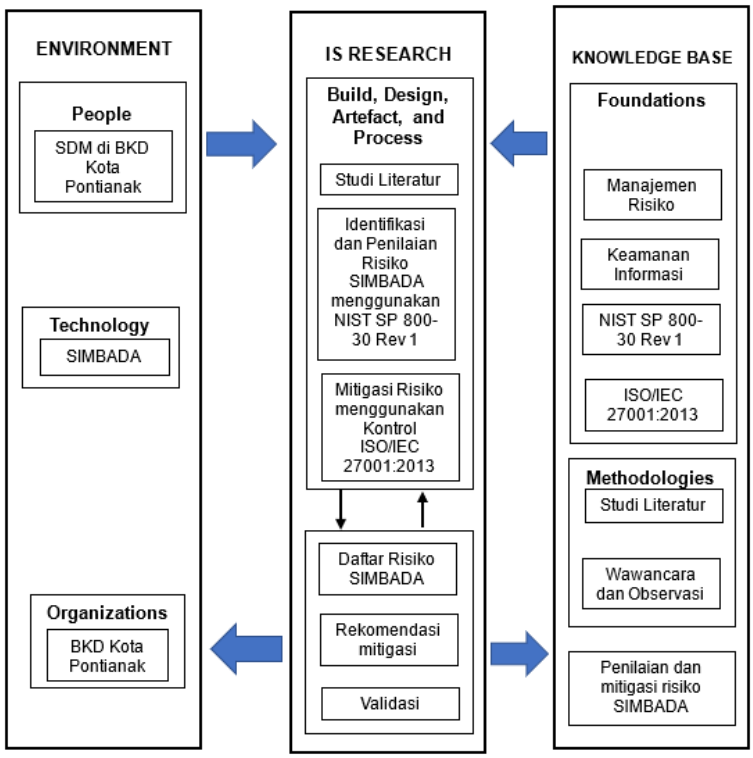
Standar Internasional ini juga melingkupi persyaratan untuk penilaian dan penindakan risiko keamanan informasi yang disesuaikan dengan keperluan organisasi. ISO 27001:2013 memiliki 14 klausul, 35 Kontrol Objektif dan 114 Kontrol Keamanan. Kontrol Objektif menekankan pada objek-objek apa saja yang perlu untuk diberi tindakan pengamanan, sedangkan Kontrol Keamanan lebih kepada aktivitas atau kegiatan yang harus dilakukan guna mencapai pengamanan pada objek tertentu.

2.5 Sistem Informasi Manajemen Barang dan Aset Daerah

SIMBADA merupakan program aplikasi yang dibuat dengan tujuan memudahkan pemerintah daerah dalam mengatur barang milik daerah. Aplikasi SIMBADA dimaksudkan untuk memperlancar pengumpulan informasi mengenai inventarisasi barang daerah. Tentunya tujuan dari pelaksanaan SIMBADA adalah untuk mendapatkan data produk daerah yang lebih tepat dan akurat. Selanjutnya, proses pemulihan data jauh lebih efektif karena pengguna hanya perlu mengakses Internet dan memiliki koneksi jaringan [13].

3. Metodologi Penelitian

Metodologi penelitian yang diterapkan yakni kerangka penelitian *Information System (IS) Research* atau yang disebut dengan *Framework Hevner* yang berfungsi untuk memaparkan tahapan pelaksanaan penelitian untuk memecahkan permasalahan guna mencapai tujuan penelitian. Adapun metodologi penelitian dapat dilihat pada Gambar 1 berikut.



Gambar 1. ***Framework IS Research***

Tahap awal yang dilaksanakan adalah melakukan studi literatur dengan mencari dan mengamati teori mengenai topik yang akan dibahas. Dalam tahap ini, semua teori yang terkait dengan topik manajemen risiko, keamanan Informasi dan teknologi informasi dikumpulkan dari berbagai sumber antara lain seperti buku, jurnal serta internet yang bersinggungan dengan tema penelitian yaitu “Manajemen Risiko Keamanan Sistem Informasi Manajemen Barang dan Aset

Daerah (SIMBADA) menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO 27001:2013".

Tahap kedua yaitu melakukan identifikasi dan studi lapangan ke BKD Kota Pontianak untuk mendapatkan informasi dan data mengenai manajemen risiko pada SIMBADA. Pendekatan analisis yang digunakan yaitu berorientasi pada aset/dampak (*asset/impact-oriented*), sehingga yang menjadi fokus dalam pengelolaan risiko berdasarkan aset yang ada dan kemungkinan dampak yang ditimbulkan dari aset tersebut atas SIMBADA. Penggalian data dan fakta dilakukan melalui wawancara dan observasi. Wawancara dilaksanakan dengan cara tanya jawab langsung kepada Kepala Kantor Badan Keuangan Daerah (BKD) Kota Pontianak, Kepala Bidang Pengelolaan Aset, dan Administrator SIMBADA terkait pengelolaan aset pada BKD Kota Pontianak dan penggunaan SIMBADA sebagai sistem penunjang dalam pengelolaan aset. Wawancara langsung perlu dilakukan untuk mendapatkan data yang real dan sahih. Wawancara ini dilakukan kepada pihak yang memahami kegiatan keamanan informasi atau pengelolaan Sistem Informasi Manajemen Barang dan Aset Daerah.

Pada tahap observasi dilakukan pemantauan dan peninjauan langsung terhadap subjek yang akan diteliti yaitu pada Sistem Informasi Manajemen Barang dan Aset Daerah (SIMBADA), hardware yang digunakan, pengkabelan penunjang operasional SIMBADA, jaringan yang digunakan, dan keberadaan pengelola SIMBADA. Pengamatan yang dilakukan yaitu pada bidang Aset Badan Keuangan Daerah (BKD) Kota Pontianak. Setelah didapatkan daftar aset pendukung SIMBADA, maka selanjutnya penentuan risiko dengan cara mengidentifikasi risiko-risiko dan ancaman yang ada. Tahap berikutnya adalah penilaian risiko, pada tahapan ini dilakukannya penentuan tingkat kerugian pada SIMBADA berdasarkan ancaman yang dapat menimbulkan risiko. Penilaian risiko ini dilakukan berdasarkan identifikasi sumber ancaman, identifikasi peristiwa ancaman, identifikasi keretanan dan kondisi predisposisi, penentuan kemungkinan, penentuan dampak dan penentuan risiko.

Tahap akhir pada metodologi penelitian yaitu memberikan rekomendasi mitigasi kepada BKD Kota Pontianak atas kemungkinan adanya risiko atas SIMBADA. Mitigasi risiko dilakukan berdasarkan hasil penilaian risiko dan panduan Kontrol ISO/IEC 27001:2013. Hasil dari rekomendasi dan mitigasi risiko yang diberikan dengan tujuan untuk menghindari dan mengurangi risiko dan ancaman yang kemungkinan terjadi pada Sistem Informasi Manajemen Barang dan Aset Daerah di Badan Keuangan Daerah (BKD) Kota Pontianak. Setelah daftar mitigasi risiko telah dibuat, maka dilakukan validasi kepada pihak BKD Kota Pontianak. Validasi dilakukan dengan tujuan agar rekomendasi dan mitigasi terhadap SIMBADA sesuai dan tepat dengan tujuan Badan Keuangan Daerah Kota Pontianak. Validasi ini dilakukan dengan menyampaikan dan menjelaskan kembali hasil analisis dengan metode NIST SP 800-30 Revisi 1 dan hasil rekomendasi yang diberikan terhadap pihak yang berkaitan dengan penanganan SIMBADA di Badan Keuangan Daerah tersebut.

4. Hasil dan Diskusi

Manajemen risiko keamanan SIMBADA pada BKD Kota Pontianak dengan terlebih dahulu mengidentifikasi jenis sumber ancaman. Berdasarkan metode NIST SP 800-30 Revisi 1 jenis sumber ancaman terdiri dari *adversarial* (pihak eksternal dan disengaja), *accidental* (pihak internal dan tidak disengaja), *structural* (kerusakan aset fisik/non fisik bersifat teknis yang berdampak pada keberadaan data/informasi), *environment* (kerusakan aset fisik/non fisik disebabkan fenomena alam). Setelah jenis sumber ancaman selesai ditentukan, selanjutnya mengidentifikasi peristiwa ancaman yang dapat mengancam keamanan SIMBADA. Hasil identifikasi peristiwa dan sumber ancaman dapat dilihat pada Tabel 2.

Berdasarkan Tabel 2 didapatkan aset TI dan peristiwa ancaman yang dapat mengancam keberadaan SIMBADA, dan terdapat 5 aset TI dan 9 peristiwa ancaman. Selanjutnya dari 5 aset TI yang ditentukan akan diketahui kerentanan dan tingkat kerentanan dari masing-masing aset TI dengan mengacu pada peristiwa ancaman yang ada. Adapun hasil identifikasi kerentanan dapat dilihat pada Tabel 3.

Tabel 2. Identifikasi Peristiwa Ancaman

No	Aset TI	Peristiwa Ancaman	Sumber Ancaman	Relevansi
1	*Hardware*	Rusaknya aset karena faktor usia (sudah lama digunakan)	*Structural*	*Confirmed*
		Server *website down*	*Structural*	*Predicted*
		Terjadi bencana alam seperti banjir dan gempa bumi	*Environmental*	*Predicted*
2	*Software*	Serangan *malware* yang dilakukan oleh orang yang tidak bertanggungjawab	*Adversarial*	*Anticipated*
		Tidak ada pengaturan standar keamanan pada server yang digunakan	*Structural*	*Predicted*
3	*Brainware*	Kesalahan operasional *hardware* dan *software* yang dilakukan penanggungjawab SIMBADA	*Accidental*	*Confirmed*
		Kehilangan data yang bersifat sensitive	*Accidental*	*Confirmed*
4	*Data*	Redudansi data	*Structural*	*Confirmed*
5	*Network*	Kabel dan perangkat jaringan bermasalah akibat ketidaksengajaan pegawai	*Accidental*	*Anticipated*

Tabel 3. Identifikasi Kerentanan

No	Aset TI	Kerentanan	Skala Penilaian
1	*Hardware*	Belum terdapat prosedur untuk melakukan penanganan terhadap perangkat keras	Tinggi
		Suhu ruangan yang tidak stabil	Sedang
2	*Software*	Sistem rentan *error* dan tidak dapat dioperasikan beberapa saat karena jarang melakukan *update* sistem	Tinggi
		Serangan *malware* yang dilakukan oleh orang yang tidak bertanggungjawab	Sedang
		Kurang mengamankan *password* untuk akses ke *website*, menggunakan *password* dengan tingkat keamanan minimal sehingga mudah untuk diretas	Tinggi
		Tidak terupdatenya antivirus yang digunakan	Tinggi
3	*Brainware*	Terjadinya kesalahan operasional *hardware* dan *software* yang dilakukan penanggungjawab SIMBADA	Sedang
		Kehilangan sebagian data penting pada sistem	Sedang
4	*Data*	Banyaknya data yang akan di *input* sehingga terjadi *crash* saat melakukan *input*	Sedang
		Redudansi data	Tinggi
5	*Network*	Kurang menjaga kebersihan ruangan, kurang memperhatikan kabel yang tersambung hingga mengalami kerusakan	Sedang

Selanjutkan dilakukan penentuan adanya kemungkinan akan terjadinya ancaman berdasarkan jenis sumber ancaman yang ada yaitu *Adversarial, Accidental, Structural*, dan *Environmental*. Tahapan ini dilakukan untuk mendapatkan penilaian secara keseluruhan terhadap kemungkinan terjadinya ancaman karena adanya potensi kerentanan atau kelemahan yang dapat memicu terjadinya ancaman tersebut. Berikut merupakan hasil dari penentuan kemungkinan terjadinya ancaman dan dapat dilihat pada Tabel 4.

Langkah penting selanjutnya dalam pengukuran risiko adalah menentukan dampak negatif akibat dari potensi ancaman terhadap Sistem Informasi Manajemen Barang dan Aset Daerah. Penentuan dampak didasarkan pada jenis sumber ancaman dan jenis dampak yang ditimbulkan. Adapun penentuan dampak atas terjadinya potensi ancaman tersaji pada Tabel 5 berikut.

Tabel 4. Penentuan Kemungkinan

No	Ancaman	Ancaman Akan Terjadi	Ancaman Mengasilkan Dampak Buruk	Kemungkinan Seluruhnya
Adversarial				
1	Terjadinya serangan *bruteforce* terhadap *website* dan mencoba untuk dapat masuk ke sistem	Tinggi	Tinggi	Tinggi
Accidental				
2	Kesalahan input data oleh pegawai yang berwenang pada SIMBADA	Tinggi	Tinggi	Tinggi
Structural				
3	Rusaknya aset karena faktor usia (sudah lama digunakan)	Sedang	Sangat Tinggi	Tinggi
4	*Password* mudah diretas *hacker*	Tinggi	Tinggi	Tinggi
Environmental				

Tabel 5. Penentuan Dampak

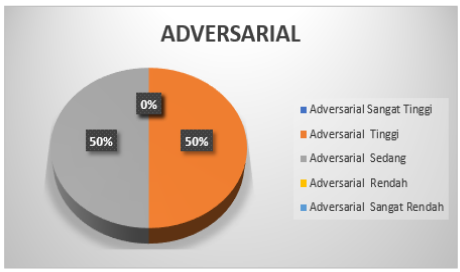
No	Jenis Dampak	Dampak	Level Dampak
Adversarial			
1	Kerugian terhadap organisasi lain	Pihak yang tidak bertanggung jawab dapat masuk dan melihat data didalam sistem disebabkan oleh penggunaan *password* kurang kuat/*default*	Tinggi
Accidental			
2	Kerugian terhadap organisasi lain	Terjadinya kesalahan pada hasil laporan terkait aset	Sangat Tinggi
Structural			
3	Kerugian terhadap aset	Mengeluarkan biaya tambahan untuk mengganti aset yang rusak	Tinggi
4	Kerugian terhadap organisasi lain	Data mudah diketahui dan dimodifikasi oleh pihak yang tidak bertanggung jawab sehingga menyebabkan kerugian pada nilai aset	Sangat Tinggi
Environmental			

Langkah akhir dari tahapan penilaian risiko yaitu penentuan risiko dengan mengumpulkan semua data yang diperoleh untuk dilakukan penilaian. Penilaian risiko didasarkan pada sumber ancaman, level kemungkinan keseluruhan, dan level dampak jika terjadi risiko. Penentuan risiko atas beberapa ancaman risiko dapat dilihat pada Tabel 6.

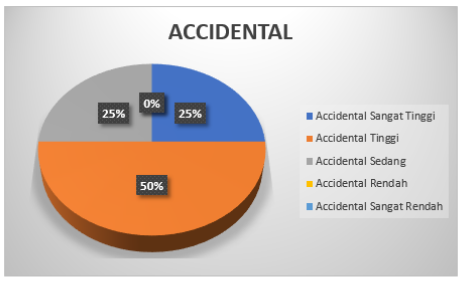
Hasil penilaian risiko yang dilakukan menunjukkan masih adanya kekurangan keamanan yang terdapat pada SIMBADA sehingga membuat penilaian berada di level sangat tinggi yang artinya peristiwa ancaman terjadi sangat parah dan berefek sangat buruk bagi sistem informasi. Pada level tinggi artinya peristiwa ancaman bisa terjadi parah dan berefek buruk pada sistem informasi. Pada level sedang artinya peristiwa ancaman bisa dapat terjadi cukup serius dan berefek buruk pada sistem informasi. Pada level rendah artinya peristiwa ancaman bisa diatasi dan berefek cukup kecil pada sistem informasi, sedangkan pada level sangat rendah artinya peristiwa ancaman bisa diabaikan. Gambar berikut merupakan persentase hasil penilaian berdasarkan sumber ancaman. Gambar 2(a) adalah risiko *adversarial* yang bersumber dari serangan pihak luar yang disengaja; Gambar 2(b) adalah risiko *accidental* yang merupakan risiko yang tidak disengaja dan biasanya berasal dari kesalahan user/admin; Gambar 2(c) adalah risiko *stuctural*, merupakan risiko dari sumber ancaman yang berpengaruh terhadap keberlangsungan jaringan komunikasi informasi dan/atau keberadaan data, seperti kerusakan kabel jaringan atau adanya virus yang sengaja dimasukkan seseorang; Gambar 2(d) adalah risiko *environmental*, merupakan risiko dari sumber ancaman yang berasal dari lingkungan seperti banjir, kebakaran, dan angin/badai.

Tabel 6. Penentuan Risiko

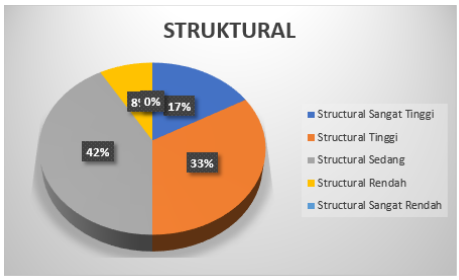
No	Ancaman	Sumber Ancaman	Level Kemungkinan	Level Dampak	Risiko
1	*Password* dengan tingkat keamanan minimal sehingga mudah diretas *hacker*	*Adversarial*	Tinggi	Tinggi	Tinggi
2	Kesalahan input data oleh pegawai yang berwenang pada Sistem Informasi Manajemen Barang dan Aset Daerah (SIMBADA)	*Accidental*	Tinggi	Sangat Tinggi	Sangat Tinggi
3	Rusaknya aset karena faktor usia (sudah lama digunakan)	*Structural*	Tinggi	Tinggi	Tinggi
4	Dimodifikasi oleh pihak yang tidak bertanggung jawab sehingga menyebabkan kerugian pada nilai aset	*Structural*	Tinggi	Sangat Tinggi	Sangat Tinggi
5	Kabel dan perangkat jaringan bermasalah akibat ketidaksengajaan pegawai	*Accidental*	Sedang	Tinggi	Sedang
6	Terjadi bencana alam seperti banjir dan gempa bumi yang menyebabkan kerusakan pada perangkat pendukung SIMBADA	*Environmental*	Rendah	Sangat Tinggi	Sedang
7	Gangguan tegangan listrik/tegangan listrik tidak stabil menyebabkan terganggunya operasional pada SIMBADA	*Environmental*	Tinggi	Sedang	Sedang
8	Kesalahan operasional *hardware* dan *software* yang dilakukan penanggungjawab pada SIMBADA	*Accidental*	Tinggi	Tinggi	Tinggi
9	Sever *website down*	*Structural*	Tinggi	Tinggi	Tinggi
10	OS pada server tidak berjalan semestinya	*Structural*	Sedang	Sangat Tinggi	Tinggi



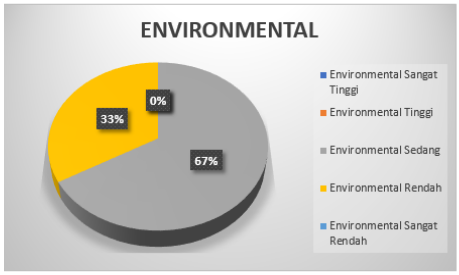
Gambar 2(a). Risiko *Adversarial*



Gambar 2(b). Risiko *Accidental*



Gambar 2(c). Risiko *Structural*



Gambar 2(d). Risiko *Environmental*

Guna mengurangi dampak dari terjadinya risiko pada SIMBADA, maka disusun rekomendari mitigasi. Rekomendasi mitigasi dibuat dengan menggunakan acuan kontrol pengendalian pada Kontrol ISO/IEC 27001:2013. Rekomendasi ini dibuat untuk meminimalisir risiko yang ada saat ini hingga ke tingkat yang dapat diterima organisasi. Tabel 7 disajikan

beberapa rekomendasi mitigasi untuk SIMBADA dari total 54 rekomendasi dan 39 kontrol berdasarkan ISO/IEC 27001:2013 yang didapatkan dalam penelitian pada BKD Kota Pontianak.

Tabel 7. Rekomendasi Mitigasi

No	Aset TI	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanan
1	*Hardware*	Rusaknya aset karena faktor usia (sudah lama digunakan)	A.11-Keamanan fisik dan lingkungan	A.11.1-Daerah Aman	A.11.1.4-Perlindungan Terhadap Ancaman Eksternal
				A.11.2-Peralatan	A.11.2.4-Kontrol Pemeliharaan Peralatan
2	*Software*	*Password* dengan tingkat keamanan minimal	A.9- Kontrol Akses	A.9.1-Kebutuhan Bisnis dari Kontrol Akses	A.9.1.1- Kebijakan kontrol akses
					A.9.1.2- Akses ke layanan jaringan
		Tidak ada pengaturan standar keamanan pada server yang digunakan	A.8-Manajemen Aset	A.8.2-Klasifikasi Informasi	A.8.2.1- Klasifikasi Informasi
					A.8.2.3- Penanganan Aset
3	*Brainware*	Kesalahan operasional *hardware* dan *software* yang dilakukan penanggungjawab SIMBADA	A.7- Kebijakan Sumber Daya Alam	A.7.2-Selama bekerja	A.7.2.2- Kesadaran keamanan informasi, pendidikan dan pelatihan
			A.11-Keamanan fisik dan lingkungan	A.11.2-Peralatan	A.11.2.1- Penempatan peralatan dan perlindungan
					A.11.2.4- Pemeliharaan peralatan
4	*Data*	Redudansi Data sehingga menghabiskan tempat penyimpanan data	A.8-Manajemen Aset	A.8.1-Tanggung jawab atas aset	A.8.1.3- Pengunaan aset yang dapat diterima
5	*Network*	Kabel LAN bermasalah hingga koneksi jaringan terputus	A.11-Keamanan Fisik dan Lingkungan	A.11.1-Keamanan Area	A.11.1.3-Keamanan ruang kerja, kantor serta lingkungan sekitar
				A.11.2-Peralatan	A.11.2.3- Keamanan Kabel

Berdasarkan rekomendasi mitigasi yang diberikan pada Tabel 7, pemilihan kontrol keamanan ISO/IEC 27001:2013 sudah sesuai dan memenuhi target pada studi kasus di BKD Kota Pontianak. Kesesuaian dan pemenuhan tersebut didasarkan pada fokus aset yang diteliti, kesesuaian antara peristiwa ancaman dan/atau risiko yang terjadi dengan klausul pada ISO/IEC 27001:2013. Sehingga rekomendasi mitigasi yang diberikan dapat menjadi masukan dalam manajemen risiko SIMBADA di BKD Kota Pontianak. Setelah mendapatkan rekomendasi mitigasi keamanan SIMBADA, maka selanjutnya dilakukan validasi kepada BKD Kota Pontianak. Hasil validasi menerangkan bahwa rekomendasi mitigasi yang diberikan kepada BKD Kota Pontianak terkait manajemen risiko keamanan informasi SIMBADA sudah sesuai dengan tujuan dari BKD Kota Pontianak terutama dalam pengelolaan SIMBADA.

5. Kesimpulan dan Saran

Berdasarkan hasil penelitian yang dilakukan di Kantor Badan Keuangan Daerah Kota Pontianak pada Sistem Informasi Manajemen Barang dan Aset Daerah menggunakan metode NIST SP 800-30 Revisi 1 untuk melakukan penilaian risiko dan Kontrol ISO/IEC 27001:2013 sebagai acuan untuk memberikan rekomendasi mitigasi risiko keamanan sistem informasi, maka didapatlah kesimpulan bahwa penelitian ini menghasilkan kontrol keamanan untuk mengurangi ancaman keamanan informasi pada SIMBADA yang merupakan program aplikasi untuk membantu pemerintah daerah dalam mengatur barang milik daerah untuk memperlancar pengumpulan informasi mengenai inventarisasi barang daerah sehingga bisa meminimalisir risiko yang dapat terjadi pada SIMBADA menggunakan metode NIST SP 800-30 Revisi 1 dan Kontrol

ISO/IEC 27001:2013. Sedangkan hasil analisis risiko yang dilakukan pada SIMBADA menggunakan langkah pada metode NIST SP 800-30 Revisi 1 terdapat 20 daftar ancaman risiko yang dapat terjadi, kemudian daftar risiko tersebut dinilai kemungkinan dan dampak nya sehingga didapatkan 3 risiko pada kategori sangat tinggi, 7 risiko pada kategori tinggi, 8 risiko pada kategori sedang dan 2 risiko pada kategori rendah. Risiko yang di kategori tinggi artinya risiko tersebut memiliki efek buruk pada SIMBADA jika terjadi. Diberikan 54 rekomendasi untuk mitigasi yang berpedoman pada Kontrol ISO/IEC 27001:2013 dalam 39 kontrol keamanan yang dapat dilakukan dan digunakan pada Kantor Badan Keuangan Daerah untuk Sistem Informasi Manajemen Barang dan Aset Daerah. Adapun saran yang diberikan peneliti lain dapat melanjutkan penelitian yang menggunakan metode lain sehingga terdapat hasil evaluasi dan rekomendasi dapat dibandingkan.

Referensi

[1] Utomo, M., Utomo, M., Ali, A. H. N., & Affandi, I. 2012. Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005. *Jurnal Teknik ITS*, *1*(1), A288–A293.

[2] Mahardika, F. 2017. Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang). *Jurnal Informatika:Jurnal Pengembangan IT (JPIT)*, *02*(02), 1–8.

[3] Kasidi. (2010). Manajemen Risiko. Bogor: Ghalia Indonesia

[4] Permatasari, D. A., Putra, W. H. N., & Perdanakusuma, A. R. 2019. Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(6), 6001–6008. http://j-ptiik.ub.ac.id

[5] Husaini, H., & Fitria, H. 2019. Manajemen Kepemimpinan Pada Lembaga Pendidikan Islam. *JMKSP (Jurnal Manajemen, Kepemimpinan, Dan Supervisi Pendidikan)*, *4*(1), 43. https://doi.org/10.31851/jmksp.v4i1.2474

[6] Harsanto, K., & Hidayat, D. 2018. Sistem Informasi Manajemen Risiko dengan Menggunakan Framework National Institute of Standards and Technology pada Lembaga Pendidikan. *Jurnal Ipsikom*, *6*(1).

[7] Putro, A.A, Ambarwati, and E. Setiawan, "Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1", JATI, vol. 11, no. 2, pp. 125-136, Sep. 2021

[8] Setiawan, I., Sekarini, A., Waluyo, R., & Afiana, F. (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto. MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer, 20(2), 389-396.

[9] Rosadi, M. I., & Hakim, L. 2015. Pengukuran dan Evaluasi Keamanan SIAKAD Universitas Yudharta Menggunakan Indeks KAMI. *Explore IT: Jurnal Keilmuan & Aplikasi Teknik Informatika Universitas Yudharta Pasuruan*, *7*(1), 33–42.

[10] Syafrizal, M. 2012. ISO 17799 : Standar Sistem Manajemen Keamanan Informasi. *Seminar Nasional Teknologi 2012 (SNT 2012)*, *2012*(November), 1–12.

[11] Rebecca M. Blank. Patrick D. Gallagher. 2012. NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Special Publication*, *September*, 95.

[12] ISO/IEC. 2013. ISO/IEC 27001 *Security Techniques Information Security Management Systems Requirement*: ISO/IEC.

[13] Wulandari, A. S., & Putra, I. S. 2015. Analisis Penerapan Sistem Informasi Manajemen Barang Daerah Dengan Metode Technology Acceptance Model Pada Pemerintah Kabupaten Blitar. *Riset Mahasiswa Ekonomi (RITMIK)*, *2*, 239–258