ANALISIS MANAJEMEN RISIKO PADA APLIKASI E-OFFICE YANG DIKELOLA OLEH PT TELKOM INDONESIA MENGGUNAKAN STANDAR ISO/IEC 27005:2018

ANALYSIS OF RISK MANAGEMENT IN E-OFFICE APPLICATION MANAGED BY PT TELKOM INDONESIA USING ISO/IEC 27005:2018 STANDARD

Syasya Sahira[1], Rokhman Fauzi[2], Iqbal Santosa[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]**syasyasahira@student.telkomuniversity.ac.id**, [2]**rokhmanfauzi@telkomunivesity.ac.id**,
[3]**iqbals@telkomuniversity.ac.id**

Abstrak

Informasi sebagai salah satu aset yang penting dan sangat berharga bagi perusahaan. Analisis manajemen risiko dilakukan untuk melindungi aset informasi yang terdapat disebuah aplikasi dari berbagai ancaman untuk minimalisir kebocoran data, pengunaan akses *user*, dan kesalahan pengembangan aplikasi selanjutnya. Pada penelitian ini, standar internasional ISO/IEC 27005 digunakan dalam melakukan manajemen risiko keamanan informasi di salah satu perusahaan yang merupakan penyedia jasa yang bergerak di bidang jasa layanan teknologi informasi dan komunikasi. Sesuai kondisi perusahaan saat ini, aplikasi masih dilakukan pengembangan dan belum pernah dilakukan analisis manajemen risiko pada aplikasi tersebut. Rekomendasi manajemen risiko menggunakan kontrol dari ISO/IEC 27002. Prioritas utama hasil analisis adalah penilaian risiko, penyusunan kebijakan dan prosedur.

Kata kunci: Manajemen Risiko, Aset TI, ISO/IEC 27005, ISO/IEC 27002, Keamanan Informasi.

Abstract

Information as one asset that is important and very valuable for the company. Risk management analysis is done to protect the information assets contained in an application from various threats to minimize data leakage, user access usage, and subsequent application development errors. In this study, International standard ISO/IEC 27005 is used in conducting information security risk management in one of the companies which is a provider of services engaged in the service of information technology and communications. According to the company's current condition, the application is still done development and has never done risk management analysis on the application. Risk management recommendations use controls from ISO/IEC 27002. The main priorities of the analysis are risk assessment, policy drafting and procedures.

Keyword: risk management, IT Asset, ISO/IEC 27005, ISO/IEC 27002, information security.

1. Pendahuluan

Perkembangan Sistem Informasi di era *digital* pada Lembaga Pemerintahan kini berkembang sangat pesat dan memberikan peluang pemerintah untuk membangun sistem aparatur negara dengan memanfaatkan Teknologi Informasi dan Komunikasi (TIK) melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Dengan adanya Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) merupakan kebijakan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya berbasis elektronik. Salah satu penerapan SPBE berperan penting di bidang persuratan untuk menyusun strategi kearsipan yang saling korespondensi dengan berbasis elektronik atau disebut *E-Office*.

Salah satu aplikasi untuk mendukung sistem pemerintah berbasis elektronik atau *E-Office* ialah Sistem Informasi Persuratan Terpadu (SIPT) yang di-*develop* oleh Telkom Indonesia. Proses bisnis pengiriman surat pada Sekretariat Kabinet sebelumnya masih menggunakan cara konvensional. melakukan tanda tangan pada kertas secara langsung, proses arsip surat masih dalam bentuk dokumen fisik, proses penyimpanan informasi surat didalam tumpukan file

sehingga menyulitkan untuk mencari surat yang ingin digunakan kembali. Maka dari itu diciptakannya aplikasi SIPT untuk mengubah proses konvensional menjadi digital. Namun dalam menciptakan aplikasi pasti ada kendala yang dialami, mulai dari eror saat mencoba penggunaan aplikasi, data pengiriman surat tidak tersimpan pada database dan web tidak bisa digunakan sementara karena adanya bug.

Aplikasi SIPT yang digunakan oleh Sekretariat Kabinet ini berisi data akun user, profil user dan file perusahaan dimana jika data tersebut terungkap ke publik, berubah, terhapus, tidak dapat diakses akan merugikan user sehingga diperlukan analisis manajemen risiko keamanan informasi yang sesuai standar ISO 27005 agar setiap risiko yang mungkin terjadi pada aplikasi SIPT dapat ditangani dengan baik, dan menjadi bahan evaluasi untuk pengembangan aplikasi SPBE lainnya.

2. Tinjauan Pustaka

2.1 Risiko

Menurut Kamus Besar Bahasa Indonesia, Risiko dapat diartikan sebagai akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Dengan kata lain risiko merupakan kemungkinan menderita kerugian karena kehilangannya sebagian atau seluruh modal. Risiko sendiri ditimbulkan karena adanya ketidakpastian [4].

Sedangkan dilihat dari risiko bisnis. Risiko merupakan peluang terjadinya ancaman atau serangan sehingga memberikan akibat atau dampak terganggunya proses bisnis pada suatu organisasi atau instansi atau bahkan menyebabkan gagalnya tujuan organisasi.

Untuk rumus risiko secara umum bisa dilihat gambar dibawah ini [5]:

Gambar 2.1 Rumus Risiko

Risiko ini dapat diatasi dengan menerapakn Kontrol TI. Ada 4 Kontrol TI yang dapat dilakukan, yaitu:

1) *Accept the Risk*
2) *Avoid the Risk*
3) *Transfer the Risk*
4) *Mitigate the Risk*

2.2 Manajemen Risiko

Manajemen risiko merupakan proses yang terdiri dari kegiatan mengindentifikasi, menganalisis dan melakukan penanganan dengan tujuan mengurangi dampak risiko pada proses bisnis organisasi[3]. Proses manajemen risiko keamanan informasi yang dilakukan pada penelitian ini menggunakan proses manajemen risiko yang terdapat di ISO 27005. Berikut ini adalah penjabaran dari masing-masing proses manajemen risiko keamanan informasi yang ada di ISO 27005. [6]

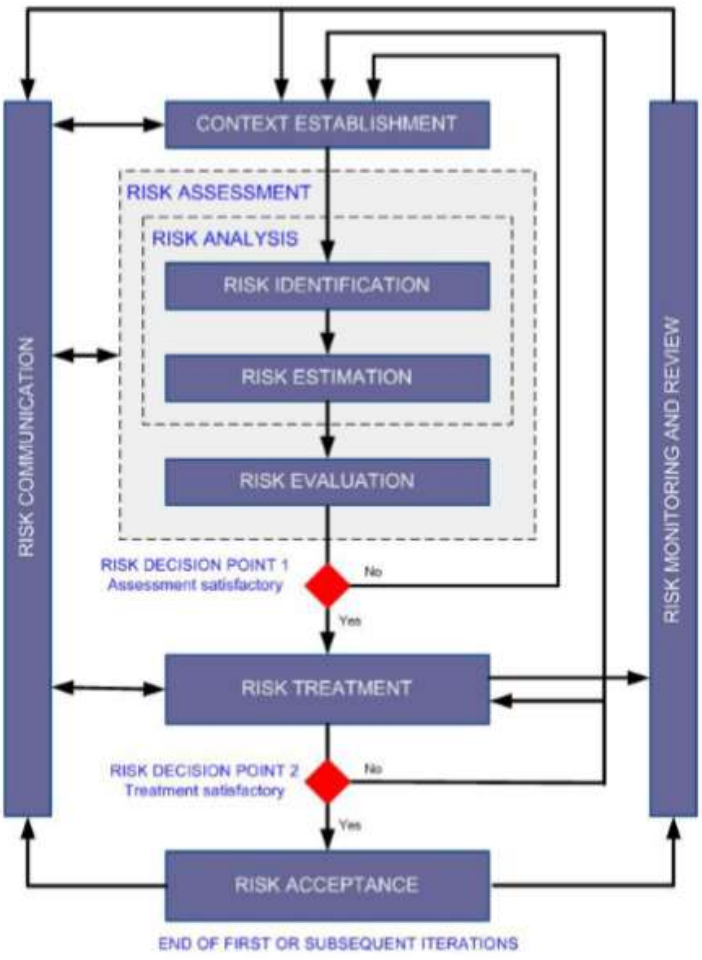
a. *Context Establishment*
   Penetapan konteks manajemen risiko keamanan informasi berisi mengenai kriteria dasar penilaian risiko, ruang lingkup dan batasan, dan organisasi manajemen risiko.
b. *Risk Assessment*
   Penilaian risiko terdiri dari kegiatan identifikasi aset, identifikasi ancaman, dan identifikasi kerentanan. Risiko yang telah teridentifikasi kemudian diurutkan sesuai nilai prioritas yang didapat dari matriks risiko.

c. *Risk Treatment*
Dalam rangka untuk mengurangi dampak atau kemungkinan dari risiko yang telah diidentifikasi, maka langkah selanjutnya yang harus dilakukan adalah menerapkan kontrol. Terkait proses penerapan kontrol, penelitian ini menggunakan proses mitigasi risiko yang terdapat di NIST SP 800-30. Adapun kontrol yang diterapkan dapat bersifat *preventive* atau *detective*.

d. *Risk Acceptance*
Proses untuk menerima risiko berdasarkan selera risiko dari pemilik risiko, baik dengan penetapan kontrol maupun tidak.

e. *Risk Communication*
Sharing informasi terkait risiko yang telah diidentifikasi, yang dilakukan oleh pemilik bisnis terhadap seluruh stakeholder yang memiliki kaitan dengan bisnis yang ada.

f. *Risk Monitoring and Review*
Kegiatan yang berkesinambungan untuk terus mengidentifikasi kerentanan, dan ancaman, yang dari waktu ke waktu mengalami perubahan. [7]



Gambar 2.2 Konsep Risiko ISO 27005:2018

2.2 Manajemen Aset Informasi

Manajemen aset berarti melakukan tanggung jawab terhadap aset yang dimiliki dengan mempertahankan dan melakukan perlindungan yang tepat untuk melindungi aset organisasi. Aset biasanya meliputi aset nonfisik dan informasi seperti sistem, database, dokumentasi, layanan, orang, dan berwujud seperti reputasi. Aset juga akan digunakan dalam penilaian risiko. Untuk setiap aset, kepemilikan aset harus ditetapkan dan harus diidentifikasi (ISO/IEC 27002, 2013).

Menurut Sutabri (2012:196), aset- aset yang dapat dimaksud dalam sistem informasi dapat dikategorikan sebagai berikut : personel, hardware, software, sistem software, data, fasilitas, penunjang.

2.3 Manajemen Keamanan Informasi

Menurut Cazemier et al. (2010:2), manajemen keamanan informasi adalah proses untuk memastikan bahwa informasi dan pengolahan informasi dapat diandalkan, terjaga kerahasiannya dan tersedia kapan dan untuk siapa bila dibutuhkan. Membatasi akses ke informasi dan pengolahan informasi kepada orang-orang yang berwenang dan sesuai fungsinya.

Sedangkan menurut ISO/IEC 27001:2013, "the information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed". Dari pengertian tersebut dapat dijelaskan bahwa sistem manajemen keamanan informasi melindungi kerahasiaan, integritas dan ketersediaan informasi 20 dengan menerapkan proses manajemen risiko dan memberikan kepercayaan kepada pihak terkait risiko yang memadai untuk dikelola.

Konsep utama ISMS untuk suatu organisasi adalah untuk merancang, menerapkan, dan memelihara suatu rangkaian terpadu proses dan sistem untuk secara efektif mengelola keamanan informasi dan menjamin kerahasiaan (***Confidentiality***), integritas (***Integrity***) dan ketersediaan (***Availability***) informasi [8].

2.4 ISO/IEC 27000 Series

Pada tahun 2005, ISO (International Organization for Standarization) bekerja sama dengan IEC (International Electronichal Comission) mengeluarkan standarisasi untuk Informatioan System Managemen Security (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) yang dikelompokkan dalam seri ISO/IEC 27000. Seri 27000 dari kemanan informasi dapat dilihat melalui tabel sebagai berikut [3]:

Table 2-0-1 ***ISO/ IEC 27000 Series***

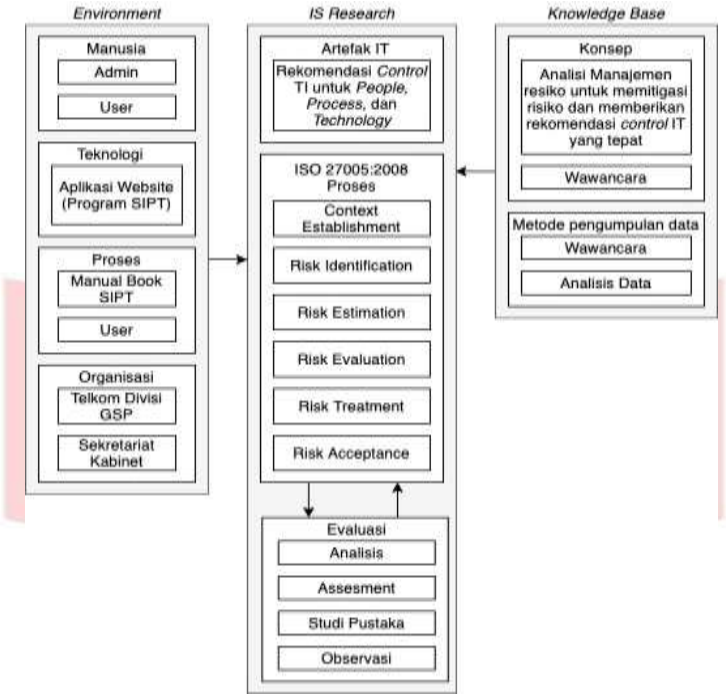
No.	*Series*	*Objective*
1.	*ISO/ IEC 27000:2009*	*ISMS Overview and Vocabularies*
2.	*ISO/ IEC 27001:2005*	*ISMS Requirements (revised BS 7799 Part 2: 200)*
3.	*ISO/ IEC 27002:2005*	*Code of Practice for Information Security Management, was ISO/ IEC 17799*
4.	*ISO/ IEC 27003:2009*	*ISMS Implementation Guidance*
5.	*ISO/ IEC 27004:2009*	*Information Security Management Measurement & Metrics*
6.	*ISO/ IEC 27005:2008*	*Information Security Risk Management*
7.	*ISO/ IEC TR 27008:2011*	*Guidelines for Auditors on Information*
8.	*ISO/ IEC 27031:2011*	*ICT Readiness for Business Continuity*

3. Metode Penelitian

3.1 Model Konseptual

Pada penelitian ini dimulai dengan pemahaman terlebih dahulu mengenai Telkom Indonesia, Sekretariat Kabinet, Aplikasi SIPT kemudian penentuan permasalahan yang terdapat pada Aplikasi SIPT yang menjadi latar belakang penelitian. Penelitian ini dilakukan berdasarkan kerangka kerja dari ISO 27005 tahun 2018.

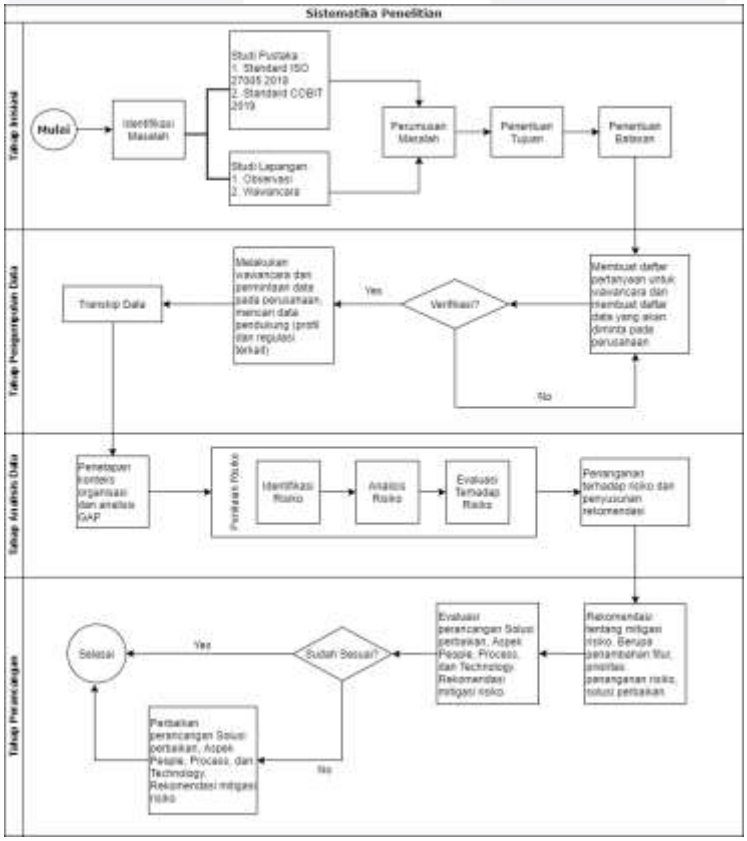
Pengumpulan data yang dilakukan menggunakan tahap wawancara dan studi pustaka. Hasil penelitian ini merupakan Rekomendasi tentang mitigasi risiko. Berupa rekomendasi penambahan fitur, prioritas penanganan risiko, solusi perbaikan mengenai aspek *people*, *process*, dan *technology*.



Gambar 3.1 Model Konseptual Hevner

3.2 Sistematika Penelitian

Sistematika penilitian menjelaskan alur penelitian dari awal penelitian hingga akhir penelitian sebagai tahapan dalam penyelesaian masalah yang ada. Disini menggunakan konsep ISO 27005:2008 yang memiliki 8 proses. Berikut merupakan *flow* dari sistematika penelitian:



Gambar 3.2 Sistematika Penelitian

Disini menjelaskan ada 4 tahapan pada sistematika penelitian. Berikut merupakan tahapan pada sitematika penelitian:

1) Tahap Inisiasi

Tahap ini kita mulai melakukan identifikasi mengenai masalah apa yang muncul, lalu ditentukan standarisasi untuk mengukur risiko tersebut menggunakan standar dan dengan cara seperti apa mengetahuinya.

2) Tahap Pengumpulan Data
Pada tahap ini pengumpulan data dilakukan pada tanggal 16 Mei 2019 sampai dengan 19 Juli 2019 Telkom Indonesia, Menara Multimedia Lt.12, Jakarta Pusat. Penelitian yang dilakukan membutuhkan data yang dapat berasal dari berbagai sumber yang dikumpulkan menggunakan beberapa teknik selama kegiatan penelitian berlangsung. Data yang digunakan yaitu data primer dan data sekunder.

3) Tahap Analisis Data
Data yang sudah terkumpul lalu kita lalukan analisis, dan pemetaan data berdasarkan penilaian risiko nya. Lalu, dibuatlah penangan risiko dan rekomendasinya.

4) Tahap Perancangan
Terakhir, ditahap perancangan ini dapt diberikan rekomendasi risiko nya yang sesuai dan solusi nya terkait aspek *people*, *process*, dan *technology* nya akan seperti apa. Jika masih gagal dalam penyesuaian rekomendasi, maka akan terus dilakukan rekomendasi dan evaluasi perancangannya.

4. Pembahasan

4.1 Manajemen Risiko

Pada proses ini dilakukan analisis manajemen risiko pada website SIPT, menggunakan konsep manrisk dari ISO 27005 tahun 2018. Tapi ditahap risk communication dan risk monitoring and review tidak dilakukan karena disini melakukan analisis atas penanganan yang sudah direkomendasikan untuk PT. Telkom Indonesia, Tbk dan Sekretariat Kabinet. Berikut merupakan hasil dari analisis yang dilakukan:

a. Context Establishment

Table 2-2 Kriteria *Probability*

Bobot Penilaian	Tingkat Kejadian	Jumlah Frekuensi Kemungkinan Terjadi dalam Setahun	Persentase kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	X < 2 kali	X ≤ 5%
2	Jarang Terjadi	2 ≤ X ≤ 5 kali	5% < X ≤ 10%
3	Kadang-Kadang Terjadi	6 ≤ X ≤ 9 kali	10% < X ≤ 20%
4	Sering Terjadi	10 ≤ X ≤ 12 kali	20% < X ≤ 50%
5	Hampir Sering Terjadi	> 12 kali	X > 50%

Table 0-1.3 Kriteria *Impact*

Tingkat Dampak	Reputasi	Operasional	Aset Informasi
1 (Tidak Signifikan)	Tidak berpengaruh pada reputasi.	Tidak berpengaruh pada kegiatan operasional.	Tidak mempengaruhi keamanan pada aset informasi
2 (Jarang Terjadi)	Kerusakan reputasi yang tidak menyeluruh, hanya satuan kerja tertentu.	Penurunan kegiatan operasional yang tidak menyeluruh, hanya pada jaringan.	Aset berupa data fisik dan non-fisik yang hilang, rusak, salah atau tidak dapat digunakan atau di akses sementara waktu. diperlukan waktu yang sebentar untuk mengembalikannya.

Tingkat Dampak	Reputasi	Operasional	Aset Informasi
3 (Kadang-Kadang Terjadi)	Kerusakan reputasi yang tidak menyeluruh, hanya di divisi/bagian/tim tertentu.	Kegiatan operasional yang tidak menyeluruh, tidak bisa di akses hanya disatu pihak si pemegang akses tertentu (Admin Telkom).	Aset berupa data fisik dan non - fisik yang hilang, rusak atau tidak dapat digunakan atau diakses untuk jangka waktu tertentu. Diperlukan waktu tindak lanjut agak lama untuk mengembalikannya.
4 (Signifikan)	Kerusakan reputasi yang tidak menyeluruh, hanya pelanggan atau partner bisnis (*counterparties*) tertentu	Kegiatan operasional yang tidak menyeluruh, tidak bisa di akses hanya disatu pihak si pengirim surat tertentu.	Aset berupa data fisik dan non-fisik yang hilang, rusak atau tidak dapat digunakan atau diakses untuk jangka waktu lebih lama. Diperlukan waktu tidak lanjut yang cukup lama untuk mengembalikannya.
5 (Sangat Signifikan)	Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan di mata pelanggan dan masyarakat secara global dan regional	Terhentinya kegiatan operasional yang serius, *website* tidak dapat di akses oleh semua pihak (*User*, Admin Telkom)	Penyimpanan data pada *cloud* dicuri oleh orang tidak dikenal, mengakibatkan kehilangan data penting non-fisik dan terjadi kebakaran menyebabkan data fisik terbakar tidak ada salinan *copy* data.

b. Risk Assessment

Table 2-4 Aset IT

Kategori	Jenis Aset	Aset	Deskripsi	Alasan Pemilihan Aset
Aset Primer	Proses Bisnis dan Aktivitas	*Procedure* (SOP)	Standar Operasional Prosedur berisi aturan-aturan tentang aplikasi SIPT	Sebagai standar dalam mengoperasikan/menjalankan aplikasi SIPT
	Informasi	Proses/Alur penggunaan aplikasi SIPT (User Guide)	Memberikan panduan penggunaan aplikasi	Karena sebagai pedoman dalam mengoperasikan aplikasi SIPT
Aset Pendukung	*Hardware*	*Router*	Menghubungkan beberapa jaringan untuk mempermudah pengiriman pesan/paket	Menghubungkan beberapa Access Point agar aplikasi SIPT dapat digunakan diseluruh ruangan/divisi
		Access Point	Menghubungkan jaringan dengan nirkabel untuk sebuah daerah (LAN)	Menjadi sebuah titik akses setiap ruangan/divisi agar memiliki akses untuk menerima/mengirim pesan ke ruangan lain
		PC/Laptop/ Mobile Phone	Perangkat untuk mengirim/menerima pesan	Perangkat untuk mengirim/menerima pesan

		Data Center Telkom	Ruangan Infrastruktur berbagai perangkat komputer/jaringan	Menjadi tempat pusat telkom untuk penyimpanan basis data dan server utama
	Software	*Aplikasi SIPT*	Sistem Informasi untuk melakukan persuratan	Aplikasi utama dalam penggunaan pengiriman/penerimaan pesan (surel)
		Lostus Domino (Platform)	Sebuah platform aplikasi SIPT	Manajemen Surat, melakukan koneksi ke database NoSQL
		NoSQL (Database)	Struktur Basis Data aplikasi SIPT	Untuk menyimpan beberapa tabel tanpa relasi dan query
	Network	Internet (Layanan Internet Astinet Telkom)	Jaringan Global (Dunia) yang saling terhubung	Memungkinkan untuk berkomunikasi, mengirim pesan jarak jauh
	Personel	*End User* (Sekretariat Kabinet)	Seseorang yang menggunakan aplikasi SIPT	Membuat dokumen surat administrasi, perizinan dan teknis
		Web Developer (Telkom)	Seseorang yang membuat/mengelola aplikasi SIPT	Membuat front-end, back-end, dan koneksi ke database aplikasi SIPT

Table 2-5 Bentuk Ancaman

Types	***Example of Vulnerabilities***	***Example of Threats***	**Prioritas Risiko**
Software	Kegagalan untuk mengadopsi secara tepat waktu dan mengeksploitasi perangkat lunak baru (fungsi, optimasi, dll)	*Error in use*	*HIGH*
	Modifikasi disengaja atau manipulasi perangkat lunak yang mengarah ke data yang salah	*Error in use*	*MEDIUM*
	Modifikasi yang disengaja atau manipulasi perangkat lunak yang mengarah pada tindakan curang	*Abuse of rights*	*MEDIUM*
Personel	Kesalahan oleh staf TI (selama pencadangan, selama peningkatan sistem, selama pemeliharaan sistem, dll)	*Illegral Processing of data*	*MEDIUM*
	Informasi yang salah dimasukkan oleh staf TI atau pengguna sistem	*Illegral Processing of data*	*MEDIUM*
	Penggunaan perangkat lunak baru yang tidak efisien oleh *user*	*Breach personnel of availability*	*LOW*
	Perusakan situs web	*Destruction of equipment or media*	*MEDIUM*
Network	Gangguan layanan akibat serangan Denial-of-Services (DoS)	*Denial of action*	*MEDIUM*
	Serangan malware	*Error in use*	*MEDIUM*

Types	*Example of Vulnerabilities*	*Example of Threats*	Prioritas Risiko
	kurangnya akses karena kejadian yang mengganggu di tempat lain	*Unauthorised use of equipment*	*LOW*
Organization	kurangnya kesadaran akan potensi perubahan regulasi yang mungkin berdampak pada bisnis	*Abuse of right*	*MEDIUM*
	Kegagalan untuk mengidentifikasi tren teknologi baru dan penting	*Breach of information system maintanbility*	*MEDIUM*
	Kegagalan untuk mengadopsi dan mengeksploitasi teknologi baru pada waktu yang tepat (fungsi, proses mengoptimalkan, dll)	*Breach of information system maintanbility*	*MEDIUM*
Hardware	Peralatan yang tidak ramah lingkungan (misalnya, konsumsi daya, pengemasan)	*Loss of power supply*	*LOW*

Table 2-6 Estimasi Risiko

Nilai	Tingkat Prioritas Risiko	Estimasi Penanganan Risiko
1-9	Low	< 3 Hari
10 – 16	Medium	4 sampai 6 Hari
17 – 25	High	> 7 Hari

c. *Risk Treatment*

Table 2-7 Penangan Risiko

No	Kemungkinan Risiko	Bobot Kejadian	Sebelum Penanganan						
			Tingkat Dampak					Penjelasan Dampak	Opsi Penanganan
			Reputasi	Operasional	Aset Informasi	Total Dampak	Skor Risiko		
1.	Kegagalan untuk mengadopsi dan mengeksploitasi perangkat lunak baru secara tepat waktu (fungsionalitas, optimisasi, dll)	4	4	5	3	5.3	21	**HIGH**	**Mitigate**
2.	Kesalahan oleh staf TI (selama pencadangan, selama peningkatan sistem, selama pemeliharaan sistem, dll)	2	3	5	3	4.3	9	**MEDIUM**	**Mitigate**
3.	Salah memasukkan informasi oleh staf TI atau pengguna sistem	3	3	4	2	4.0	12	**MEDIUM**	**Mitigate**
4.	Modifikasi atau manipulasi perangkat lunak yang disengaja mengarah ke data yang salah	1	4	4	4	4.3	4	**MEDIUM**	**Accept**
5.	Modifikasi yang disengaja atau manipulasi perangkat lunak yang mengarah pada tindakan curang	1	5	4	4	4.7	5	**MEDIUM**	**Avoid**
6.	penggunaan perangkat lunak baru tidak efisien oleh user	2	2	1	1	2.0	4	**LOW**	**Transfer**

No	Kemungkinan Risiko	Bobot Kejadian	Sebelum Penanganan						
			Tingkat Dampak					Penjelasan Dampak	Opsi Penanganan
			Reputasi	Operasional	Aset Informasi	Total Dampak	Skor Risiko		
7.	Gangguan layanan karena serangan penolakan layanan (DoS)	2	2	2	4	3.3	7	**MEDIUM**	**Transfer**
8.	Perusakan situs web	3	3	5	3	4.7	14	**MEDIUM**	**Avoid**
9.	Serangan malware	3	2	2	4	3.7	11	**MEDIUM**	**Mitigate**
10.	Kurangnya kesadaran akan kemungkinan perubahan regulasi yang mungkin berdampak bisnis	2	4	1	3	3.3	7	**MEDIUM**	**Transfer**
11.	Kurangnya akses karena insiden gangguan di tempat lain	2	1	2	1	2.0	4	**LOW**	**Transfer**
12.	Kegagalan untuk mengidentifikasi tren teknologi baru dan penting	3	2	5	1	3.7	11	**MEDIUM**	**Transfer**
13.	Kegagalan untuk mengadopsi dan mengeksploitasi teknologi baru secara tepat waktu (fungsionalitas, mengoptimalkan proses, dll.)	3	2	3	3	3.7	11	**MEDIUM**	**Mitigate**
14.	Perlengkapan yang tidak ramah lingkungan (mis., Konsumsi daya, kemasan)	2	1	2	1	2.0	4	**LOW**	**Accept**

d. Risk Acceptance

Table 2-8 Opsi Penanganan

Opsi Penanganan	Deskripsi	Jumlah
Accept (Menerima)	Menerima risiko yang terjadi	2 Risiko
Avoid (Menghindar)	Menghindari risiko dengan tidak memulai atau lanjut dengan aktivitas yang menimbulkan risiko tersebut	2 Risiko
Mitigate (Mengurangi)	Mengurangi tingkat kejadian atau dampak negatif dari risiko tersebut	5 Risiko
Transfer (Membagikan)	Berbagi risiko dengan pihak lain	5 Risiko

4.2 Rekomendasi Kontrol Berdasarkan ISO 27002:2013

Evaluasi akan diberikan pada tabel dibawah ini:

Table 2-9 Kontrol Risiko

No.	Risiko	Kontrol risiko	Kode	Kontrol	Kategori Kontrol	Dokumen Relevan
1.	Kegagalan untuk mengadopsi dan mengeksploitasi perangkat lunak baru secara tepat waktu (fungsionalitas, optimisasi, dll)	(A. 12.6) Manajemen kerentanan teknis	(A. 12.6.2) Pembatasan instalasi perangkat lunak	Aturan yang mengatur instalasi perangkat lunak oleh pengguna harus dibuat dan diimplementasikan	Proses	Katalog Perangkat Lunak
2.	Kesalahan oleh staf TI (selama pencadangan, selama peningkatan sistem, selama pemeliharaan sistem, dll)	(A. 12.3) Cadangan	(A. 12.3.1) Cadangan informasi	Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji regulary sesuai dengan kebijakan cadangan yang disepakati.	Proses	Kebijakan Pencadangan
3.	Salah memasukkan informasi oleh staf TI atau pengguna sistem	(A.7.2) Selama Ketenagakerjaan	(A.7.2.2) Kesadaran keamanan informasi, pendidikan dan pelatihan	Semua karyawan organisasi dan, jika relevan, kontraktor harus menerima pendidikan kesadaran yang tepat dan pelatihan dan update reguler dalam organisasi, kebijakan dan prosedur, yang relevan untuk fungsi pekerjaan mereka.	People	Rencana Pelatihan Penggunaan Aplikasi
4.	Serangan malware	(A. 12.2) Perlindungan dari malware	(A.12.2.1) Kontrol terhadap malware	Kontrol deteksi, pencegahan, dan pemulihan untuk memproyeksikan malware akan diterapkan, dikombinasikan .dengan kesadaran pengguna yang sesuai.	Proses	Kebijakan Perlindungan Malware
5.	Kegagalan untuk mengadopsi dan mengeksploitasi teknologi baru secara tepat waktu (fungsionalitas, mengoptimalkan proses, dll.)	(A. 12.6) Manajemen kerentanan teknis	(A. 12.6.1) Manajemen kerentanan teknis	Informasi tentang kerentanan teknis dari sistem informasi yang digunakan harus diperoleh secara tepat waktu, organisasi paparan kerentanan dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko yang terkait.	Proses	Prosedur *Vulnerability Assessment*

4.3 Rekomendasi Solusi untuk Mitigasi Risiko SIPT

Dilihat dari 2 aspek yaitu:

1) People

Memberikan pelatihan penggunaan aplikasi SIPT berbasis website.

2) Process
   a) Melakukan penilaian penggunaan aplikasi pertahun (Template penilaian penggunaan aplikasi dapat dilihat dilampiran A)
   b) Menyusun katalog perangkat lunak (Template katalog perangkat lunak dapat dilihat dilampiran B)
   c) Menyusun prosedur pencadangan (Prosedur pencadangan dapat dilihat di lampiran C)
   d) Menyusun Kebijakan Perangkat Lunak (D)
   e) Menyusun Kebijakan Perlindungan *Malware* (E)
   f) Menyusun Prosedur *Vulnerability Assessment* (F)

Rekomendasi *Technology* tidak ada. Karena pada *assessment* risiko sebelumnya tidak ada dibutuhkan rekomendasi kearah teknologi. Dan aplikasi yang digunakan sudah baik dalam versi web.

4.4 Roadmap

Table 2-10 Roadmap

No	Inisiatif	2020		2021			
		Q3	Q4	Q1	Q2	Q3	Q4
1.	Memberikan pelatihan penggunaan aplikasi SIPT berbasis website						
2.	Menyusun katalog perangkat lunak						
3.	Melakukan penilaian penggunaan aplikasi pertahun						
4.	Menyusun Kebijakan Perangkat Lunak						
5.	Mensosialisasikan Kebijakan Perangkat Lunak						
6.	Menyusun Kebijakan Perlindungan *Malware*						
7.	Mensosialisasikan Kebijakan Perlindungan *Malware*						
8.	Menyusun kebijakan pencadangan						
9.	Menyusun Prosedur *Vulnerability Assessment*						

5. Kesimpulan

Berdasarkan penelitian yang telah dilakukan pada aplikasi SIPT menggunakan pendekatan ISO/IEC 27005:2018 dapat diperoleh kesimpulan sebagai berikut:

1. Hasil identifikasi jenis ancaman dan kemungkinan risiko secara keseluruhan yakni terdapat 14 jenis ancaman yang mungkin terjadi pada aset aplikasi SIPT. Jenis ancaman yang mungkin terjadi dibagi kedalam tiga kategori yaitu ancaman rendah (*Low*), anacaman sedang (*Medium*) dan ancaman Tinggi (*High*), dimana 1 aset bisa memiliki beberapa ancaman yang sama jenisnya dan juga berbeda jenisnya. Sehingga dari hasil identifikasi diperoleh jenis ancaman dengan rincian yakni 3 ancaman dengan tingkat ancaman rendah (*Low*), 10 ancaman dengan tingkat ancaman sedang (*Medium*) dan 1 ancaman dengan tingkat ancaman tinggi (*High*). Hal ini berarti aset pada aplikasi SIPT mayoritas memiliki tingkat kemungkinan terjadinya ancaman yang rendah (*Medium*).

2. Hasil penelitian dan analisis risiko diketahui terdapat 5 risiko diatas batas *acceptance* level. Selanjutnya dilakukan kontrol rekomendasi risiko yang diambil dari annex ISO/IEC 27002:2013 yang meliputi kontrol terhadap *malware*, pencadangan informasi dan perangkat lunak.

Daftar Pustaka

[1] D. S. Dewandaru, "Pemanfaatan Aplikasi E-Office Untuk Mendukung Reformasi Birokrasi Studi Kasus : Pusjatan," *Seminar Nasional Sistem Informasi Indonesia*, no. 4022, pp. 2–4, 2013.

[2] E. E. Reader *et al.*, "TATA NASKAH DINAS," *Resources*, vol. 2, no. 10, pp. 1–19, 2012.

[3] A. Asriyanik and Prajoko, "Manajemen Keamanan Informasi pada Sistem Informasi Akademik Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 4, no. 2, pp. 315–325, 2018.

[4] D. W. Gustini and S. Afriani, "Analisis Manajemen Risiko Pada Kantor Pusat Pt. Bank Bengkulu," *EKOMBIS REVIEW: Jurnal Ilmiah Ekonomi dan Bisnis*, vol. 2, no. 1, pp. 105–121, 2015.

[5] I. S. O. ISO, J. T. C. I. J. 1, I. Technology, and I. S. techniques Subcommittee SC 27, "Iso/Iec 27005:2008," vol. 3, p. 61, 2008.

[6] F. O. R. Standardization and D. E. Normalisation, "International Standard Iso," vol. 1987, 1987.

[7] E. Supristiowadi and Y. G. Sucahyo, "Manajemen Risiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," *Indonesian Treasury Review: Jurnal Perbendaharaan, Keuangan Negara dan Kebijakan Publik*, vol. 3, no. 1, pp. 23–33, 2018.

[8] M. T. . Vicho Septian Darta, S.T., "Mengenal Standard ISO 27001," *05 Feb*, 2020. [Online]. Available: https://www.indonesiare.co.id/id/knowledge/detail/333/Mengenal-Standard-ISO-27001.