Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun

Medina Amirinnisa[1], Rahadian Bisma[2]

[1,2]Program Studi Sistem Informasi, Universitas Negeri Surabaya

[1]medinaamirinnisa16051214034@mhs.unesa.ac.id

[2]rahadianbisma@unesa.ac.id

Abstrak— **Penggunaan teknologi informasi yang semakin pesat membutuhkan suatu sistem untuk menjaga keamanan data dan informasi. Dinas Komunikasi dan Informatika Kota Madiun merupakan lembaga pemerintahan yang memiliki tanggung jawab untuk mengelola teknologi informasi dan komunikasi di Kota Madiun. Sebagai instansi yang bertugas untuk melayani dan memberikan informasi kepada masyarakat, DISKOMINFO Kota Madiun rentan terhadap potensi ancaman keamanan informasi yang dapat menghambat kinerjanya. Oleh karena itu, untuk memenuhi standar keamanan informasi ISO 27001:2013 maka dibutuhkan suatu penilaian analisis keamanan informasi berdasarkan pemetaan ISO 27005:2013 sebagai acuan standar keamanan informasi internasional dengan metode *Failure Model Effect Analysis* (FMEA). Metode yang digunakan yaitu dengan melakukan pemetaan referensi kontrol dan Annex A pada perencanaan ruang lingkup sistem keamanan informasi yang dibangun dan bukti dokumen terkait. Berdasarkan hasil penelitian ditunjukkan bahwa penilaian risiko pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun berada di tingkat level *low* dan *medium* dan didapatkan rekomendasi SOP sebagai bentuk mitigasi risiko.**

Kata Kunci— **Analisis Risiko, ISO 27001:2013, ISO 27005:2013, Keamanan Informasi, FMEA.**

I. PENDAHULUAN

Risiko merujuk pada situasi atau kejadian yang jika terjadi, berpotensi menghalangi kemajuan pencapaian tujuan atau target suatu divisi atau perusahaan. Sumber dari risiko ini bisa berasal dari faktor internal maupun eksternal perusahaan.[1]. Sumber risiko merujuk pada elemen atau unsur, baik secara individu maupun berinteraksi dengan elemen lainnya, yang memiliki kemungkinan untuk menyebabkan timbulnya risiko. Dengan demikian, sumber risiko adalah akar atau asal mula dari peristiwa atau kejadian yang berpotensi menimbulkan dampak negatif pada suatu entitas atau proses. [2].

Aset dalam hal ini dapat berupa *information, network, hardware, software, infrastructure, organization, physical/site, people, dan business activity*. Keamanan informasi adalah suatu tindakan yang dilakukan untuk melindungi informasi dan sistem informasi dari berbagai ancaman yang dapat mempengaruhi aset-aset yang terkait. Tujuan utama dari keamanan informasi adalah untuk memastikan kelangsungan operasional bisnis dan mengurangi risiko yang mungkin terjadi akibat potensi gangguan atau akses tidak sah terhadap informasi yang sensitif [3].

Peraturan Presiden No.95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik adalah salah satu peraturan perundangan yang mengatur mengenai organisasi pemerintah daerah yang menerapkan aspek pengendalian keamanan informasi dalam beberapa bidang penerapan. Peraturan ini menerapkan bahwa setiap organisasi daerah perlu menerapkan aspek pengendalian keamanan informasi, manajemen keamanan informasi, dan audit keamanan informasi.

ISO 27001:2013 adalah sebuah standar sertifikasi terbaru dalam seri 27000 yang dirilis pada tahun 2013. Standar ini berkaitan dengan Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) yang memberikan panduan secara umum mengenai langkah-langkah yang harus diambil oleh organisasi atau perusahaan untuk menerapkan konsep keamanan informasi. ISO 27001:2013 bertujuan untuk membantu organisasi dalam memahami, mengelola, dan mengurangi risiko keamanan informasi, sehingga mereka dapat melindungi informasi sensitif dan menjaga kelangsungan bisnis dengan lebih baik[4].

Dinas Komunikasi dan Informatika (Diskominfo) Kota Madiun berfungsi sebagai pelayanan publik dalam bidang teknologi informasi. Tugas utamanya adalah memastikan keamanan, kerahasiaan, integritas, dan ketersediaan data untuk masyarakat dan pemerintah. Namun, kurangnya kesadaran akan pentingnya keamanan informasi dapat menyebabkan risiko seperti kebocoran, kerusakan, ketidakakuratan, atau ketidaktersediaan data yang berharga.

Berdasarkan masalah diatas, dibutuhkan sebuah solusi yakni pembuatan prosedur risiko.

Pembuatan prosedur risiko ini sebagai upaya untuk mengantisipasi seluruh potensi serta peluang risiko yang mungkin timbul. Dalam melakukan penilaian risiko perlu adanya suatu tindakan yaitu dengan cara mengidentifikasi risiko, menganalisa risiko, dan mengevaluasi risiko pada kemanan informasi di Diskominfo Kota Madiun dengan standar ISO 27001 : 2013.

Oleh karena itu, dari hasil penilaian risiko menggunakan framework ISO 27001 : 2013 tersebut dapat memberikan gambaran mengenai risiko apa saja yang mungkin terjadi terhadap aset informasi yang dimiliki, kebutuhan, dan kearsipan aset yang dapat menghasilkan rancangan manajemen risiko keamanan informasi untuk perbaikan dan peningkatan kualitas pada pemerintah Kota Madiun.

II. LANDASAN TEORI

A. *Informasi*

Informasi merupakan aset berharga yang memerlukan perlindungan agar tetap aman. Keamanan secara umum berarti berada dalam kondisi bebas dari ancaman atau bahaya. Untuk mencapai keamanan, logikanya adalah dengan melindungi informasi dari segala potensi ancaman dan bahaya yang mungkin timbul. [5].

Informasi merupakan data yang telah diproses menjadi relevan dan bermakna bagi penerimanya. Informasi biasanya dianggap sebagai sumber daya yang berharga dan dapat dikelola untuk membantu pengambilan keputusan bagi suatu instansi, baik dalam keadaan saat ini maupun di masa depan. Karena pentingnya peran informasi dalam proses pengambilan keputusan, distribusi dan penyebaran informasi dianggap sebagai hal yang sangat penting [6].

B. Aset

Aset adalah sumber daya yang dimiliki oleh instansi atau semua hak yang dapat dimanfaatkan oleh instansi. Termasuk di dalam aset adalah kewajiban yang tertunda yang dinilai dan diakui sesuai dengan prinsip ekonomi yang berlaku. Menurut FASB (Financial Accounting Standard Boards), aset dijelaskan sebagai potensi keuntungan ekonomi yang akan diperoleh atau dikendalikan oleh instansi di masa depan sebagai hasil dari transaksi atau kejadian yang telah terjadi di masa lalu. [6].

Aset informasi adalah sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti, keahlian, waktu, sumber daya dan* kombinasinya serta diakui sebagai sesuatu yang berharga bagi organisasi. Aset informasi pada penelitian ini akan mengacu pada definisi komponen. Sistem aset informasi adalah sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti, keahlian, waktu, sumber daya, dan kombinasinya serta diakui sebagai sesuatu yang berharga bagi organisasi. Komponen sistem informasi dibangun berdasarkan komponen-komponen pendukung yang meliputi sember daya manusia (*people*), perangkat keras (*hardware*), perangkat lunak (*software*), data dan jaringan (*network*) [3].

C. Keamanan Informasi

Keamanan informasi adalah tindakan untuk melindungi informasi dari berbagai ancaman yang dapat terjadi, dengan tujuan memastikan kelangsungan bisnis, mengurangi risiko bisnis, dan mengoptimalkan pengembalian investasi serta peluang bisnis. [4].

Aspek dari keamanan informasi meliputi tiga hal yaitu CIA diantaranya *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). Aspek tersebut dapat dilihat sebagai berikut [3].

1) Kerahasiaan (Confidentiality) Kerahasiaan informasi berarti melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.
2) Integritas (Integrity) Integritas informasi menandakan bahwa informasi harus utuh dan tidak mengalami perubahan yang tidak sah atau tidak diinginkan.
3) Ketersediaan (Availability) Ketersediaan berarti memastikan bahwa layanan, fungsi sistem, dan informasi tersedia untuk pengguna saat diperlukan.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Contoh dari kemanan informasi antara lain [5] :

1) *Physical Security* merupakan aspek keamanan informasi yang berfokus pada strategi untuk melindungi individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman seperti bahaya kebakaran, akses yang tidak diotorisasi, dan bencana alam.
2) *Personal Security* sering kali terkait dengan aspek-aspek yang berkaitan dengan personil organisasi dan saling berhubungan dengan ruang lingkup keamanan informasi secara keseluruhan"*Physical Security"*.
3) *Operation Security* fokus pada strategi organisasi untuk melindungi kemampuan operasional organisasi dari gangguan atau

hambatan yang dapat mengganggu kelangsungan berfungsinya organisasi secara normal. Hal ini melibatkan upaya dalam menjaga kontinuitas operasional agar organisasi tetap dapat berfungsi dengan baik tanpa terganggu oleh berbagai ancaman atau insiden keamanan.

4) *Communication Security* ditujukan untuk melindungi media komunikasi, teknologi komunikasi, dan isinya. Selain itu, keamanan informasi ini juga bertujuan untuk memastikan bahwa organisasi dapat memanfaatkan media dan teknologi komunikasi dengan aman guna mencapai tujuan yang telah ditentukan.
5) *Network Security* keamanan informasi yang berfokus pada cara melindungi peralatan jaringan, data organisasi, jaringan itu sendiri, serta kemampuan untuk menggunakan jaringan tersebut dalam mendukung fungsi komunikasi dan pertukaran data organisasi.

Setiap komponen di atas memiliki peran penting dalam program keamanan informasi secara menyeluruh. Keamanan informasi adalah tindakan melindungi informasi, termasuk sistem dan perangkat yang digunakan untuk menyimpan dan mengirim informasi. Tujuannya adalah untuk melindungi informasi dari berbagai ancaman, sehingga dapat menjamin kelangsungan bisnis, mengurangi dampak kerusakan yang diakibatkan oleh ancaman, dan meningkatkan pengembalian investasi serta peluang bisnis.

D. Risiko

Risiko adalah ketidakpastian yang dapat mempengaruhi pencapaian sasaran. Sasaran menjadi titik acuan dalam mendefinisikan risiko yang harus jelas dan baik. Risiko dapat berdampak negatif, positif, atau keduanya tergantung pada dampak yang dihasilkan. [2].

Risiko umumnya terkait dengan sumber risiko, peristiwa yang mungkin terjadi, dampak dari peristiwa tersebut, dan tingkat kemungkinan terjadinya peristiwa. Risiko yang belum terjadi dapat menjadi potensi masalah di masa depan. Dampak atau konsekuensi dapat muncul akibat tindakan atau kegagalan dalam mengatasi peluang atau ancaman tertentu. [2]. Ketika ancaman berhasil mengeksploitasi kerentanan, risiko tersebut dapat menyebabkan kerusakan atau dampak negatif pada organisasi[7].

Risiko merujuk pada kemungkinan bahwa sumber ancaman dapat mengeksploitasi kerentanan potensial, yang kemudian mengakibatkan dampak negatif pada organisasi. Memahami dan mengidentifikasi risiko menjadi hal penting bagi organisasi. Dengan kemampuan tersebut, organisasi dapat mengurangi dampak yang mungkin terjadi dan mengambil langkah-langkah untuk meminimalkan risiko yang dihadapi. [3].

E. Risiko Teknologi Informasi

Dalam penggunaan teknologi informasi, terdapat enam kategori risiko yang perlu diperhatikan:

1) 1) Keamanan: Risiko terjadinya perubahan atau penggunaan informasi oleh pihak yang tidak berwenang.
2) 2) Ketersediaan: Risiko tidaknya data dapat diakses setelah terjadi kegagalan sistem, disebabkan oleh kesalahan manusia, konfigurasi instansi, atau kurangnya penggunaan arsitektur yang tepat.
3) 3) Pemulihan: Risiko ketidakmampuan memulihkan informasi yang diperlukan setelah terjadinya kegagalan dalam perangkat lunak, perangkat keras, ancaman eksternal, atau bencana alam.
4) 4) Performa: Risiko ketidaktersediaan informasi saat dibutuhkan, akibat arsitektur terdistribusi, permintaan yang tinggi, dan variasi topografi informasi teknologi.
5) 5) Skalabilitas: Risiko yang muncul akibat perkembangan bisnis, hambatan pengaturan, dan arsitektur yang tidak mampu menangani banyak aplikasi baru dengan biaya yang efisien.
6) 6) Kepatuhan: Risiko terkait manajemen atau penggunaan informasi yang melanggar kebutuhan dari pihak pengatur, termasuk aturan pemerintah, panduan instansi, dan kebijakan internal..

F. Manajemen Resiko

Manajemen risiko adalah rangkaian proses untuk mengidentifikasi risiko, menilai risiko, dan merencanakan tindakan untuk mengurangi risiko hingga mencapai tingkat yang dapat diterima oleh organisasi. Dalam mengimplementasikan manajemen risiko teknologi informasi di sebuah organisasi, akan ditemui berbagai ancaman yang berpotensi menimbulkan risiko dan mengganggu proses bisnis. Penelitian sebelumnya telah melakukan identifikasi ancaman berdasarkan aset-aset teknologi informasi yang dimiliki organisasi. [3].

Tabel 2.1 Tabel Kategori Aset Teknologi Informasi

No.	Kategori Aset TI	Ancaman
1.	*Hardware*	- Pelanggaran pemeliharaan sistem informasi - Hilangnya pasokan listrik - Debu, korosi, kerusakan fisik - Dicuri
2.	*Software*	- *User interface* sulit dipahami dan

		digunakan - Serangan virus
3.	*Network*	- Adanya gangguan pada *gateway* - Kesalahan konfigurasi - Ada kesalahan pada data center - Kerusakan fisik pada kabel dan komponen lain
4.	Data dan Informasi	- Kebocoran data - Data hilang/rusak - Penyalahgunaan atau modifikasi data - Data *overload*
5.	*People*	- Kekurangan tenaga kerja - Kesalahan operasional *(human error)* - Pemalsuan hak - Penyalahgunaan wewenang

Manajemen risiko adalah rangkaian kegiatan organisasi yang terarah dan terkoordinasi yang berfokus pada pengelolaan risiko. Komponen-komponen dari manajemen risiko meliputi prinsip-prinsip, kerangka kerja, dan proses yang digunakan untuk mengidentifikasi, menilai, dan mengatasi risiko dalam suatu organisasi. Proses manajemen risiko terdiri dari beberapa langkah berikut: [1]

1) Memahami sasaran dan konteks
   Risiko dapat diartikan sebagai ancaman dan peluang yang muncul karena ketidakpastian dalam mencapai sasaran. Ketidakpastian ini disebabkan oleh perubahan dalam konteks atau lingkungan yang dihadapi oleh organisasi, baik dari lingkungan eksternal maupun internal.
2) Identifikasi risiko
   Identifikasi risiko adalah langkah untuk mengenali ketidakpastian yang mencakup peristiwa-peristiwa yang berpotensi terjadi selama proses pencapaian sasaran, baik yang terjadi di dalam maupun di luar organisasi, serta memiliki dampak yang dapat bersifat positif atau negatif terhadap sasaran tersebut.
3) Analisis risiko
   Pada tahapan ini ialah prediksi tingkat kemungkinan terjadinya dan dampak risiko yang telah diidentifikasi.
4) Evaluasi risiko
   Proses evaluasi ini merujuk pada langkah memprioritaskan risiko sesuai dengan kategori atau tingkat prioritasnya.
5) Perlakuan risiko
   Perlakuan risiko dilakukan sesuai dengan kebutuhan dan melibatkan beberapa langkah. Dimulai dari pemilihan opsi risiko, penetapan sasaran perlakuan risiko, perencanaan perlakuan risiko, analisis manfaat dan biaya, kemudian dilanjutkan dengan pelaksanaan rencana perlakuan risiko, serta monitoring dan review. Beberapa opsi perlakuan risiko yang dapat dipilih meliputi menghindari risiko, menerima risiko, berbagi risiko, serta melakukan mitigasi risiko baik yang bersifat negatif maupun positif.
6) Pelaporan risiko
   Pelaporan risiko adalah proses menyajikan secara komprehensif seluruh tahapan dari tahap awal hingga tahap akhir dalam manajemen risiko untuk memastikan bahwa proses tersebut berjalan sesuai dengan prosedur yang telah ditetapkan.

G. SNI ISO/IEC 27001 : 2013

SNI ISO/IEC 27001:2013 adalah standar nasional Indonesia yang berfokus pada Sistem Manajemen Keamanan Informasi (SMKI). Standar ini ditujukan untuk menyediakan persyaratan dalam penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap SMKI. Standar ini telah ditetapkan oleh Badan Standarisasi Nasional melalui Keputusan Nomor 61/KEP/BSN/4/2016.[8].

Standar ini menggunakan model "Plan-Do-Check-Act" (PDCA) untuk penerapan Sistem Manajemen Keamanan Informasi (SMKI). Penerapan model PDCA mencerminkan prinsip-prinsip yang ada dalam Panduan OECD (2002) yang mengatur keamanan sistem informasi dan jaringan.

Tabel 2.2 Tabel PDCA *(Plan-Do-Check-Act)*

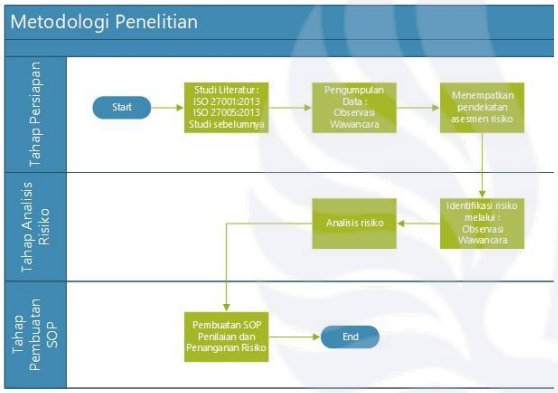
Plan (establish the ISMS)	Mengembangkan kebijakan, tujuan, proses, dan prosedur untuk Sistem Manajemen Keamanan Informasi (ISMS) yang terkait dengan manajemen risiko dan peningkatan keamanan informasi. Tujuan dari langkah ini adalah untuk mencapai hasil yang konsisten dengan kebijakan dan tujuan keseluruhan dari organisasi.
Do (implement and operate the ISMS	Menerapkan dan mengoperasikan kebijakan, kontrol, proses, dan prosedur ISMS
Chck (monitor and review the ISMS	Melakukan evaluasi dan, jika memungkinkan, mengukur kinerja proses sesuai dengan kebijakan, tujuan, dan pengalaman praktis Sistem Manajemen Keamanan Informasi (ISMS), serta melaporkan hasilnya kepada manajemen sebagai tinjauan..
Act (maintain and improve	Melakukan tindakan perbaikan dan pencegahan berdasarkan hasil audit

the ISMS)	internal ISMS dan tinjauan manajemen, serta informasi lain yang relevan, dengan tujuan mencapai peningkatan berkelanjutan dalam Sistem Manajemen Keamanan Informasi (ISMS)..

III. METODOLOGI PENELITIAN

A. Metode Penelitian

Metode penelitian adalah rangkaian langkah atau prosedur yang digambarkan secara terperinci untuk memperoleh dan mengumpulkan data dengan fungsi dan tujuan tertentu dalam suatu penelitian. Berikut merupakan *flowchart* metode penelitian yang akan digunakan pada penelitian ini dan penjabaran metodologi yang menjelaskan tiap proses alur *flowchart* :



Gambar 3.1 *Flowchart* Metode Penelitian

Berdasarkan pada gambar 3.1, berikut merupakan penjelasan mengenai proses tahapan-tahapan pada metodologi penelitian :

1) Tahap Persiapan

Tahap persiapan ini merupakan tahap awal yang dilaksanakan untuk memulai penelitian dengan memperhatikan studi literatur dan studi lapangan sebagai pengumpulan data. Berikut merupakan beberapa proses yang ada pada tahap persiapan.

a. Studi Literatur

Pada tahap studi literatur, peneliti melakukan analisis mendalam dari berbagai jurnal yang memiliki relevansi dengan penelitian yang dilakukan agar peneliti dapat mengetahui posisi penelitiannya dan melihat dimana letak perbedaan antara penelitian ini dengan penelitian sebelumnya. Selain itu studi literatur juga bisa menjadi referensi untuk mempermudah penelitian dengan cara mengumpulkan dan mempelajari informasi dari berbagai pustaka seperti *e-book*, buku, hasil penelitian terdahulu dalam bentuk skripsi maupun jurnal. Studi literatur dilakukan untuk memberikan gambaran bagaimana tahapan-tahapan dalam melakukan penilaian risiko dan pembuatan SOP penilaian risiko berdasarkan Standar Nasional Indonesia ISO/IEC 27001 : 2013 dan ISO/IEC 27005 : 2013.

b. Pengumpulan Data

Pada tahap ini dilaksanakan guna mendapatkan informasi yang dibutuhkan guna mencapai tujuan penelitian. Hasil dari studi literatur dapat membantu peneliti untuk menentukan teknik pengumpulan data yang akan digunakan diantaranya adalah melakukan survei atau observasi, melakukan wawancara kepada subjek dari penelitian terkait dan juga melakukan penyebaran kuisioner kepada subjek yang dipilih. Pengumpulan data yang dilakukan di Diskominfo Kota Madiun pada penelitian ini meliputi observasi pada Diskominfo Kota Madiun , wawancara kepada narasumber dan penetapan pendekatan asesmen risiko.

2) Tahap Analisis

Pada tahap analisis, dilakukan identifikasi sistem dan ruang lingkup penerapannya untuk mengamati kondisi aktual, serta membandingkan kesesuaian persyaratannya dengan standar ISO/IEC 27001:2013. Selain itu, untuk analisis manajemen risiko keamanan informasi, digunakan Standar ISO/IEC 27005:2013. Berikut beberapa proses pada tahap analisa.

a. Identifikasi Risiko

Pada tahap identifikasi risiko yang didukung dengan proses observasi dan wawancara bertujuan untuk mengidentifikasi kontrol yang ada serta pengaruhnya terhadap risiko, mengidentifikasi konsekuensi yang mungkin terjadi dan membuat prioritas risiko sesuai dengan kriteria evaluasi risiko yang ditetapkan dalam pembentukan konteks. Identifikasi risiko mencakup sumber risiko yang berada di bawah kendali Diskominfo Kota Madiun. Oleh karena itu, penulis

menyiapkan beberapa hal seperti daftar aset, daftar ancaman, kelemahan serta dampaknya (CIA).

b. Analisis Risiko

Analisis penilaian risiko yang dilakukan oleh penulis adalah dengan menggunakan metode FMEA berdasarkan daftar risiko yang sudah terurutkan prioritasnya.

3) Tahap Pembuatan SOP

Tahap pembuatan SOP *(Standard Operating Procedure)* merupakan tahap pengendalian dan implementasi yang dilaksanakan untuk menunjukkan *output* yang didapat dari tahap analisis yaitu berupa SOP Penilaian dan Penanganan Risiko. Selain itu pembuatan dokumen SOP Penilaian dan Penanganan Risiko ini juga berguna untuk meningkatkan kualitas kinerja suatu organisasi.

Pada tahapan ini, peneliti akan membuat dokumen SOP sesuai dengan hasil analisa yang telah peneliti lakukan sebelumnya sesuai dengan kriteria dan format yang sesuai dengan standarisasi ISO/IEC 27001 : 2013 dan didampingi oleh ISO 27005 : 2013.

B. Model Konseptual

Model yang digunakan pada penelitian ini adalah menggunakan ISO/IEC 27001 : 2013, ISO/IEC 27002 : 2013, dan ISO 27005 : 2013 yang berfokus pada risiko karena penelitian ini bertujuan untuk membuat tata kelola risiko keamanan informasi.

1) ISO/IEC 27001 : 2013

Menurut Standar International, ISO 27001:2013 adalah versi terbaru dari sertifikasi seri ISO 27001 yang dirilis pada tahun 2013. ISO 27001:2013 merupakan sebuah dokumen standar untuk Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) yang memberikan gambaran secara umum mengenai langkah-langkah yang harus diambil oleh sebuah organisasi atau perusahaan dalam upaya menerapkan konsep-konsep keamanan informasi. Standar ini terdiri dari 14 klausul, 35 objektif kontrol, dan 144 kontrol keamanan yang harus dipatuhi oleh organisasi dalam rangka mencapai tingkat keamanan informasi yang sesuai..

2) ISO/IEC 27005 : 2013

Menurut *International Standardization*, ISO 27005 : 2013 menjelaskan tentang proses umum untuk ISMS *(Information Security Management System)* dan mendefinisikan pendekatan dalam mengelola risiko. Standar ini juga berisi tentang pedoman untuk pengembangan konteks penilaian risko, komunikasi risiko, dan perawatan akan tetapi tidak memberikan metodologi untuk menentukan sifat dan dampak risiko aktual. Selain itu juga berisi tentang panduan untuk mengelola risiko yang dihadapi oleh organisasi sesuai dengan kebutuhannya.

C. Jenis Penelitian

Penelitian ini merupakan penelitian dengan pendekatan metode kualitatif dan kuantitatif dimana penelitian terkait merupakan gabungan penelitian dengan memberi suatu batas yang jelas secara deskriptif dan juga memberikan penjelasan tentang perhitungan data secara kompleks dan sistematis. Jenis penelitian ini dipilih karena disesuaikan dengan tujuan penelitian ini yaitu untuk mengetahui perhitungan analisis penilaian risiko pada Diskominfo Kota Madiun sesuai dengan standarisasi ISO 27001 : 2013. Penelitian ini menggunakan pendekatan penelitian kualitatif karena data yang dihasilkan merupakan data deskriptif berupa kata-kata tertulis dan dari lisan narasumber. Selain itu pendekatan penelitian kuantitatif juga digunakan untuk mengetahui hasil analisis yang akurat dari awal hingga akhir dari data yang diambil. Teknik pengumpulan data menggunakan observasi dan wawancara kepada narasumber berdasarkan kerangka kerja ISO/IEC 27001 : 2013 sehingga hasil dari observasi dan wawancara tersebut bisa langsung dianalisis dan diimplementasikan pada objek terkait.

D. Tempat dan Waktu Penelitian

1) *Tempat Penelitian*

Penelitian ini dilaksanakan di Dinas Komunikasi dan Informatika pada pemerintah Kota Madiun yang berada di Jl. Mastrip No.40, Klegen, Kec. Kartoharjo, Kota Madiun, Jawa Timur. Berikut merupakan peta lokasi Diskominfo Kota Madiun.

Gambar 3.1 Peta Lokasi Dsikominfo Kota Madiun

2) Waktu Penelitian

Pihak peneliti akan melaksanakan penelitian ini pada bulan Maret 2020 sampai dengan terselesainya kontrak penelitian.

IV. Hasil dan Pembahasan

A. *Identify Staff Knowledge*

Dalam melakukan tahap observasi, peneliti melakukan *interview protocol* dengan narasumber. Narasumber terkait adalah staf atau pegawai langsung dari Diskominfo Kota Madiun. Dan hasil dari *interview protocol* dapat dilihat pada Lampiran A. Berikut merupakan hasil identifikasi dari narasumber.

1) Aset-aset penting menurut staf atau pegawai Diskominfo Kota Madiun meliputi server, jaringan, *hardware*, *software*, *database*, SDM (Sumber Daya Manusia) dan lain-lain.
2) Diskominfo Kota Madiun memiliki beberapa aset aplikasi seperti E-Kinerja, E-Budgeting, E-Monev, E-Surat, E-SPPD, E-Reminder, E-SIKD, E-LPPD, E-UMKM, E-Data (Satu Data), E-Ruang Rapat, E-Pendekar Kelurahan dan lain-lain.
3) Diskominfo Kota Madiun menyediakan pelatihan *(training)* khusus untuk meningkatkan kemampuan *(skill)* dari masing-masing staf atau pegawai.
4) Diskominfo Kota Madiun melakukan proses pencadangan data *(data back up)* selama satu minggu sekali.
5) Setiap user ID yang digunakan oleh staf atau pegawai harus secara otentikasi ganda *(double-authentication).*
6) Untuk pengamanan ruang server dan data center hanya diberikan akses untuk beberapa orang saja dan tidak sembarang staf atau pun pegawai bisa masuk.
7) Belum ada prosedur kebijakan untuk mengatasi masalah yang terjadi pada proses penganggaran dan pengadaan barang ketika *hearing* dengan yudikatif.

B. *Daftar Kriteria Risk Acceptance*

Berikut merupakan kriteria penerimaan risiko yang menjadi acuan dalam menganalisis risiko pada Diskominfo Kota Madiun.

Tabel 4.1 Daftar Kriteria *Risk Acceptance*

Kriteria	Keterangan
Tidak Mengganggu	Dampak yang terjadi tidak mempengaruhi jalannya proses bisnis
Membahayakan	Dampak yang terjadi mempunyai kemungkinan untuk mempengaruhi jalannya proses bisnis
Mengganggu	Dampak yang terjadi mempengaruhi jalannya proses bisnis
Terhenti	Dampak yang terjadi membuat proses bisnis tidak dapat berjalan

C. *Daftar Aset Kritis*

Pembuatan daftar aset bertujuan untuk menentukan aset yang berharga dan penting bagi Diskominfo Kota Madiun. Selain itu daftar aset juga berguna untuk mengetahui aset apa saja yang dimiliki serta kebutuhan keamanan ancaman dan kekuatan serta kelemahan dalam instansi terkait. Berikut merupakan daftar aset yang ada pada *Data Center* Diskominfo.

Tabel 4.2 Daftar Aset

Kategori	Aset	Fungsi Aset
Hardware	*Portable Generating Set*	Digunakan sebagai energi cadangan apabila terjadi pemadaman listrik secara tiba-tiba oleh PLN, atau pun untuk menambah daya ketika daya listrik yang digunakan tidak mencukupi
	PC Unit	Digunakan untuk mengolah data *input* dan menghasilkan *output* berupa data/informasi sesuai dengan keinginan pengguna
	Printer	Digunakan untuk mencetak sebuah berkas/dokumen
	UPS *(Unit Power Supply)*	Digunakan sebagai alat yang menyediakan suplai arus listrik ketika tegangan utama (PLN) tidak berfungsi
	Hard Disk	Digunakan untuk menyimpan dan mengambil informasi digital menggunakan cakram yang dilapisi

		dengan bahan magnetik
	Memory Programmer	Digunakan untuk menyimpan data yang sedang aktif digunakan. Misal: RAM (*Random-Access Memory*), ROM (*Read-Only Memory*), dan *Cache Memory*
	Stabilizer	Digunakan untuk menjaga tegangan arus listrik agar stabil (normal)
	AC *Split (Air Conditioning)*	Digunakan untuk mengondisikan udara
	Mesin Absensi (*Time Recorder*)	Digunakan untuk mencatat kehadiran pegawai sebuah instansi
	CCTV	Digunakan sebagai media pengawas yang di ambil oleh kamera pengintai dan di tampilkan melalui monitor
	IPTV	Digunakan sebagai media pengawas dengan menggunakan kamera IP
Network	*Server*	• Menyediakan fitur keamanan komputer • Melindungi semua komputer yang terhubung menggunakan *firewall* Menyediakan IP *Address* untuk mesin komputer yang terhubung
	Router	Digunakan untuk mengirimkan paket data atau suatu informasi melalui internet atau jaringan dari lokasi tertentu ke jaringan lainnya
	Hub	Digunakan sebagai penerima sinyal dari sebuah komputer dan merupakan titik pusat yang menghubungkan ke seluruh komputer dalam jaringan tersebut
	Switch	Digunakan sebagai pengatur dan pembagi sinyal data dari suatu komputer ke komputer lainnya
	Modem	Digunakan untuk mengubah sinyal informasi menjadi sinyal pembawa yang siap dikirimkan dan memisahkan antara sinyal informasi dari sinyal pembawa yang
		diterima dengan baik
	Netware Interface External	Digunakan untuk menghubungkan antara sebuah host ke host lain ataupun ke network
	Crimping Tool	Digunakan untuk memasang kabel UTP ke konektor RJ-45 / RJ-11 tergantung kebutuhan
Software	E-Kinerja	• Mengukur dan memantau kinerja ASN secara periodik • Sebagai salah satu data acuan pemberian tunjangan kinerja yang diterima pegawai Memetakkan kinerja PNS dalam rangka *merit system*
	E-Budgeting	Digunakan untuk menyusun anggaran secara efektif dan efisien guna mengatasi kekurangan dari penyusunan anggaran secara manual
	E-Monev	Digunakan sebagai upaya untuk mengefektifkan dan mengefisienkan pelaporan menuju pada peningkatan kualitas dengan melakukan penyederhanaan terhadap format, aplikasi dan mekanisme pelaporan monev kinerja pembangunan
	E-Surat	Digunakan untuk memudahkan dalam surat menyurat sehingga bisa untuk merespon informasi yang masuk atau keluar lebih cepat
	E-SPPD	Digunakan untuk mengelola dokumen perjalanan dinas dalam maupun luar daerah yang efektif
	E-Reminder	Digunakan sebagai pengingat jadwal maupun hal-hal penting yang harus dilakukan
	E-SIKD	Digunakan untuk menangani pengelolaan arsip dinamis
	E-LPPD	Digunakan untuk memudahkan dalam pembuatan laporan penyelenggaraan pemerintah daerah guna mengisi realisasi

		capaian masing-masing indikator yang telah ditetapkan
	E-UMKM	Digunakan untuk memasarkan produk UMKM Indonesia
	E-Data (Satu Data)	Digunakan untuk menyimpan dan menyediakan data dalam format yang mudah dicari dan diakses
	E-Ruang Rapat	Digunakan untuk memudahkan dalam mengatur jadwal kegiatan rapat
	E-Pendekar Kelurahan	Digunakan untuk memberikan laporan pelayanan dengan keterpaduan
Information	*Database*	Digunakan sebagai penyimpanan data seperti mengelompokkan data untuk mempermudah identifikasi data serta menyiapkan data yang sesuai dengan permintaan *user* terhadap suatu informasi
	Datafile	Digunakan sebagai penyimpanan dokumen
	System Documentation	Digunakan untuk mendokumentasikan suatu sistem
	User Manual	Digunakan sebagai petunjuk bagi pengguna
	SOP	Digunakan sebagai panduan/ pedoman dalam memudahkan kerja yang berisi tahapan dan urutan suatu pekerjaan.
People	Staf/pegawai Data Center	Staf yang bertanggung jawab dan mengawasi keseluruhan ruang data center

D. Kebutuhan Keamanan Aset Kritis

Keamanan informasi merupakan langkah-langkah untuk melindungi informasi dari berbagai ancaman dengan tujuan memastikan kelangsungan proses bisnis, mengurangi risiko bisnis, mengoptimalkan pengembalian investasi, dan memanfaatkan peluang bisnis. Prinsip dasar keamanan informasi yang dikenal dengan CIA (Confidentiality, Integrity, dan Availability) digunakan sebagai pedoman dalam menjaga keamanan informasi. Pada penelitian ini, prinsip CIA digunakan sebagai kategori dalam mengidentifikasi kebutuhan keamanan aset kritis.

Tabel 4.4 Daftar Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Keamanan	Penjelasan
Server	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang
	Integritas *(Integrity)*	Server tidak boleh diakses oleh mesin atau pihak yang tidak berwenang yang dapat mengubah konten
	Ketersediaan *(Availability)*	Akses harus tersedia 24 jam
• *PC Unit* • *Printer* • UPS *(Unit Power Supply)* • *Hard Disk* • *Memory Programmer* • *Stabilizer* • AC *Split (Air Conditioning)* • Mesin Absensi (*Time Recorder*) • CCTV • IPTV	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang
	Integritas *(Integrity)*	Melakukan *monitoring* untuk memastikan daya kerja
	Ketersediaan *(Availability)*	Akses harus tersedia 24 jam
• *Router* • *Hub* • *Switch* • *Modem* • *Netware Interface External* • *Crimping Tool*	Kerahasiaan *(Confidentiality)*	Adanya *firewall* untuk melakukan *filtering access* dan memastikan tidak terjadi pelanggaran yang dapat menimbulkan masalah fatal
	Integritas *(Integrity)*	Melakukan *monitoring* jaringan untuk memastikan keaslian data
	Ketersediaan *(Availability)*	Terpasangnya sensor untuk memonitor peralatan jaringan agar selalu dapat digunakan
Portable Generating Set	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang
	Integritas *(Integrity)*	Melakukan *monitoring* untuk memastikan daya kerja
	Ketersediaan *(Availability)*	Akses harus tersedia 24 jam
• E-Kinerja • E-	Kerahasiaan *(Confidentiality)*	Aplikasi hanya dapat diakses oleh staf/pegawai

Budgeting • E-Monev • E-Surat • E-SPPD • E-Reminder • E-SIKD • E-LPPD • E-UMKM • E-Data (Satu Data) • E-Ruang Rapat • E-Pendekar Kelurahan		Diskominfo terkait yang memiliki wewenang
	Integritas *(Integrity)*	Informasi harus lengkap dan akurat
	Ketersediaan *(Availability)*	• Akses harus tersedia 24 jam • Data yang tersedia harus sering u*pdate*
• *Database* • *Datafile* • *System Documentation* • *User Manual* • SOP	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang
	Integritas *(Integrity)*	Informasi harus lengkap dan akurat
	Ketersediaan *(Availability)*	Akses harus tersedia 24 jam
Staf/ pegawai *Data Center*	Kerahasiaan *(Confidentiality)*	*Senior Management* harus memastikan bahwa karyawan tidak membocorkan data informasi penting kepada pihak yang tidak berwenang
	Integritas *(Integrity)*	• Staf/ pegawai harus mematikan semua informasi sudah lengkap dan akurat • Staf/ pegawai harus mengikuti *training* terkait teknologi informasi
	Ketersediaan *(Availability)*	Kurangnya staf IT pada bidang komunikasi informatika

E. Identifikasi Ancaman pada Aset Kritis

Pada proses identifikasi ancaman pada aset kritis, penulis melakukan penggabungan informasi yang telah diperoleh dari narasumber dengan profil ancaman terhadap aset kritis. Selain itu, beberapa daftar ancaman juga mengacu pada Standar ISO 27005 : 2013.

Tabel 4.5 Identifikasi ancaman pada aset kritis

Aset	Ancaman
Server	Kesalahan konfigurasi dan perawatan server
	Server lemot
	Terjadi kebocoran air AC di ruangan server
	AC di ruangan server mati/rusak
	Memori server penuh
	Overload user
	Server terserang *virus/malware*
	Hilangnya pasokan listrik
	Voltase yang bervariasi
	Debu dan korosi pada *hardware*
• *PC Unit* • *Printer* • UPS *(Unit Power Supply)* • *Hard Disk* • *Memory Programmer* • *Stabilizer* • AC *Split (Air Conditioning)* • Mesin Absensi (*Time Recorder*) • CCTV • IPTV	Perusakan peralatan/media
	Debu, korosi, pendingin, air
	Hilangnya pasokan listrik
	Korsleting
	Pencurian
	Maintanance yang kurang teratur
	Terserang virus
• *Router* • *Hub* • *Switch* • *Modem* • *Netware Interface External* • *Crimping Tool*	Penyadapan informasi penting melalui jaringan
	Kabel LAN digigit tikus
	Jaringan LAN lemot
	Remote Spying
	Kejenuhan sistem informasi
	Konektifitas internet menurun
	Koneksi terputus
	Celah masuknya *hacker*
	Kesalahan pengalamatan IP
Portable Generating Set	Perusakan peralatan/media
	Pencurian
	Maintanance yang kurang teratur
	Debu, korosi, air
• E-Kinerja • E-Budgeting • E-Monev • E-Surat • E-SPPD • E-Reminder • E-SIKD • E-LPPD • E-UMKM • E-Data (Satu Data) • E-Ruang Rapat • E-Pendekar Kelurahan	Aplikasi terserang *virus*
	Aplikasi *bug/error*
	Aplikasi terserang *hacker*
• *Database* • *Datafile* • *System Documentation* • *User Manual* • SOP	Redudansi data
	Data tidak lengkap
	Data hilang
	Data tidak ter-*back up*
	Data *corrupt*
	Pembobolan data
	Database penuh
Staf/pegawai *Data Center*	Kekurangan tenaga kerja
	SDM tidak memperhatikan prosedur yang ada
	Kesalahan penggunaan *(human*

	error)
	Penggunaan peralatan yang tidak sah
	Tidak ada batasan hak akses
	Share login
	Password pada PC diketahui orang lain
	Penyalahgunaan wewenang pada hak akses yang dimiliki
	Pemalsuan hak/wewenang
	Kesalahan *input/delete* data
	Penyangkalan atas tindakan
	Pengolahan data secara ilegal
	Kesalahan konfigurasi PC

F. Identifikasi Kerentanan pada Aset Kritis

Kerentanan adalah kondisi di mana tidak ada prosedur keamanan, kontrol teknik, kontrol fisik, atau kontrol lainnya yang dapat mencegah atau melindungi dari eksploitasi oleh ancaman. Kerentanan berkontribusi pada tingkat risiko yang lebih tinggi karena keberadaannya memungkinkan ancaman untuk menyebabkan kerugian atau gangguan pada sistem atau aset yang rentan tersebut.

Tabel 4.6 Identifikasi Kerentanan

Aset	Kerentanan
Server	Beban kerja server yang tinggi
	Pasokan listrik yang tidak stabil
	Pertambahan memori yang cepat dalam pemrosesan data
	Kerentanan terhadap voltase yang bervariasi
• *PC Unit* • *Printer* • UPS *(Unit Power Supply)* • *Hard Disk* • *Memory Programmer* • *Stabilizer*	Kurangnya pemeliharaan/ prosedur untuk pemeliharaan rumit
	Kurangnya skema pergantian secara berkala
	Kerentanan terhadap kelembaban, air, debu dan kotoran
	Kerentanan terhadap nilai informasi yang tersimpan pada PC
	Kerentanan terhadap voltase yang bervariasi
• AC *Split (Air Conditioning)* • Mesin Absensi (*Time Recorder*) • CCTV • IPTV	Kurangnya pemeliharaan/ prosedur untuk pemeliharaan rumit
	Kurangnya skema pergantian secara berkala
	Kerentanan terhadap kelembaban, air, debu dan kotoran
• *Router* • *Hub* • *Switch* • *Modem* • *Netware Interface External* • *Crimping Tool*	Jalur komunikasi yang tidak dilindungi
	Sambungan kabel yang buruk
	Arsitektur jaringan yang tidak aman
	Ketahanan *routing* yang tidak cukup
	Kualitas jaringan yang kurang baik
	Peletakan kabel yang sembarangan
	Tidak ada pelindung kabel
Portable Generating Set	Kurangnya pemeliharaan/ prosedur untuk pemeliharaan rumit
• E-Kinerja	Tidak ada atau tidak cukup pengujian
• E-Budgeting • E-Monev • E-Surat • E-SPPD • E-Reminder • E-SIKD • E-LPPD • E-UMKM • E-Data (Satu Data) • E-Ruang Rapat • E-Pendekar Kelurahan	*(testing)* pada *software*
	Software yang digunakan usang/ tidak terkini
	Menerapkan program aplikasi untuk data yang salah dalam hal waktu
	Kurangnya dokumentasi *user manual* untuk aplikasi
	Kurangnya mekanisme identifikasi dan otentifikasi pengguna aplikasi
	Pengimplementasian *password* yang lemah atau sudah pernah digunakan sebelumnya
• *Database* • *Datafile* • *System Documentation* • *User Manual* • SOP	Terlalu banyak data yang di *input*
	Kurangnya salinan *back up*
	Data terlalu sering di *update*
	Data tidak di *update*
Staf/ pegawai *Data Center*	Absen atau ketidakhadiran dari staf/pegawai
	Pelatihan terkait teknologi informasi yang tidak cukup
	Pelatihan keamanan informasi yang tidak cukup
	Kurangnya kesadaran akan keamanan informasi
	Kurangnya mekanisme pemantauan atau bekerja tanpa pengawasan
	Kurangnya kebijakan untuk penggunaan yang benar dan tepat atas media komunikasi

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil dan pembahasan penelitian, berikut merupakan beberapa kesimpulan yang dapat diambil :

a. Proses penilaian risiko terhadap aset layanan teknologi informasi pada Dinas Komunikasi dan Informatika Kota Madiun dilakukan dikategorikan dalam beberapa level penilaian risiko, yaitu *very* low (1 risiko dengan nilai RPN 16) , *low* (mempunyai 2 risiko dengan nilai RPN 30 dan 56), *high* (mempunyai 2 risiko dengan nilai RPN 84 dan 96).

b. Proses penyusunan rekomendasi SOP *(Standard Operating Procedure)* yang dilakukan sebagai bentuk mitigasi risiko berdasarkan pemetaan referensi standar kontrol/Annex A ISO 27001 : 2013 dan ISO 27005 : 2013 oleh penulis dan mendapatkan kesimpulan SOP yang sudah baik sejumlah 35 dimana prosedur yang sudah ada pada instansi tersebut tidak perlu adanya perbaikan, SOP yang

perlu perbaikan sejumlah 1 dimana prosedur tersebut telah diperbaiki pada bagian alur *flowchart* pada proses penanganan insiden, dan SOP yang harus dibuat dalam rangka memenuhi ISO 27001 : 2013 dan ISO 27005 : 2013 berjumlah 22.

B. Saran

Berdasarkan penelitian tugas akhir, disarankan menggunakan hasil penelitian sebagai rekomendasi untuk penelitian analisis penilaian risiko keamanan informasi selanjutnya, mengacu pada kontrol ISO 27001:2013 dan ISO 27005:2013 dengan metode FMEA sebagai acuan dasar dalam organisasi. Meskipun ada keterbatasan ruang lingkup dan informasi, penggunaan sebagian klausul dari ISO 27001:2013 diharapkan dapat memberikan kontribusi positif bagi pengembangan keamanan informasi..

UCAPAN TERIMA KASIH

Penulis ingin mengungkapkan rasa syukur kepada Tuhan YME dan terima kasih yang tulus kepada semua pihak yang telah berperan selama proses penyelesaian penelitian ini.

REFERENSI

[1] S. M. C. R. C. Hery, Manajemen Risiko Bisnis, Jakarta: PT Grasindo, 2019.

[2] L. J. Susilo and V. R. Kaho, Manajemen Risiko Panduan untuk Risk Leaders dan Risk Practitioners ISO 31000 : 2018, Jakarta: PT Grasindo, 2018.

[3] K. H. Dewantara, "Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan Standar ISO 27001 : 2005 dan ISO 27002 : 2013 Menggunakan Metode FMEA (Studi Kasus : ISNET)," *RepositoryITS*, 2016.

[4] I. S. I. 27001, ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements, 2013-11 ed., 2013.

[5] S. Riyanarto, Sistem Manajemen Keamanan Informasi : Berbasis ISO 27001, Surabaya: ITS Press, 2009.

[6] W. A. Pratiwi, "Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 Pada Kominfo Jawa Timur," *Stikom Surabaya*, p. 7, 2019.

[7] I. S. I. 27002, Information Technology - Security Techniques - Code of Practice for Information Security Management, 2013-10-01, 2013.

[8] D. Ikasari, "Perancangan Tata Kelola Keamanan Informasi Berdasarkan Information Security Management System (ISMS) ISO/IEc 27001:2005 Untuk Pengelolaan Data Migas yang Dikelola Oleh Pihak Ketiga : Studi Kasus Pusat Data dan Teknologi Informasi Energi dan Sumber Daya Mi," *Fasilkom UI*, 2015.

[9] I. S. I. 27005, Information Technology - Security Techniques - Information Security Risk Management, 2011 - 06 01 ed., 2013.

[10] I. 2. TechnicalGuide, FAIR - ISO/IEC 27005 Cookbook, The Open Group, 2010.

[11] F. Andreani, G. Winata and E. Halim, "Gap Analysis of Traveloka.Com: Hotel Consumers' Expectations and Preceptions of The Website," *ISSN 1411-1438*, 2018.

[12] H. Afandi and A. Darmawan, "Audit Keamanan Informasi Menggunakan ISO 27002 Pada Data Center PT. Gigipatra Multimedia," *ISSN:2442-5567*, 2015.

[13] I. Y. Ikhwana, R. R. Saedudin and D. B. Rahmad, "Implementation and Assessment of Risk on Application at PT. XYZ Using Cobit 5 Framework," *ISSN : 2355-9365*, 2018.

[14] F. I. S. Yudha and R. E. Gunadhi, "Risk Assessment Pada Manajemen Risiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management," *ISSN : 2302-7339*, 2016.

[15] R. Fauzi, "Implementasi Awal Sistem Manajemen Keamanan Informasi Pada UKM Menggunakan Kontrol ISO/IEC 27002," *DOI : 10.31544*, 2018.

[16] M. Azizah, "Pemilihan Metode Risk Assessment Pada UPT-TIK di Perguruan Tinggi Menggunakan Metode AHP (Analytical Hierarchy Process)," 2019.

[17] I. Meriah and L. B. A. Rabai, "Comparative Study of Ontologies Based ISO 27000 Series Security Standard," *Procedia Computer Science 160 (2019) 85-92*, 2019.

[18] H. Bahtit and B. Regragui, "Risk Management for ISO 27005 Decision Support," *ISSN : 2319-8753*, 2013.

[19] E. Kaban and N. Legowo, "Audit Information SYstem Risk Management Using ISO 27001 Framework at Private Bank," *ISSN : 1992-8645*, 2018.

[20] W. Apriani and A. Sasongko, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 : 2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus : Diskominfo Kota Sukabumi)," *ISSN : 2088-5407*, 2018.

[21] A. Yulianti, C. Rudianto and A. F. Wijaya, "Analisis dan Perancangan Tata Kelola Persandian Pengamanan Informasi Menggunakna Standar ISO 27001 : 2013 (Studi Kasus di Diskominfo Kota Salatiga)," *ISSN:2460-6839*, 2018.

[22] I. G. N. N. Bagiarta, "Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005," *Jurnal Teknologi Informasi ESIT*, 2012.

[23] Y. C. Yuze, Y. Priyadi and C. , "Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 : 2013 Serta Rekomendasi Model SIstem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi," *DOI: 10.21456*, 2016.

[24] B. L. Maheresmi, F. A. Muqtadiroh and B. C. Hidayanto, "Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave dan Kontrol ISO 27001 Pada Dishub Kominfo Kabupaten Tulungagung," *Seminar Nasional Sistem Informasi Indonesia*, 2016.

[25] S. Salahuddin, A. Ambarwati and M. N. Al Azam, "Identifikasi Risiko Keamanan Informasi Menggunakan ISO 27005 Pada Sebuah Perguruan Tinggi Swasta di Surabaya," *Universitas Narotama*.