CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 2, November 2023, hlm. 76-82

Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi

Moh. Abdul Fattah Ys[1], Bita Parga Zen[2], Dewi Endah Wasitarini[3]

[1,2]Institut Teknologi Telkom Purwokerto
[3]Perpustakaan Nasional RI
Email: [1]19103093@ittelkom-pwt.ac.id, [2]bita@ittelkom-pwt.ac.id, [3]dewi_wasitarini@perpusnas.go.id

Abstrak

Perpustakaan Nasional RI (Perpusnas) merupakan sebuah institusi yang menyimpan dan mengelola informasi dan pengetahuan nasional, harus memastikan bahwa teknologi informasi yang digunakan dalam operasinya aman dan terlindungi dari serangan siber dan ancaman lainnya. Saat ini manajemen risiko tata kelola teknologi informasi (TI) pada Perpusnas belum diterapkan seperti Standar ISO 27001 tujuan dari penelitian ini adalah menyusun dampak risiko yang ada di Perpustakaan Nasional RI menggunakan standar ISO 27001. Penelitian ini mengadopsi pendekatan kualitatif dan data diperoleh melalui wawancara dengan Ketua Tim Audit Perpusnas yang terlibat dalam manajemen TI. Hasil dari penelitian adalah menemukan beberapa risiko yang masih belum terbaiki. Yang saya temukan diantara adalah atap ruangan yang rusak tidak diperbaiki, beberapa aset yang tidak teridentifikasi, pegawai yang merangkap tugas, dan kekurangannya pegawai. peneliti berharap dengan adanya penelitian ini pihak perpusnas segera diperbaiki untuk pelayanan yang lebih bagus kembali.

Kata kunci: ISMS, ISO 27001, Perpustakaan Nasional RI

Risk Management Of Information Technology Governance Using Iso 27001 Standard In The National Library Of The Republic Of Indonesia

Abstract

The National Library of Indonesia (Perpusnas) is an institution that stores and manages national information and knowledge, must ensure that the information technology used in its operations is safe and protected from cyber attacks and other threats. Currently, information technology (IT) governance risk management at the National Library has not been implemented according to the ISO 27001 standard. The purpose of this research is to compile the impact of risks that exist in the National Library of Indonesia using the ISO 27001 standard. This study adopted a qualitative approach and the data was obtained through interviews with the chairman. National Library of Indonesia Audit Team involved in IT management. The result of the research is to find some risks that are still not resolved. Researcher find that among them was the damaged roof of the room that was not repaired, several unidentified assets, employees who had multiple tasks, and a shortage of employees With this research, ideally, the National Library of Indonesia will immediately improve it for better service again.

***Keywords**: ISMS, ISO 27001, RI National Library*

1. PENDAHULUAN

Perpustakaan Nasional merupakan sebuah institusi pemerintah yang tidak terafiliasi dengan departemen lain yang bertugas dalam konteks perpustakaan, perannya mencakup sebagai perpustakaan yang mendukung pengembangan, perpustakaan yang menyediakan sumber referensi, perpustakaan yang menerima simpanan koleksi, perpustakaan yang fokus pada penelitian, perpustakaan yang berfokus pada pelestarian, dan sebagai pusat jaringan perpustakaan dan berlokasi di pusat pemerintahan negara. Perpustakaan Nasional Republik Indonesia terletak di Jl.Medan Merdeka Selatan No.11, Jakarta, Indonesia(Jumino and Mu'alifah, 2022).

Pada era globalisasi saat ini, beberapa standar keamanan yang ada dapat digunakan sebagai metode penelitian, salah satunya adalah penggunaan metode standar keamanan ISO 27034:2014 untuk investigasi smart router xiaomi guna mengekstra data bukti digital yang kelak dapat digunakan untuk proses penegakan hukum(Hariyadi et al., 2021). Standarisasi keamanan tersebut memiliki keterkaitan antara proses dengan sistem informasi sangat erat. Sistem informasi menjadi media untuk mendukung kebutuhan proses di suatu organisasi dalam mengelola data. Teknologi bermanfaat bagi manusia

dari berbagai aspek(Syafnel, Darmawan and Mulyana, 2019). Teknologi sangat penting bagi kemajuan kita karena sejalan dengan perkembangan ilmu pengetahuan. Pada masa digitalisasi ini, teknologi informasi dapat digunakan dalam berbagai bidang, termasuk kedokteran, pendidikan, manajemen, dan lainnya. Hal ini menunjukkan bahwa informasi yang mudah diakses, cepat, dan valid sangat diperlukan dalam berbagai bidang(Malinda, Rani and Mardiani, n.d.).

Sistem informasi juga memiliki berbagai risiko seperti gangguan pasokan listrik, kesalahan manusia, pencurian data oleh peretas, kerusakan sistem akibat serangan virus, dan lainnya. Untuk mengurangi risiko, diperlukan praktik tata kelola risiko yang baik dan efektif. Kemampuan untuk mengatasi risiko yang telah terjadi, meminimalisir risiko potensial yang mungkin muncul, dan pengaturan yang efektif dari tata kelola risiko dapat dicapai melalui manajemen risiko(Setiawan et al., 2021).

Metode yang digunakan oleh berdasarkan iso 27001. Identifikasi masalahnya adalah Tingkat pematangan penerapan manajemen risiko di perpusnas indeksnya rendah. Tujuan penelitian ini adalah untuk Perancangan Manajemen Risiko Keamanan Informasi yang ada di Perpustakaan Nasional RI mengadopsi standar ISO 27001. Manfaat dari penelitian ini adala Mempermudah Tim Audit Internal dan Sistem Manajemen Keamanan Informasi (SMKI) Perpustakaan Nasional RI untuk mengetahui dampak risiko jika tidak ditangani dengan baik dan tepat, Meningkatkan tingkat keamanan untuk tahun selanjutnya, Manajemen Risiko dokumen hasil penelitian memiliki peran penting sebagai panduan bagi organisasi dalam mengurangi risiko melalui penyusunan langkah-langkah mitigasi.

2. TINJAUAN PUSTAKA

2.1. Manajemen Risiko

Manajemen risiko didefinisikan sebagai keahlian seorang manajer dalam mengatur fluktuasi pendapatan dengan mengurangi tingkat kerugian yang terjadi dan disebabkan dengan mempertimbangkan keputusan yang diambil dalam kondisi yang tidak melibatkan kepastian. Prinsip-prinsip dasar dalam manajemen risiko yang dapat dipahami oleh manajemen perusahaan meliputi bahwa manajemen risiko bukan semata-mata metode yang digunakan juga adalah strategi yang dapat diimplementasikan pada berbagai sektor industri(Handayani et al., 2018).

2.2. Indeks Keamanan Informasi (KAMI) tools SMKI

Indeks KAMI adalah sebuah indeks yang instrumen penilaian yang digunakan untuk mengukur tingkat kesiapan dapat dijelaskan sebagai keamanan informasi di instansi pemerintah. Instrumen evaluasi ini dirancang untuk mengevaluasi kematangan atau efektivitas perlindungan yang telah diterapkan, bukan untuk memberikan evaluasi kualitatif atas kondisi persiapan (kecukupan dan kesiapan) kerangka kerja keamanan informasi yang dimiliki pimpinan perusahaan. Evaluasi dilakukan terhadap berbagai aspek yang menjadi fokus penerapan keamanan informasi dengan cakupan pembahasan yang mencakup semua aspek keamanan yang telah ditetapkan oleh standar SNI ISO/IEC 27001(Sundari and Wella, 2021).

2.3. ISO 27001:2013

Menurut Sarno (2009), standar ISO/IEC 27001:2013 adalah suatu standar sistem manajemen keamanan informasi yang memberikan panduan secara umum mengenai prosedur perusahaan yang harus dilakukan dalam proses evaluasi, implementasi, dan pengendalian keamanan informasi berdasarkan praktik terbaik dalam pengendalian perlindungan informasi(Nurfadilah, Putra and Rachmadi, 2020).

Standar tersebut mengatur persyaratan yang harus dipenuhi dalam menetapkan, menerapkan, menjaga, dan terus-menerus memperbaiki Sistem Manajemen Keamanan Informasi (SMKI) di suatu perusahaan dan organisasi. Selain itu, memenuhi persyaratan untuk mengevaluasi dan menangani kebutuhan akan keamanan informasi yang penyesuaian sesuai dengan kebutuhan spesifik organisasi. Kriteria yang harus dipenuhi tercantum di standar SMKI. Pada standar ini memiliki sifat yang bersifat universal dan dapat diadopsi oleh berbagai organisasi, dengan berbagai kategori, dimensi, dan karakteristik. Tidak ada pengecualian yang dapat dibuat terhadap setiap persyaratan yang terdapat dalam Klausul 5 hingga 18 jika organisasi ingin menyatakan kesesuaian dengan standar ini(Badan Standarisasi Nasional, 2014).

Gambar 1. Kerangka Keamanan Informasi

ISO 27001 terdiri dari 14 klausul (clause) yang meliputi (Humphreys, 2016):

a. A.5 Kebijakan keamanan informasi : Untuk memberikan panduan implementasi dan bantuan

manajemen dalam mengimplementasikan pengamanan informasi yang sesuai dengan persyaratan konteks bisnis, regulasi, dan kepatuhan hukum yang berlaku.

b. A.6 Organisasi keamanan informasi : Untuk menciptakan struktur manajemen yang memberikan kerangka kerja dalam mengontrol dan memulai pelaksanaan serta pengoperasian keamanan informasi di dalam organisasi.
c. A.7 Keamanan sumber daya manusia : Untuk memastikan bahwa staf dan pihak kontrak memiliki pemahaman yang jelas tentang kewajiban mereka dan mematuhi posisi yang telah ditetapkan untuk individu-individu tersebut.
d. A. 8 Manajemen aset : Untuk mengenali Harta kekayaan perusahaan dan sumber daya organisasi dan menetapkan Tanggung jawab yang tepat dalam melindungi aset tersebut.
e. A. 9 Kendali akses : Mengatur akses dengan batasan yang ditetapkan ke data dan infrastruktur pengolahan data.
f. A. 10 Kriptografi : Untuk memastikan penerapan yang tepat dan efektif dalam penggunaan kriptografi dalam menjaga privasi, otentikasi, dan keutuhan informasi.
g. A. 11 Keamanan fisik dan lingkungan : Untuk menghindari upaya akses fisik yang tidak sah, kerusakan, atau gangguan terhadap data dan infrastruktur pengolahan data perusahaan.
h. A. 12 Keamanan operasi : Agar memastikan bahwa pengoperasian fasilitas pemrosesan informasi dilakukan dengan tepat dan dalam keadaan yang terjamin atau terlindungi.
i. A. 13 Keamanan komunikasi : Agar memastikan keamanan data yang berada dalam jaringan dan fasilitas pendukung pengolahan data yang dikumpulkan.
j. A. 14 Akuisisi, pengembangan dan perawatan sistem : Agar memastikan keamanan informasi menjadi komponen penting dalam keseluruhan tahapan sistem informasi. Hal ini juga mencakup kebutuhan bagi sistem informasi yang memberikan layanan melalui jaringan publik.
k. A. 15 Hubungan pemasok : Untuk menjamin keamanan dan perlindungan dari harta kekayaan organisasi yang mampu dijangkau oleh penyedia.
l. A. 16 Manajemen insiden keamanan informasi : Untuk menjamin pendekatan yang seragam dan efisien dalam menajemen kejadian keamanan informasi, termasuk proses komunikasi terkait tentang Peristiwa dan kerentanan keamanan yang terkait.
m. A. 17 Aspek keamanan informasi dari manajemen keberlangsungan bisnis : Kontinuitas keamanan informasi harus dijaga dan ditanamkan dalam kerangka manajemen keberlangsungan bisnis perusahaan terkait.
n. A. 18 Kesesuaian : Untuk mencegah pelanggaran terhadap ketentuan hukum, peraturan, atau regulasi ketentuan kewajiban kontraktual. Berkaitan dengan perlindungan kebutuhan keamanan informasi dan persyaratan terkait lainnya.

Setiap klausul dalam ISO 27001 memiliki persyaratan yang diharuskan terpenuhi oleh organisasi harus memastikan perlindungan informasi yang efektif. Organisasi harus mengevaluasi dan mengelola risiko keamanan informasi, mengimplementasikan kontrol keamanan yang sesuai, dan secara terus-menerus meningkatkan sistem manajemen keamanan informasi mereka untuk memenuhi persyaratan standar(Rutanaji, Kusumawardani and Winarno, 2018).

Dari 14 Klausul diatas peneliti menggunakan, Klausul 6 Organisasi keamanan informasi pada ISO 27001 dikarenakan di klausul tersebut menjelaskan tentang proses risk assessment. Klausul ini menjelaskan bahwa organisasi harus mengevaluasi risiko keamanan informasi yang mungkin timbul dan mengambil tindakan yang sesuai untuk mengelola dan mengurangi risiko tersebut. Klausul ini juga menjelaskan bahwa organisasi harus mengevaluasi risiko secara berkala dan melakukan tindakan yang sesuai digunakan mengatasi risiko yang muncul dari perubahan lingkungan operasional atau perubahan dalam sistem, aplikasi atau data(Pratiwi, 2019).

3. METODOLOGI

3.1. Subjek dan Objek Penelitian

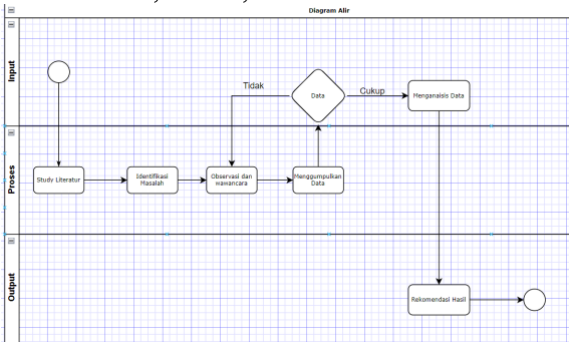
Berdasarkan penelitian, peneliti melakukan :

1. Subjek Penelitian

Subjek dari penelitian ini adalah Perpustakaan Nasional Republik Indonesia, yang berlokasi di Jalan Medan Merdeka Selatan No.11, Jakarta, Indonesia.

2. Objek Penelitian

Objek penelitian ini adalah Pusat Data Center dan Informasi Perpustakaan Nasional Republik Indonesia yang berada di Jalan Medan Merdeka Selatan No.11, Jakarta, Indonesia.



Gambar 2. Diagram Alir Penelitian

Gambar 2 di atas merupakan gambar mengenai tahapan alir penelitian, tahapan alur penelitian tersebut meliputi Studi Literatur, Identifikasi Masalah, Observasi dan Wawancara, Menggumpulkan Data, Mengelompokkan Data dan

Menganalisis Data, Rekomendasi Hasil, Kesimpulan dan rekomendasi.

,

Tahapan masing-masing alur penelitian :

A. Study Literatur

Studi literatur melibatkan pencarian referensi teori yang sama dengan masalah yang akan diteliti oleh peneliti yang berada di Perpustakaan Nasional RI. Khususnya Tentang Manajemen Risiko Tata Kelola Sistem Informasi Menggunakan ISO 27001. Melakukan studi literatur akan membantu dalam proses pembuatan penelitian dan menyelesaikan masalah yang ada.

B. Identifikasi Masalah

Tahap penelitian ini dilakukan proses wawancara dengan Ketua Tim audit Perpustakaan Nasional RI bagian Pusat Data dan Informasi yang mempunyai peran penting sebagai Ketua tim di Pusat Data dan Informasi, Dari adanya wawancara tersebut dapat ditemukan permasalahan pada internal yaitu indeks Sistem Pemerintahan Berbasis Elektronik (SPBE) masih di bawah indeks.

C. Observasi dan wawancara

Observasi dilakukan melalui pengamatan langsung di lokasi Perpustakaan Nasional Republik Indonesia yang berada di Jalan Medan Merdeka Selatan No.11, Jakarta, Indonesia. Untuk melihat bagaimana sistemnya yang masih di bawah Indeks, Observasi dilakukan pada tanggal 19 Desember 2022. Selanjutnya Peneliti melakukan wawancara kepada Tim Audit Pusat Data dan Informasi yaitu Ibu Dewi Endah Wasitarini, S.Kom., MT pada tanggal 19 Desember 2022.

D. Menggumpulkan Data

Proses penghimpunan data yang dibutuhkan untuk memenuhi study ini dilakukan dengan proses melakukan wawancara dengan pihak yang terkait yaitu unit Audit Perpusnas. Dari temuan dari sesi wawancara tersebut didapatkan dokumen Penilaian Indeks KAMI.

3.2. Mengidentifikasi Data Sesuai Standar Keamanan ISO 27001

Tahap ini penulis mengidentifikasi data yang di peroleh dari tahap sebelumnya untuk di identifikasi apakah sudah sesuai standar ISO 27001 atau tidak. Dalam Menyusun Standart ISO 27001 terdapat beberapa langkah berikut ini adalah penjelasan dari setiap langkah-langkah dalam menyusun ISO 27001 diantaranya yaitu :

1. Klausul 4 Bussiness Context ISO 27001

Dalam Menyusun Bussiness Context, Menagacu pada Bisnis proses yang ada pada setiap organisasi atau perusahaan. Bussiness Context mencakup dokumen PEST (Politik,Ekonomi, Sosial dan Teknologi) dan dokumen SWOT (Strength, Weakness, Opportunity, Threat). Dokumen PEST sendiri merupakan dokumen untuk mengidentifikasi isu eksternal organisasi atau perusahaan sedangkan dokumen SWOT digunakan untuk mengidentifikasi Isu internal organisasi atau instansi.

2. Klausul 6 Planning ISO 27001

Dalam menyusun klausul 6 ini terdapat Beberapa langkah yang terdiri dari pembuatan dokumen Risk Register, Risk Assessment, Worksheet, Risk Treatment Plan, Treat and Vulneraabilities Checklist. Sedangkan dalam menyusun manajemen risiko terdapat beberapa tahapan lagi diantaranya yaitu identifikasi aset, identifikasi risiko (Threat), identifikasi kerentanan (vurlnerability), identifikasi dampak, identifikasi kemungkinan (Likelihood), dan identifikasi kontrol sistem.

3.3. Mengelompokkan Data dan Menganalisis Data

Tahap ini penulis Mengelompokkan Data yang di peroleh dari Penggumpulan Data untuk di analisis kedalam kausul Manajemen Risiko Tata Kelola Informasi dengan Menggunakan Standar ISO 27001. Didalamnya terdapat seperti dibawah ini : Risk Register, Risk Assessment, Worksheet, Risk Treatment Plan, Treat and Vulneraabilities Checklist. Sedangkan dalam menyusun manajemen risiko terdapat beberapa tahapan lagi diantaranya yaitu identifikasi aset, identifikasi risiko (Threat), identifikasi kerentanan (vurlnerability), identifikasi dampak, identifikasi kemungkinan (Likelihood), dan identifikasi kontrol sistem.

3.4. Rekomendasi Hasil

Adapun rekomendasi hasilnya adalah aset teridentifikasi memiliki risiko tertentu yang tinggi. Salah satunya adalah risiko yang terkait dengan server yang tinggi disebabkan keberadaan ancaman kebakaran dan serangan hacker merupakan faktor yang masih menjadi penyebab utama belum adanya kekurangan dalam sistem pendeteksi dini kebakaran dan kurangnya pemantauan dalam pengelolaan informasi. Sedangkan untuk semua server belum tersedia kembali server back up. Dan untuk para pegawainya diharapkan sesuai dengan tugasnya masing-masing dan tidak merangkap tugas ditakutkan ada kendala yang lain dan tidak sesuai dengan Standar ISO 27001

4. PEMBAHASAN

4.1. Pengumpulan Data

Proses penghimpunan data yang dibutuhkan untuk memenuhi study ini dilakukan dengan proses melakukan wawancara dengan pihak yang terkait yaitu unit Audit Perpusnas. Dari temuan dari sesi wawancara tersebut didapatkan dokumen Penilaian Indeks KAMI.

4.2. Menyusun Standar Sesuai ISO 27001

Dalam Menyusun Standart ISO 27001 terdapat beberapa langkah berikut ini adalah penjelasan dari setiap langkah-langkah dalam menyusun ISO 27001 diantaranya yaitu :

4.2.1. Klausul 4 Bussiness Context ISO 27001

Dalam Menyusun Bussiness Context, Mengacu pada Bisnis proses yang ada pada setiap organisasi atau perusahaan. Bussiness Context mencakup dokumen PEST (Politik,Ekonomi, Sosial dan Teknologi) dan dokumen SWOT (Strength, Weakness, Opportunity, Threat). Dokumen PEST sendiri merupakan dokumen untuk mengidentifikasi isu eksternal organisasi atau perusahaan sedangkan dokumen SWOT digunakan untuk mengidentifikasi Isu internal organisasi atau instansi. Untuk lebih jelasnya berikut isu Eksternal dan Internal di Perpustakaan Nasional RI :

1. Analisis Kasus Eksternal

Dalam penyusunan dan anilisis kasus Eksternal mengacu dokumen PEST(Political, Economic, Social, and Technological) yang merupakan dokumen sebagai alat bantu untuk mengidentifikasi tantangan eksternal yang dihadapi oleh sebuah organisasi atau perusahaan. Semua aspek yang mengarah kepada keamanan informasi akan dianalisis berdasarkan kategori isu politik, ekonomi, sosial, dan teknologi. Sehingga akan diketahui dampak yang akan terjadi dari isu tersebut terhadap organisasi atau perusahaan baik atau buruk. Berikut Tabel 4.1 yang menunjukan hasil dari analisis isu eksternal pada Perpustakaan Nasional RI.

2. Analisis Kasus Internal

Analisis Isu internal berbeda dengan analisis kasus eksternal, perbedaannya yaitu terdapat pada dokumen yang digunakan sebagai acuan. Analisis SWOT. Dalam melakukan analisis SWOT keamanan informasi Perpustakaan Nasioanl RI berfokus beberapa layanan diantaranya yaitu datacenter menajemen, dan layanan pengembangan aplikasi. Dari layanan tersebut dilakukan analisis terkait SWOT untuk mengetahui kelemahan yang ada di Perpustakaan Nasional RI.

3. Pihak-pihak Terkait

Stakeholder yang terlibat langsung dengan manajemen keamanan informasi, Yaitu : Masyarakat, Vendor, Industri, Pegawai dan karyawan

4. Ruang Lingkup

Skala penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan hasil wawancara dengan Ketua Tim Audit yaitu mencangkup seluruh yang ada di gedung Perpustakaan Nasional RI.

4.2.2. Klausul 6 Planning ISO 27001

Dalam menyusun klausul 6 ini terdapat Beberapa langkah yang terdiri dari pembuatan dokumen Risk Register, Risk Assessment, Worksheet, Risk Treatment Plan, Treat and Vulneraabilities Checklist. Sedangkan dalam menyusun manajemen risiko terdapat beberapa tahapan lagi diantaranya yaitu identifikasi aset, identifikasi risiko (Threat), identifikasi kerentanan (vurlnerability), identifikasi dampak, identifikasi kemungkinan (Likelihood), dan identifikasi kontrol sistem.

4.3. Risk Register

A. Identifikasi Aset

Langkah pertama dalam mengembangkan manajemen risiko adalah mengidentifikasi aset yang terlibat. Aset yang terlibat adalah Website perpusnas,Website OPAC, Website Onesearch, Website K-OL, dan Website ISBN.

B. Menghitung Nilai Aset

Langkah ini dilakukan setelah melakukan identifikasi Aset yang ada di Perpustakaan Nasional RI.

C. Identifikasi Risiko

Identifikasi Risiko merupakan tahapan kedua dalam pengembangan manajemen risiko.

D. Identifikasi Penilaian Kemungkinan

Identifikasi dilakukan untuk mengevaluasi potensi ancaman yang dapat terjadi akan dilakukan dengan mempertimbangkan adanya ancaman dan kerentanan. Evaluasi ini dapat didasarkan pada sejarah ancaman sebelumnya yang pernah terjadi. Untuk menentukan nilai kemungkinan mengacu pada matriks risiko berikut :

Nilai Aset = NC + NI + NA (1)

Keterangan :

NC : Nilai Convidenity(Kerahasiaan)

NI : Nilai Integrity (Keutuhan)

NA : Nilai Availability (Ketersediaan)

Tabel 1. 2 Matrik 5x5 Analisis Risiko

		Dampak / Akibat				
Kemungkinan		1	2	3	4	5
	1	Paling rendah	Paling rendah	Paling rendah	Paling rendah	Paling rendah

	2	Paling rendah	Paling rendah	Rendah	Rendah	Rendah
	3	Paling rendah	Rendah	Rendah	Sedang	Sedang
	4	Paling rendah	Rendah	Sedang	Atas	Paling atas
	5	Paling rendah	Rendah	Sedang	Paling atas	Paling atas

Tabel 2. 3 Range Nilai Risiko

Level	Scor	Keterangan
5	20-25	Paling atas
4	16-19	Atas
3	12-15	Sedang
2	6-11	Rendah
1	1-5	Paling rendah

E. Mengidentifikasi Nilai Dampak Risiko

Tahap nilai dampak risiko adalah tahap untuk menentukan seberapa besar dampak yang diakibatkan oleh ancaman dan kerentanan. Identifikasi nilai dampak risiko hampir sama dengan tahap identifikasi nilai kemungkinan yaitu dengan menggunakan matrix 5x5.

F. Perhitungan Nilai Risiko

Tahap ini merupakan langkah untuk menentukan nilai risiko yang disebabkan oleh adanya ancaman dan kerentanan. Tujuan menghitung nilai risiko adalah untuk mengetahui tingkat risiko yang ada pada masing-masing aset sehingga lebih mudah dalam menentukan prioritas penanganan risiko. Untuk menghitung nilai risiko adalah dengan cara mengkalikan nilai dampak dan kemungkinan yang sudah diidentifikasi sebelumnya.

G. Kontrol Sistem

Kontrol sistem adalah tahap yang dilakukan untuk mendokumentasikan semua aset-aset yang ada di Perpustakaan Nasional RI. Untuk mengontrol keadaan aset tersebut dalam keadaan baik maupun tidak supaya proses bisnis dapat berjalan dengan baik. Kontrol yang diberikan disesuaikan dengan ancaman yang mungkin terjadi pada aset yang telah diidentifikasi.

H. Perhitungan Nilai Sisa Risiko

Pada tahap ini adalah melakukan perhitungan nilai sisa risiko, nilai suatu risiko didapatkan ketika diorganisasi yaitu Perpusnas sudah menerapkan kontrol untuk menangani atau mengurangi terjadinya risiko yang ada pada masing-masing aset.

I. Mengidentifikasi Level Risiko

Mengidentifikasi level risiko bertujuan untuk mengetahui tingkat risiko yang didapatkan dari adanya dampak dan kemungkinan yang akan terjadi disuatu perusahaan atau organisasi.

J. Mengidentifikasi Penanganan Risiko

Tahap ini Tujuan utamanya adalah untuk menerima risiko dari setiap aset yang ada. Identifikasi Penanganan Risiko dilakukan untuk menentukan tindakan penanganan risiko yang sesuai dengan kriteria penanganan risiko, seperti penerimaan risiko (*risk acceptance*), pengurangan risiko (*risk reduction*), penolakan risiko (*risk avoidance*), dan transfer risiko (*risk transfer*). Jika di website Perpusnas respon websitenya lama atau bahkan tidak bisa terbuka maka penangan risikonya adalah *risk acceptance.*

K. Kontrol Pengendalian Risiko

Setelah menentukan penanganan risiko tahap selanjutnya yaitu menentukan kontrol keamanan pada masing-masing aset yang memiliki level risiko tinggi. Dalam menentukan kontrol objektif dan kontrol keamanan dilakukan sesuai dengan ancaman dan kerentanan pada masing-masing aset. Contohnya adalah di server, jika server mengalami kebakaran maka risikonya adalah perangkat tidak berfungsi secara maksimal atau bahkan tidak berfungsi kembali untuk kontrol keamanan adalah di A.11.1.4 Melindungi dari ancama Eksternal dan lingkungan.

5. KESIMPULAN

Dengan adanya ISO 27001 memberikan kerangka kerja yang terstruktur untuk Perpusnas dalam mengelola risiko terkait keamanan informasi. termasuk proses identifikasi risiko, penilaian risiko, pemilihan kontrol keamanan, dan pemantauan dan pengukuran kinerja.

Identifikasi dan Evaluasi Risiko: ISO 27001 membantu organisasi Perpusnas dalam mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan keamanan informasi. Ini mencakup ancaman terhadap kerahasiaan, integritas, dan ketersediaan informasi. dengan demikian, kontribusi utamanya adalah memperkuat disiplin ilmu manajemen risiko dalam konteks IT.

Berdasarkan analisis data, beberapa aset di Perpusnas teridentifikasi memiliki risiko tertentu yang tinggi. Salah satunya adalah risiko yang terkait dengan server yang tinggi disebabkan keberadaan ancaman kebakaran dan serangan *hacker* merupakan faktor yang masih menjadi penyebab utama belum adanya kekurangan dalam sistem pendeteksi dini kebakaran dan kurangnya pemantauan dalam pengelolaan informasi. Sedangkan untuk semua server belum tersedia kembali server back up.

DAFTAR PUSTAKA

Badan Standarisasi Nasional, 2014. Teknologi Informasi - Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (SNI ISO/IEC

27037:2014).

Handayani, N.U., Wibowo, M.A., Sari, D.P., Satria, Y. and Gifari, A.R., 2018. Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001. TEKNIK, 39(2), pp.78–85.

Hariyadi, D., Kusuma, M., Sholeh, A. and Fazlurrahman, 2021. Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework. [online] International Conference on Science and Engineering (ICSE-UIN-SUKA 2021). Atlantis Press. pp.143–147. https://doi.org/10.2991/aer.k.211222.023.

Humphreys, E., 2016. Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech house.

Jumino, J. and Mu'alifah, O.L., 2022. Peran Perpustakaan Nasional Republik Indonesia dalam Penyediaan Sumber Daya Informasi Elektronik sebagai Upaya Mengatasi Infodemi pada Masa Pandemi Covid-19. Anuva: Jurnal Kajian Budaya, Perpustakaan, dan Informasi, 6(2), pp.141–162.

Malinda, M., Rani, R. and Mardiani, M., n.d. Sistem Informasi Kecelakaan Kerja Peserta Pada PT TASPEN (Persero) Palembang Berbasis Website.

Nurfadilah, D.R., Putra, W.H.N. and Rachmadi, A., 2020. Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001: 2013 (Studi Kasus: Aplikasi E-Kinerja). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 4(9), pp.3014–3020.

Pratiwi, W.A., 2019. Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001: 2013 pada Kominfo Provinsi Jawa Timur. Institut Bisnis dan Informatika STIKOM, Surabaya.

Rutanaji, D., Kusumawardani, S.S. and Winarno, W.W., 2018. Penggunaan Kerangka Kerja SNI ISO/IEC 27001: 2013 untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI). Seminar Nasional GEOTIK 2018.

Setiawan, I., Sekarini, A.R., Waluyo, R. and Afiana, F.N., 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), pp.389–396.

Sundari, P. and Wella, W., 2021. SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR). Ultima InfoSys: Jurnal Ilmu Sistem Informasi, 12(1), pp.35–42.

Syafnel, M.Z., Darmawan, I. and Mulyana, R., 2019. Analisis dan Perancangan Tata Kelola Data sistem Pemerintahan Berbasis Elektronik Domain Master Data Management (MDM) pada Dama Dmbok V2 di Diskominfotik Kbb. eProceedings of Engineering, 6(2).