PENILAIAN RISIKO DATA SIMPUS DAN ASET MENGGUNAKAN ISO 27005 PADA PUSKESMAS DI SAMPIT

[1] Jonny, [2] Awalludiyah Ambarwati, [3] Cahyo Darujati
[1,2]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
[3]Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Narotama
Jl. Arief Rachman Hakim No. 51 Surabaya 60117, Telp. (031)5946404, 5995578, Fax. (031)5931213
Email: joenysby@gmail.com, ambarwati1578@yahoo.com, cahyo.darujati@narotama.ac.id,

ABSTRACT

Puskesmas Pasir Putih is part of the local government that provides services in health care that has implemented and developed IT for health service activities. There is a problem in patient service when virus computer attack SIMPUS (Sistem Informasi Puskesmas or health center information system). That incident cause SIMPUS cannot be used temporarily. This research was conducted to assess the risk of possible threats and risks that arise using ISO 27005. The result shown that the average risk assessment of moderate risk and high risk are still small on the threats that might occur and the risk management of 30 possible threat scenarios such as, risk modification (RM) 20 scenarios, risk Avoidance (RA) 3 scenarios and risk sharing (RS) 7 scenarios. There are several recommendations for risk management at Puskesmas Pasir Putih. Policies and rules need to be made by the head of the Puskesmas to maintain the main assets of the SIMPUS application for processing, deleting and outputing the SIMPUS data. Conducted training for both managers and user of SIMPUS applications. Added security, maintenance and control of supporting assets.

Keywords: *Puskesmas Pasir Putih, ISO 27005, Risk Assessment*

ABSTRAK

Puskesmas Pasir Putih yang merupakan bagian dari instansi pemerintah daerah yang melakukan pelayanan dalam bidang kesehatan yang telah menerapkan dan mengembangkan TI untuk kegiatan pelayanan kesehatan. Namun ada permasalahan pada sistem informasi puskesmas dalam pelayanan pasien, pada komputer terkena virus sehingga SIMPUS (Sistem Informasi Manajemen Puskesmas) tidak bisa digunakan sementara. Penelitian ini dilakukan untuk penilaian risiko terhadap kemungkinan ancaman dan risiko yang muncul menggunakan ISO 27005. Hasil penelitian dari penilaian risiko rata-rata risiko sedang dan risiko tinggi masih kecil pada ancaman yang mungkin terjadi dan penanganan risiko dari 30 skenario ancaman yang mungkin terjadi yaitu, *risk modification* (RM) 20 skenario, *risk Avoidance* (RA) 3 skenario dan *risk sharing* (RS) 7 skenario. Rekomendasi untuk penanganan risiko pada Puskesmas Pasir Putih yaitu perlu adanya kebijakan dan aturan dari kepala puskesmas terhadap aset utama aplikasi SIMPUS untuk pengolahan, penghapusan dan output data SIMPUS. Dilakukan pelatihan terhadap pengelola dan pengguna aplikasi SIMPUS. Penambahan keamanan, pemeliharaan dan kontrol pada aset pendukung dan menambah kebutuhan yang diperlukan.

Kata Kunci: Puskesmas Pasir Putih, ISO 27005, Penilaian Risiko

1 PENDAHULUAN

Manajemen risiko teknologi informasi mempunyai manfaat untuk pemerintah daerah berupa pengamanan terhadap aset teknologi informasi yang berfungsi sebagai penyimpanan, pengolah, dan penyebar informasi. Aset yang dimiliki harus dijaga dan dilindungi dari terjadinya risiko. Puskesmas Pasir Putih yang merupakan bagian dari instansi pemerintah daerah yang melakukan pelayanan dalam bidang kesehatan. Puskesmas Pasir Putih telah menerapkan dan mengembangkan TI untuk kegiatan pelayanan kesehatan. SIMPUS yang merupakan sistem informasi manajemen yang digunakan oleh staf puskesmas guna mendukung kegiatan pelayanan kesehatan kepada masyarakat.

Beberapa permasalahan pernah dialami Puskesmas Pasir Putih di antaranya sistem informasi puskesmas dalam pelayanan pasien, pada komputer terkena virus sehingga sistem SIMPUS tidak bisa digunakan sementara. *Switch hub* pada LAN jaringan komputer terkena petir sehingga komputer yang terhubung mengalami kerusakan karena kelalaian. Data SIMPUS jarang di *backup* karena belum ada

komputer khusus untuk sistem pelayanan. Agar menghindari kejadian yang sama terulang kembali, perlu dilakukan penilaian risiko. Penelitian ini dilakukan untuk penilaian risiko terhadap kemungkinan ancaman dan risiko yang muncul. Dalam penilaian risiko keamanan data SIMPUS dan aset TI pada Puskesmas Pasir Putih di Sampit menggunakan ISO 27005/2011. ISO 27005/2011 merupakan standar international yang menyediakan pedoman untuk manajemen risiko keamanan informasi (*information security risk management*) pada suatu organisasi.

2 TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Penelitian terdahulu merupakan pengamatan awal terhadap fakta awal dari kegiatan sebuah penelitian yang nantinya dapat menjadi dasar perbandingan dengan penelitian saat ini. Adanya kendala pada akademik SIM-PTS yang sering dialami adalah sulitnya akses pengguna akibat paket data yang dikirim ke *server* melebihi kapasitas yang adakalanya membuat *server down*. Selain itu pernah beberapa kali terjadi peretasan website yang digunakan. Sehingga yang dilakukan bagaimana melakukan identifikasi risiko keamanan informasi menggunakan ISO 27005/2011 dan menentukan apa yang dapat terjadi hingga memiliki potensi menyebabkan kerugian. Dan hasil penelitian mengidentifikasi risiko terdiri dari identifikasi *assets*, *threats*, *existing controls*, *vulnerabilities* dan *consequences* pada PTS di Surabaya, menunjukkan bahwa DSTI telah berupaya melakukan perlindungan terhadap aset yang dimiliki. Beberapa kontrol yang ada belum didokumentasikan dan belum disosialisasikan kepada seluruh civitas akademika, masih terbatas pada personel DSTI [1].

Kondisi penyelenggara sertifikasi elekronik (PSrE) BPPT saat ini belum memiliki sistem manajemen keamanan informasi yang menjadi salah satu syarat apabila BPPT mau menjadi penyelenggara sertifikasi elektronik (PSrE) berinduk. Sehingga dilakukan bagaimana analisis manajemen risiko keamanan informasi menggunakan ISO 27005/2013 yang secara spesifik dan komprehensif untuk melakukan assessment terhadap keamanan informasi. Hasil dari penelitian, penerimaan risiko berdasarkan ISO/IEC 27005:2013 pihak yang bertanggung jawab sebagai personal incharge (PIC) untuk melakukan kontrol akan setiap ancaman terhadap aset ditentukan, membuat dan memonitor kontrol terhadap aset. Seluruh risiko pada kelompok yang bukan termasuk kelompok risiko rendah akan ditangani dan kerangka kerja yang digunakan adalah ISO/IEC 27005:2013 [2].

Belum adanya evaluasi risiko keamanan informasi pada media elektronik atau non-elektronik terhadap informasi yang direkam, diproses, disimpan, dikirim atau diambil. Untuk upaya perlindungan dan memastikan keberlanjutan bisnis dan investasi. Sehingga bagaimana meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan menggunakan ISO 27005. Hasil dari penelitian ini, identifikasi adanya risiko pada proses bisnis dan aset dilakukan dengan mengidentifikasi risiko yang mungkin muncul pada aset-aset yang berkaitan dengan aplikasi SIM akademik serta kelemahan yang mengancam terjadinya risiko [3].

Belum adanya manajemen risiko keamanan informasi pada badan pertanahan nasional. Sehingga dilakukan bagaimana identifikasi risiko dan hasil *risk assessment* menggunakan standar ISO 27005. Hasil dari penelitian ini, dapat memenuhi tujuan awal sehingga di dapatkannya hasil akhir dari proses *assessment* sampai pada tahap evaluasi risiko. Risiko yang telah teridentifikasi telah diprioritaskan berdasarkan penilaian yang ditentukan menurut standar ISO dari prioritas risiko mana yang paling berpengaruh ke tingkat risiko yang paling kecil [4].

Belum adanya manajemen risiko keamanan informasi sehingga memunculkan ancaman pada SIAK UMMI, adanya laporan terjadinya serangan siber dan upaya *hacking* terhadap sistem informasi di UMMI. Sehingga dilakukan bagaimana melakukan manajemen risiko pada sistem informasi akademik UMMI dengan menggunakan standar ISO 27005. Hasil dari penelitian ini dapat diketahui bahwa aset SIAK UMMI terbagi menjadi empat aset utama, yaitu perangkat keras dan jaringan, perangkat lunak aplikasi dan pendukung SIAK UMMI, SDM dan data informasi yang ada pada SIAK UMMI dan berdasarkan proses penilaian risiko, terdapat 73 skenario ancaman yang mungkin terjadi [5]. Belum adanya penilaian risiko keamanan informasi yang kemungkinan memunculkan terjadinya serangan oleh pihak yang tidak bertanggung jawab pada sistem berbasis website dan *mobile* di suatu universitas. Sehingga yang dilakukan bagaimana membangun aplikasi penilaian risiko keamanan informasi berbasis ISO 27005 menggunakan metode *Prototyping*. Hasil penelitian ini menghasilkan sebuah penilaian risiko berbasis web yang dapat mudah digunakan oleh berbagai tipe pengguna [6].

Begitu banyak masalah yang datang pada bagian *Helpdesk* di UPT SAMSAT Denpasar atau dari UPT lain sekaligus dari transaksi UPT SAMSAT Denpasar. Ada 75% dari total masalah yang masuk ke *helpdesk*. Dimana ada 8 skenario ISO/IEC 27005 termasuk identifikasi aset, *asset appraisal*, *impact assessment*. Hasil studi ini menunjukan bahwa daftar aset yang rata-rata memiliki tingkat risiko tertinggi termasuk aset utama [7].

Tidak adanya standar ISO 27005 manajemen risiko keamanan informasi (ISRM) sehingga organisasi belum memiliki tanggung jawab untuk melindungi informasi ini dan memastikan kerahasiaan, integritas, dan ketersediaannya. Bagaimana mengidentifikasi objek informasi dalam organisasi yang akan diperlukan dalam tugas ISRM, Bagaimana objek informasi ISRM dapat diklasifikasikan dalam tugas ISRM. Hasil dari penelitian ini, adalah untuk mengusulkan kerangka kerja untuk menunjukkan berbagai objek informasi yang terlibat dalam standar manajemen risiko ISO 27005 dan mengklasifikasikan informasi berdasarkan pedoman yang disediakan oleh skema UNINETT, Skenario kasus klinik kesehatan dikembangkan untuk mengidentifikasi objek informasi terkait ISRM menggunakan kerangka kerja yang diusulkan dan mengklasifikasikannya informasi menggunakan skema UNINETT.[8].

Organisasi belum secara optimal mengendalikan dampak ancaman potensial. Cara menyediakan survei tentang metode dan alat manajemen risiko keamanan informasi yang tersedia, cara menyajikan deskripsi EBIOS, Mehari, SP800-30 (NIST), CRAMM, dan ISO 27005, cara memberikan analisis komparatif, cara mengusulkan pendekatan dan dalam 6 itu akan memperkenalkan perumusan risiko matematika. Hasil dari penelitian ini, untuk mengusulkan formulasi matematis risiko dengan menggunakan tingkat granularitas elemen yang lebih rendah: ancaman, probabilitas, kriteria yang digunakan untuk menentukan nilai aset, paparan, frekuensi dan ukuran perlindungan yang ada [9].

Dalam tugas manajemen risiko, keputusan yang salah sering dibuat oleh praktisi risiko dan pemangku kepentingan lainnya (pengambil keputusan, pemilik produk) karena kurangnya pengetahuan tentang domain keamanan, aset, potensi tindakan keinginan organisasi, kebingungan antara praktisi dan pengguna risiko. karena terminologi keamanan tidak didefinisikan dengan baik. Manajer tidak memiliki pemahaman lengkap tentang infrastruktur dan konsep TI yang mendasarinya yang terkait dengan tugas manajemen risiko. Bagaimana ontologi untuk mengembangkan dan mengelola konsep inti dari fase penilaian risiko standar ISO / IEC 27005: 2011. Hasil penelitian ini, ontologi untuk menyusun dan mengatur konsep inti fase penilaian risiko. Metode ontologi pengembangan ontologi mengikuti pedoman tujuh langkah. Skenario kasus klinik kesehatan dikembangkan untuk menerapkan ontologi yang diusulkan, setiap entitas dan hubungan ontologi memberikan titik referensi bagi para profesional dan peneliti dengan menghadirkan ontology [10].

Divisi SISTEKFO yang mengelola infrastruktur TI, seringkali menemukan permasalahan yang dikarenakan kurangnya kesadaran dan pengelolaan penerapan keamanan informasi dengan benar, sehingga menyebabkan terjadinya insiden keamanan informasi dan mengganggu proses bisnis perusahaan. Maka Perancangan SMKI berbasis Manajemen Risiko yang dibangun pada penelitian ini mengacu kepada standar ISO/IEC 27001:2005, ISO/IEC 27002:2005 dan ISO/IEC 27005:2008. Hasil penelitian menghasilkan dokumentasi yang terdiri dari Manual Keamanan Informasi, Instruksi Kerja, Prosedur Kerja, dan Formulir Kerja Keamanan Informasi [11]. Implementasi infrastruktur teknologi informasi memiliki risiko yang dapat mengganggu kinerja organisasi maupun operasional. Risiko ini disebabkan oleh manusia atau sistem itu sendiri. Menggunakan *framework* ISO/IEC 27005:2011 sebagai metode penelitian risikonya Hasil penilaian risiko berdasarkan analisis menunjukkan *level* risiko cenderung berada pada *risk acceptance level*, namun ada beberapa aset yang memiliki *level* risiko diantara 6-8 (*high risk*) seperti hilangnya pasokan listrik, kerusakan pada perangkat keras, sehingga harus dilakukan penanganan yang sesuai [12].

Memiliki penerapan manajemen risiko dalam pengelolaan TI (Teknologi Informasi) dan proses bisnis pada divisi TI. Akan tetapi, penerapan tersebut belum sepenuhnya menilai adanya ancaman pada aset TI di divisi TI dan menilai seberapa jauh kontrol yang sudah ada dapat mengurangi ancaman maupun risiko yang akan datang serta dampaknya, maka dilakukan menggunakan ISO 27005 difokuskan sebagai pengelolaan aset TI. Hasil pada penelitian ini berdasarkan latar belakang tersebut, risk assessment pada aset TI menghasilkan *level of risk* yang mempunyai nilai ekstrem 2, tinggi 4, moderat 24. *Risk response* terhadap 6 ancaman yang harus dimitigasi[13]. Dengan melihat aspek manajemen risiko yang diatur dalam standar ISO 27005:2018. Namun demikian, karena pada dokumen standar tidak dijelaskan secara rinci bagaimana metodologi penilaian risiko sebagai proses

yang harus dilakukan untuk mencapai tujuan dari apa yang telah dinyatakan dalam kontrol sistem manajemen keamanan informasi (SMKI), maka digunakan pendekatan operasional dalam penilaian resiko yang disebut sebagai *Factor Analysis Information Risk* (FAIR). Dengan menggunakan metode FAIR, maka proses penilaian risiko yang ditetapkan dalam ISO 27005:2018 sebagai bentuk kelengkapan untuk SMKI klausul 6 pada ISO 27001:2013 dapat dilakukan dengan lebih mudah [14].

SAKTI masih belum memiliki alat untuk memastikan ketersediaan dan kontinuitas layanan dan perangkat yang dapat menjamin keberlangsungan dan mendukung layanan. Penelitian ini menggunakan pedoman dari beberapa kerangka kerja seperti ISO 27005 dan NIST SP 800-30. Output dari penelitian ini adalah informasi manajemen risiko keamanan untuk SAKTI, yang berisi proses identifikasi risiko, pemilihan kontrol untuk memitigasi risiko, dan penerimaan risiko oleh pemilik risiko [15]. Masalah yang terjadi dalam organisasi adalah seringnya laporan gangguan kecil dari *user* ketika waktu kerja dan ada beberapa masalah yang tidak terlalu penting membuat departemen TI datang ke tempat untuk menyelesaikannya, dan sering kali serangan virus di seperti *Denial Of Service* (DOS) atau *malware* yang sering dikirim ke email perusahaan yang dapat mengganggu kinerja perusahaan. Penilaian dan pengelolaan risiko TI dapat juga dilakukan menggunakan model kerangka kerja COBIT 4.1 dengan proses TI *Assess and Manage IT Risks* (PO9). Penelitian pada PT Dunia Saftindo menghasilkan nilai maturity level PO9 sebesar 2,6 yang dapat dikategorikan pada Level 3 (*Defined Process*). Hal ini memiliki arti bahwa PT Dunia Saftindo memiliki tingkat kemampuan yang baik dalam pengelolaan risiko TI, akan tetapi perlu peningkatan mutu dari sistem keamanan [16].

B. ISO 27005

ISO 27005 adalah suatu pendekatan sistematis terhadap manajemen risiko keamanan informasi diperlukan untuk mengidentifikasi kebutuhan organisasi mengenai persyaratan keamanan informasi dan menciptakan sistem manajemen keamanan informasi (SMKI) yang efektif. Pendekatan ini harus sesuai untuk lingkungan organisasi dan khususnya harus diselaraskan dengan manajemen risiko perusahaan secara keseluruhan. Manajemen risiko menganalisa apa yang bisa terjadi dan apa konsekuensi yang mungkin bisa. Proses manajemen risiko keamanan informasi dapat diterapkan pada organisasi secara keseluruhan, setiap bagian diskrit organisasi (misalnya departemen, lokasi fisik, layanan), setiap sistem informasi, aspek yang ada atau yang direncanakan atau kontrol tertentu (misalnya perencanaan kelangsungan bisnis).

Gambar 1 Proses manajemen risiko keamanan informasi [17]

Seperti yang digambarkan pada Gambar 1, proses manajemen risiko keamanan informasi dapat berulang untuk penilaian risiko dan/atau kegiatan perlakuan risiko. Pendekatan berulang itu memberikan keseimbangan yang baik antara meminimalkan waktu dan usaha yang dihabiskan dalam mengidentifikasi kontrol.

Tahapan dari setiap kegiatan di dalam ISO 27005:2011 terdiri dari tiga tahapan yanga dijelaskan sebagai berikut:

a. Penetapan konteks manajemen risiko keamanan informasi

Pada tahap ini dilakukan penggambaran konteks manajemen risiko keamanan informasi untuk sistem informasi yang meliputi: pertimbangan umum, kriteria dasar, ruang lingkup dan batasan, organisasi manajemen keamanan informasi.

b. Penilaian risiko keamanan informasi

Secara umum proses ini meliputi: identifikasi risiko, analisis risiko dan evaluasi risiko. Identifikasi risiko diuraikan lagi menjadi beberapa proses yaitu identifikasi aset, ancaman, identifikasi kerentanan, identifikasi dampak terjadinya ancaman atau ancaman. Proses analisis risiko meliputi penentuan kategori dampak risiko yang mungkin terjadi berdasar pada ancaman yang ada, penentuan kemungkinan terjadinya ancaman, serta menentukan level risiko yang mungkin terjadi dari setiap ancaman terhadap aset yang ada. Kategori kemungkinan (*likelyhood*) terjadinya ancaman dan dampak yang akan digunakan pada penelitian ini ditunjukan pada Tabel 1 dan Tabel 2.

Tabel 1 Kategori Kemungkinan dari Ancaman [18]

Kategori kemungkinan ancaman	Keterangan
Very unlikely (1)	Ancaman hampir tidak pernah terjadi.
Unlikely (2)	Frekuensi kejadian ancaman jarang (1-5 kali).
Possible (3)	Frekuensi kejadian ancaman cukup sering (6-10 kali).
Likely (4)	Frekuensi kejadian ancaman sering (10-20 kali).
Frequent (5)	Frekuensi kejadian ancaman sangat sering (>20 kali).

Tabel 2 Kategori dari Dampak [18]

Kategori dampak	Keterangan
Very low (1)	Dampak tidak signifikan. Artinya tidak menimbulkan gangguan aktivitas yang berarti. Untuk masalah ini toleransi.
Low (2)	Dampak gangguan kecil bukan pada program utama. Toleransi penyelesaian masalah 1-2 hari.
Medium (3)	Dampak gangguan sedang, yaitu ada gangguan kegiatan pendukung. Masalah harus diselesaikan paling lama 1 hari.
High (4)	Dampak gangguan besar, artinya menimbulkan gangguan pada kegiatan utama. Masalah harus diselesaikan <12 jam.
Very high (5)	Dampak sangat krusial. Artinya menimbulkan gangguan pada kegiatan utama dan pendukung secara kritis. Masalah ini harus diselesaikan <1 jam.

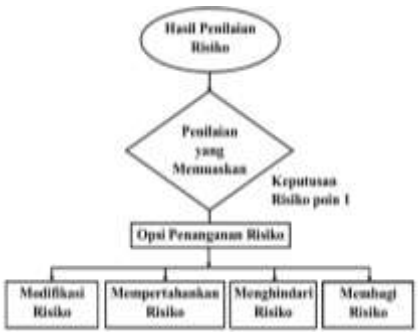
Bagian dari analisis risiko adalah membuat kategori penilaian risiko. Proses penilaian risiko ini dapat dilakukan secara kualitatif dan kuantitatif. Pada dasarnya untuk nilai risiko dihitung dengan cara mengalikan nilai dampak dan nilai kemungkinan terjadinya ancaman. Kategori penilaian risiko yang akan digunakan dalam manajemen risiko keamanan informasi pada penelitian ini dibagi menjadi tiga kategori yaitu: Risiko rendah (*low risk*), risiko sedang (*medium risk*), risiko tinggi (*high risk*). Untuk lebih jelasnya kategori risiko disajikan pada Tabel 3. Tahap terakhir dari penilaian risiko adalah evaluasi risiko, yaitu mengevaluasi risiko yang telah didapatkan pada tahap sebelumnya dan dibuat daftar prioritas risiko sesuai dengan nilai risiko.

Tabel 3 Matriks Kategori Penilaian Risiko [18]

		Kemungkinan (*likelyhood*) terjadinya ancaman				
		Very Unlikely (1)	*Unlikely (2)*	*Possible (3)*	*Likely (4)*	*Frequent (5)*
Dampak	*Very low (1)*	1/L	2/L	3/L	4/M	5/M
	Low (2)	2/L	4/L	6/M	8/M	10/M
	Medium (3)	3/L	6/M	9/M	12/M	15/H
	High (4)	4/M	8/M	12/M	16/H	20/H
	Very high (5)	5/M	10/M	15/M	20/H	25/H

c. Penanganan Risiko

Pada proses penanganan risiko didasarkan pada hasil penilaian risiko. Proses penanganan risiko meliputi pemilihan penanganan risiko, perencanaan penanganan risiko dan evaluasi sisa risiko. Langkah tersebut berulang sampai ditemukan penanganan risiko yang terbaik. Ada empat pilihan dalam penanganan risiko yaitu modifikasi risiko, mempertahankan risiko, menghindari risiko dan membagi risiko. Adapun lebih jelasnya langkah-langkah pada penanganan risiko ditunjukan pada Gambar 2. Dalam pemilihan penanganan risiko perlu diperhatikan beberapa hal, yaitu nilai risiko, biaya pemulihan dan biaya *transfer* risiko. Untuk menentukan hal ini, maka dibuat matriks keterhubungan antara ketiganya yang dapat sajikan pada Tabel 4.



Gambar 2 Alur penanganan risiko [18]

Tabel 4 Matriks pemilihan penanganan risiko [18]

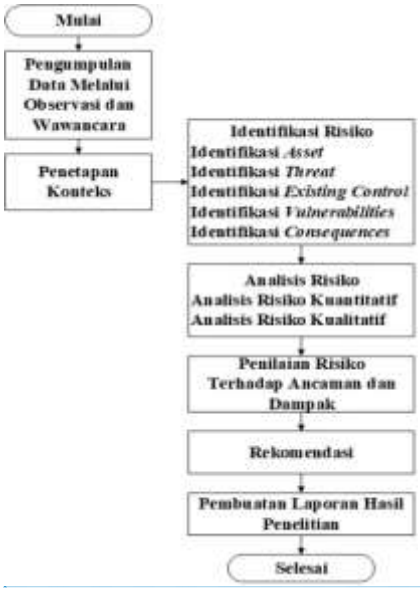
Nilai risiko	Biaya pemulihan		
	Low	*Medium*	*High*
Low	*Risk Retention*	*Risk Modification*	*Risk Sharing / Avoidance*
Medium	*Risk Modification*	*Risk Modification*	*Risk Sharing / Avoidance*
High	*Risk Avoidance*	*Risk Avoidance*	*Risk Sharing / Avoidance*
	High	***Medium***	***Low***
	Biaya *Transfer*		

3 METODE PENELITIAN

Penelitian ini menggunakan metode standar ISO 27005:2011 [18] untuk melakukan penilaian risiko keamanan data SIMPUS dan aset TI. Tahapan penelitian ini ditampilkan pada Gambar 3. Tahap pertama pengumpulan data melalui observasi dan wawancara. Pada tahap ini dilakukan pengumpulan data melalui observasi dan wawancara kepada pimpinan dan staf Puskesmas Pasir Putih. Tahap kedua penetapan konteks pada tahap ini dilakukan penggambaran konteks manajemen risiko keamanan informasi untuk data SIMPUS dan aset TI.

Tahap ketiga identifikasi risiko pada tahap ini diuraikan lagi menjadi beberapa proses yaitu identifikasi asset, *threat*, *existing control*, *vulnerabilities d*an *cosequences*. Pemilik aset perlu diidentifikasi untuk setiap aset yang dimiliki sehingga dapat diketahui *responsibility* dan *accountability*. Identifikasi threat memiliki potensi yang dapat membahayakan aset yang dimiliki Puskesmas Pasir Putih, seperti *informations*, *processes* and *systems*. Indentifikasi *existing control* harus dilakukan untuk menghindari pekerjaan berulang atau biaya tidak perlu, untuk mengidentifikasi *existing control* harus dilakukan pemeriksaan untuk memastikan bahwa kontrol bekerja dengan benar. Identifikasi *vulnerabilities* dilakukan pada data SIMPUS dan aset TI Puskesmas Pasir Putih. Identifikasi *consequences* yang dilakukan untuk mengetahui kerusakan atau konsekuensi pada Puskesmas Pasir Putih yang dapat disebabkan oleh skenario insiden.

Tahap keempat analisis risiko dalam tahap ini meliputi analisis kuantitatif dan kualitatif, dilakukan penentuan kategori dampak risiko dan kemungkinan terjadinya ancaman, serta menentukan *level* risiko. Tahap kelima penilaian risiko didasarkan pada hasil penilaian risiko. Proses penilaian risiko pada data SIMPUS dan aset TI dilakukan dengan perhitungan biaya pemulihan, *level* risiko dan biaya *transfer* sehingga hasilnya mendapatkan opsi penanganan risiko yaitu modifikasi risiko, mempertahankan risiko, menghindari risiko dan membagi risiko. Tahap keenam berupa rekomendasi bagi Puskesmas Pasir Putih. Pembuatan laporan hasil penelitian merupakan tahap akhir yang dilakukan pada penelitian ini.



Gambar 3 Tahapan penelitian

Commented [U1]: Setiap langkah yang ditampilan di sini harus ada sub bab hasil yang menjelaskan (matching antara metode dan hasil)

4 HASIL DAN PEMBAHASAN

A. Observasi dan wawancara

Observasi terkait keamanan informasi pada SIMPUS dilakukan di Puskesmas Pasir Putih. Wawancara dilakukan kepada pimpinan dan staf Puskesmas Pasir Putih. Hasil observasi dan wawancara diketahui *baseline* keamanan informasi pada data SIMPUS dan aset TI di Puskesmas Pasir Putih. Kurangnya pengamanan data SIMPUS dan aset TI, *backup* data dan *update* antivirus jarang dilakukan, merupakan kondisi pengamanan informasi saat ini di Puskesmas Pasir Putih.

B. Penetapan Konteks

Penelitian ini menetapkan konteks manajemen risiko keamanan informasi berupa data SIMPUS dan aset TI di Puskesmas Pasir Putih. Aset TI dalam hal ini adalah aset utama dan aset penunjang baik berupa perangkat keras maupun perangkat lunak yang dimiliki Puskesmas Pasir Putih.

C. Identifikasi Risiko

Identifikasi aset, Puskesmas Pasir Putih memiliki aset yang berada di ruang loket pelayanan, ruang poli pelayanan kesehatan dan ruang administrasi. Tabel 5 menyajikan aset TI yang dimiliki Puskesmas Pasir Putih yang diklasifikasikan sebagai aset utama dan pendukung. Aset utama berupa Aplikasi Pelayanan SIMPUS, Modem dan *Switch Hub*. Aset pendukung berupa perangkat keras yang dimiliki dan digunakan oleh Puskesmas Pasir Putih.

Identifikasi *threats* terhadap aset TI yang dimiliki Puskesmas Pasir Putih, beserta penyebab dan sumber ancaman disajikan pada Tabel 6. Identifikasi *existing controls* dilakukan untuk mengetahui kontrol yang telah diterapkan pada aset yang dimiliki Puskesmas Pasir Putih yang disajikan pada Tabel 7. Identifikasi *vulnerabilities* dilakukan untuk mengetahui kerentanan yang dapat terjadi pada aset yang dimiliki disajikan pada Tabel 8. Identifikasi *consequences* dilakukan untuk mengetahui kerusakan atau konsekuensi kepada Puskesmas Pasir Putih yang disebabkan oleh skenario insiden. Apabila aset TI yang dimiliki Puskesmas Pasir Putih berupa *hardware* maupun *software* mengalami masalah atau kerusakan dan *error*, maka sangat menganggu pelayanan kunjungan pasien. Jika itu terjadi cukup lama akan mempengaruhi penilaian akreditasi kepada Puskesmas Pasir Putih.

Tabel 5 Identifikasi Aset yang Dimiliki Puskesmas Pasir Putih

No	Aset	Jenis Aset	Lokasi Aset
1.	Aplikasi Pelayanan SIMPUS	Aset Utama	1.Loket, 2.Poli Umum, 3.Poli KIA, 4.Poli Gigi
2.	PC (4 unit)	Aset Pendukung	1.Loket, 2.Poli Umum, 3.Poli KIA, 4.Poli Gigi
3.	UPS	Aset Pendukung	Loket
4.	*Modem*	Aset Utama	Loket
5.	*Switch Hub*	Aset Utama	Poli Gigi
6.	Laptop L9PJUFT HP 14"	Aset Pendukung	Pelayanan Poli Umum

Sumber : hasil penelitian, diolah kembali

Tabel 6 Identifikasi Ancaman yang Dimiliki Puskesmas Pasir Putih

No	Aset	Ancaman	Penyebab Ancaman	Sumber Ancaman
1.	Aplikasi Pelayanan SIMPUS	Layanan terganggu	Aplikasi loading lama / *error* karena *troubleshooting*	Kapasitas ruang *server* tidak sesuai
2.	Windows 7	tidak berjalan lancar	Terdapat banyak virus	Virus
3.	Daya Listrik	Layanan ternganggu / lambat	Listrik tidak stabil daya kurang	1.Teknisi, 2. *Source Power*
4.	PC	PC *error* dan lambat	Adanya virus terdapat pada PC. Terdapat kendala di dalam *hardware*	1.Virus, 2.*Hardware*
5.	*Database Server*	*Password* untuk *login* standar terlalu mudah / lemah	Tidak ada batasan akses sehingga mudah diakses oleh orang yang tidak berwenang	1.Pengembang Aplikasi 2.Hacker
6.	UPS	Baterai penyimpanan lemah	UPS tidak mampu menampung beban daya perangkat *hardware*	Teknisi
7.	*Switch Hub*	Koneksi jaringan putus / terganggu	Tidak adanya kontrol untuk mematikan arus listrik terhubung dengan perangkat jaringan	*Source Power*
8.	*Modem*	Koneksi internet putus	Gangguan Sinyal jaringan dari operator	Teknisi

Sumber : hasil penelitian, diolah kembali

Tabel 7 Identifikasi *Existing Control* yang dimiliki Puskesmas Pasir Putih

No	Aset	Keterangan
1.	Aplikasi Pelayanan SIMPUS	1. User melakukan penginputan data sesuai menu aplikasi SIMPUS 2. Adanya *backup* data SIMPUS setelah selesai pelayanan.
2.	PC	*Install* Antivirus
3.	*Database Server*	Adanya *password* login hak akses
4.	UPS	Pengecekan perencanaan penggantian baterai yang sudah lemah
5.	*Switch Hub*	Terhubungnya jaringan pada komputer
6.	*Modem*	Terhubungnya jaringan internet

Sumber : hasil penelitian, diolah kembali

Tabel 8 Identifikasi *Vulnerabilities* yang Dimiliki Puskesmas Pasir Putih

No	Aset	Keterangan
1.	Aplikasi Pelayanan SIMPUS	1. Tidak adanya pelatihan berkala terhadap pengguna SIMPUS 2. Password untuk login masih standar terlalu mudah dan lemah 3. Tidak adanya kebijakan batasan penggunaan akses SIMPUS 4. Jarang dilakukan pengujian pada SIMPUS
2.	PC	1. Kurangnya kontrol dan pemeliharaan terhadap *hardware* 2. Kurangnya pemeliharaan dan kontrol pembaharuan OS 3. Kurangnya keamanan dan update antivirus
3.	*Database Server*	Tidak adanya otorisasi password hak akses kepada user yang menggunakan
4.	UPS	Perangkat keras yang terhubung pada UPS melebihi kapasitas beban daya yang dimiliki UPS tersebut
5.	*Firewall*	Menonaktifkan *firewall default*
6.	*Switch Hub*	1. Kurangnya kontrol terhadap perangkat jaringan 2. Kurangnya kontrol mematikan arus listrik yang terhubung perangkat jaringan
7.	*Modem*	Adanya gangguan koneksi internet

Sumber : hasil penelitian, diolah kembali

D. Analisis Risiko

Pada tahapan ini akan dilakukan penilaian kemungkinan (*likelyhood*) ancaman, dampak dan penilaian tingkat risiko yang mungkin terjadi pada data SIMPUS dan aset TI. Pada Tabel 9 disajikan skenario ancaman berdasarkan identifikasi sebagai tahap awal untuk melakukan penilaian risiko. Untuk penilaian kategori kemungkinan (*likelyhood*) ancaman yang mungkin terjadi, hasilnya didapatkan dari daftar skenario ancaman identifikasi risiko, disajikan pada Tabel 10. Untuk penilaian kategori dari dampak, hasilnya didapatkan dari daftar skenario ancaman identifikasi risiko. Adapun hasil penilaian kategori dari dampak disajikan pada Tabel 11.

Berdasarkan penilaian kategori kemungkinan (*likelyhood*) ancaman dan dampak dari skenario ancaman identifikasi risiko data SIMPUS dan aset TI. Maka hasil penilaian *level* risiko didapatkan dengan mengalikan kategori penilaian kemungkinan (*likelyhood*) ancaman dengan nilai dampak. Adapun hasil dari penilaian *level* risiko keamanan data SIMPUS dan aset TI disajikan pada Tabel 12 yang terdapat dua level risiko yaitu *Medium* (M) dan *High* (H).

Tabel 9 Daftar Skenario Ancaman Data SIMPUS dan Aset TI Puskesmas Pasir Putih

No. Skenario Ancaman	Penjelasan
1.	Kurangnya kontrol terhadap perangkat keras (*hardware*) yang dapat menimbulkan kerusakan sehingga mengakibatkan terganggunya penginputan data SIMPUS
2.	Kurangnya kontrol perangkat lunak (*software*) yang dapat menimbulkan *troubleshooting* sehingga mengakibatkan terganggunya penginputan data SIMPUS
3.	Terjadinya pemadaman listrik secara mendadak mengakibatkan proses SIMPUS terhenti
4.	Kurangnya kontrol untuk mematikan arus listrik yang terhubung perangkat jaringan dan komputer yang akan mengakibatkan kerusakan
5.	Gangguan koneksi internet mengakibatkan lambatnya penginputan, pengambilan dan pengiriman data
6.	Kurangnya keamanan sehingga terdapat virus pada perangkat komputer yang menjalankan SIMPUS
7.	Kurangnya pemahaman kerahasiaan data SIMPUS dan konfigurasi jaringan IP *address*
8.	Tidak adanya pelatihan berkala terhadap penanggung jawab dan *user* aplikasi SIMPUS
9.	Kurangnya kontrol perangkat jaringan komputer di PKM.PP
10.	Kurangnya pemeliharaan perangkat komputer yang sudah lama untuk di *upgrade*
11.	Banyak *user* melakukan akses SIMPUS karena tidak ada batasan yang mudah diakses oleh tidak berwenang
12.	Kurangnya pemeliharaan OS secara berkala di PKM. PP
13.	Tidak ada kontrol OS diperbarui pada perangkat komputer di PKM. PP
14.	*Password* untuk *login* SIMPUS masih standar terlalu mudah
15.	Masih kurangnya pemahaman *user* dalam menggunakan aplikasi SIMPUS karena panduan sulit dipahami
16.	Aliran listrik tidak stabil di lingkungan PKM. PP
17.	Jarang dilakukan pengujian pada aplikasi SIMPUS
18.	Terjadinya *loading* lama pada saat menjalankan aplikasi SIMPUS
19.	Tidak ada pembaruan atau terinstalasi antivirus pada perangkat komputer aplikasi SIMPUS
20.	Kurang pahamnya *user* melakukan *cleaning temporary file* setelah melakukan *browsing*
21.	Tidak adanya kebijakan tentang penggunaan hak akses pada aplikasi SIMPUS
22.	Kurangnya pemahaman penanggung jawab pengelola SIMPUS terhadap kerahasiaan data
23.	Kurangnya pemahaman penanggung jawab pengelola terhadap hak akses aplikasi SIMPUS
24.	Penerimaan tenaga admin tidak sesuai kebutuhan
25.	Adanya permasalahan koneksi jaringan putus pada perangkat komputer aplikasi SIMPUS
26.	Adanya penggunaan perangkat komputer aplikasi SIMPUS untuk tujuan lain
27.	Tidak adanya kebijakan dalam penghapusan data aplikasi SIMPUS
28.	Tidak adanya aturan penggunaan perangkat komputer yang berada di lingkungan PKM. PP
29.	Tidak pernah dilakukan pengecekan kebenaran data yang diinput ke aplikasi SIMPUS
30.	Tidak adanya aturan dalam print out data yang ada di aplikasi SIMPUS

Sumber : hasil penelitian, data history dari 5 tahun sebelumnya

Tabel 10 Kategori Kemungkinan dari Ancaman

Kategori kemungkinan Ancaman	Keterangan
Very Unlikely (1)	
Unlikely (2)	1, 2, 3, 4, 5, 7, 16, 18, 22, 23, 25
Possible (3)	8, 10, 11, 12, 13, 14, 15, 17, 19, 20, 21, 24, 26
Likely (4)	6, 9, 28
Frequent (5)	27, 29, 30

Sumber : hasil penelitian, diolah kembali

Pada bagian analisis risiko adalah membuat kategori penilaian risiko. Pada kategori penilaian risiko yang akan dilakukan adalah memasukan sesuai nomor skenario ancaman dari identifikasi risiko data SIMPUS dan aset TI yang hasil nilainya didapatkan dari kategori kemungkinan (*likelyhood*) ancaman dan dampak pada tabel matriks kategori penilaian risiko. Hasil dari kategori penilaian risiko disajikan pada Tabel 13.

Tabel 11 Kategori dari Dampak

Kategori Dampak	Keterangan
Very Low (1)	
Low (2)	
Medium (3)	1, 2, 3, 7, 9, 10, 11, 12, 13, 14, 15, 19, 20, 22, 23, 26, 28
High (4)	4, 5, 6, 8, 16, 17, 18, 21, 25, 27, 29, 30
Very High (5)	24

Sumber : hasil penelitian, diolah kembali

Tabel 12 Hasil Penilaian Level Risiko Keamanan Data SIMPUS dan Aset TI

No. Skenario	Nilai Ancaman	Nilai Dampak	Nilai Risiko	*Level* Risiko
1.	2	3	6	M
2.	2	3	6	M
3.	2	3	6	M
4.	2	4	8	M
5.	2	4	8	M
6.	4	4	16	M
7.	2	3	6	M
8.	3	4	12	M
9.	4	3	12	M
10.	3	3	9	M
11.	3	3	9	M
12.	3	3	9	M
13.	3	3	9	M
14.	3	3	9	M
15.	3	3	9	M
16.	2	4	8	M
17.	3	4	12	M
18.	2	4	8	M
19.	3	3	9	M
20.	3	3	9	M
21.	3	4	12	M
22.	2	3	6	M
23.	2	3	6	M
24.	3	5	15	M
25.	2	4	8	M
26.	3	3	9	M
27.	5	4	20	H
28.	4	3	12	M
29.	5	4	20	H
30.	5	4	20	H

Sumber : hasil penelitian, diolah kembali

Tabel 13 Matriks Kategori Penilaian Risiko

		Kemungkinan Terjadinya Ancaman				
		(1)	(2)	(3)	(4)	(5)
Dampak	(1)					
	(2)					
	(3)		1,2,3,7,22,23	10,11,12,13,14,15,19,20,26	9,28	
	(4)		4,5,16,18,25	8,17,21	6	27,29,30
	(5)			24		

Sumber : hasil penelitian, diolah kembali

E. Penilaian Risiko

Pada tahapan ini dilakukan proses penilaian risiko meliputi pemilihan penanganan risiko berdasarkan tabel matriks pemilihan penanganan risiko yaitu modifikasi risiko (*Risk Modification*/RM), mempertahankan risiko (*Risk Retention*/RR), menghindari risiko (*Risk*

Avoidance/RA) dan membagi risiko (*Risk Sharing*/RS). Kemudian hasilnya direkomendasikan sebagai pertimbangan penanganan risiko keamanan data SIMPUS dan aset TI Puskesmas Pasir Putih. Hasil penilaian risiko disajikan pada Tabel 14 dimana rata-rata risiko sedang dan risiko tinggi masih kecil pada ancaman yang mungkin terjadi dan penanganan risiko dari 30 skenario ancaman yang mungkin terjadi yaitu, *risk modification* (RM) 20 skenario, *risk Avoidance* (RA) 3 skenario dan *risk sharing* (RS) 7 skenario.

Tabel 14 Hasil Penilaian Risiko Keamanan SIMPUS dan Aset TI

No. Skenario Ancaman	*Level* Risiko	Kategori Biaya Pemulihan	Penanganan Risiko
1.	M	H	RS
2.	M	M	RM
3.	M	H	RS
4.	M	H	RS
5.	M	L	RM
6.	M	M	RM
7.	M	L	RM
8.	M	H	RS
9.	M	M	RM
10.	M	H	RS
11.	M	L	RM
12.	M	L	RM
13.	M	M	RM
14.	M	L	RM
15.	M	L	RM
16.	M	H	RS
17.	M	M	RM
18.	M	M	RM
19.	M	M	RM
20.	M	L	RM
21.	M	L	RM
22.	M	L	RM
23.	M	L	RM
24.	M	H	RS
25.	M	L	RM
26.	M	L	RM
27.	H	L	RA
28.	M	L	RM
29.	H	L	RA
30.	H	L	RA

Sumber : hasil penelitian, diolah kembali

F. Rekomendasi

Rekomendasi untuk penanganan risiko pada Puskesmas Pasir Putih diutamakan pada skenario ancaman yang memiliki level risiko *High* (H), dapat dilihat pada Tabel 14, yaitu:

a. Tidak adanya kebijakan dalam penghapusan data aplikasi SIMPUS, rekomendasi berupa pembuatan dan penerapan kebijakan dan SOP (*Standard Operating Procedure*) terkait penghapusan data aplikasi SIMPUS.
b. Tidak pernah dilakukan pengecekan kebenaran data yang di *input* ke aplikasi SIMPUS, rekomendasi berupa pembuatan dan SOP terkait validasi data pada aplikasi SIMPUS.
c. Tidak adanya aturan dalam *print out data* yang ada di aplikasi SIMPUS, rekomendasi berupa pembuatan dan penerapan kebijakan dan SOP terkait *print out data* yang ada di aplikasi SIMPUS.

Selain rekomendasi utama berupa pembuatan dan penerapan kebijakan dan SOP pengelolaan aset utama aplikasi SIMPUS, rekomendasi tambahan yang diberikan kepada Kepala Puskesmas Pasir Putih adalah melakukan pelatihan terhadap pengelola dan pengguna aplikasi SIMPUS. Rekomendasi untuk aset pendukung berupa pengamanan, pemeliharaan, kontrol dan penambahan kebutuhan yang diperlukan guna meminimalkan risiko.

5 KESIMPULAN

Berdasarkan hasil Penelitian ini, telah dilakukan penilaian risiko keamanan data SIMPUS dan aset TI menggunakan ISO 27005/2011. Hasil Penilaian risiko ancaman yang mungkin terjadi rata-rata sedang dan risiko tinggi masih kecil pada ancaman yang mungkin terjadi karena kegiatan pelayanan

masih berjalan baik. Rekomendasi utama Kepala Puskesmas Pasir Putih bahwa penanganan risiko tinggi bisa diatasi dengan adanya kebijakan dan SOP dalam pengelolaan aset utama aplikasi SIMPUS. Pengembangan penelitian selanjutnya berupa penilaian risiko dan/atau penanganan risiko ancaman bisa dikurangi atau diatasi agar pelayanan tetap berjalan dengan baik.

Commented [U2]: Berdasarkan apa rekomendasi ini diberikan? Hindari kesan rekomendasi ini muncul secara tiba-tiba. Apakah dengan adanya kebijakan dapat menjamin? Selanjut

REFERENSI

[1] S. Salahuddin, A. Ambarwati, and M. N. A. Azam, "IDENTIFIKASI RISIKO KEAMANAN INFORMASI MENGGUNAKAN ISO 27005 PADA SEBUAH PERGURUAN TINGGI SWASTA DI SURABAYA," *presented at the Seminar Nasional Sistem Informasi 2018, UNMER Malang, 2018*, pp. 990–996.

[2] W. Hermawan, "Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE)," *InComTech*, vol. 9, no. 2, pp. 130–140, Aug. 2019, doi: 10.22441/incomtech.v9i2.6474.

[3] S. M. Jaya, "Perancangan Sistem Keamanan Informasi Berbasis Penilaian Risiko Menggunakan ISO/IEC 27001 Dan ISO/IEC 27005 (Studi Kasus : Kajian Teoritis)," *J. Inform. Inti Talafa*, vol. 7, no. 2, pp. 12–22, 2015.

[4] F. I. S. Yudha and Rd. E. Gunadhi, "Risk Assessment Pada Manajemen Risiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management," *algoritma*, vol. 13, no. 1, pp. 333–340, 2016, doi: 10.33364/algoritma/v.13-2.333.

[5] Asriyanik and Prajoko, "Manajemen Risiko Keamanan Informasi 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.

[6] Asriyanik and Prajoko, "Pengembangan Aplikasi Penilaian Risiko Keamanan Informasi Berbasis ISO 27005 Menggunakan Metode Prototyping," *SANTIKA is a scientific journal of science and technology*, vol. 8, no. 2, pp. 813–822, 2018.

[7] S. Ariyani and M. Sudarma, "Implementation Of The ISO/IEC 27005 In Risk Security Analysis Of Management Information System," *J. Eng. Res. Appl.*, vol. 6, no. 8, pp. 1–6, 2016.

[8] V. Agrawal, "A Framework for the Information Classification in ISO 27005 Standard," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, USA, 2017, pp. 264–269, doi: 10.1109/CSCloud.2017.13.

[9] M. Ghazouani, S. Faris, H. Medromi, and A. Sayouti, "Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk," *IJCA*, vol. 103, no. 8, pp. 36–42, Oct. 2014, doi: 10.5120/18097-9155.

[10] V. Agrawal, "Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard," *Presented at the Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, pp. 101–111, 2016.

[11] Y. Sani, R. E. Indrajit, and M. Hendayun, "PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS MANAJEMEN RISIKO TERHADAP INFRASTRUKTUR TEKNOLOGI INFORMASI (STUDI KASUS: DIVISI SISTEKFO PT. INDUSTRI TELEKOMUNIKASI INDONESIA)," *Infosecure*, vol. 1, no. 2, Art. no. 2, 2020.

[12] R. V. Imbar and A. E. Ayala, "Penerapan Standar Keamanan Informasi Menggunakan Framework ISO/IEC 27005:2011 di Lapan Bandung," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 4, no. 1, pp. 195 – 206, Apr. 2018.

[13] M. T. M. A. Nur, I. Darmawan, and R. Fauzi, "Implementasi Risk Assessment Pada Divisi Teknologi Informasi Di PT. Xyz Menggunakan Iso 27005:2008," vol. 7, no. 1, pp. 2111–2118, Apr. 2020.

[14] W. Yustanti, A. Qoiriah, R. Bisma, and A. Prihanto, "Strategi Identifikasi Risiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018," *JIEET (Journal of Information Engineering and Educational Technology)*, vol. 3, no. 2, Art. no. 2, 2019, doi: 10.26740/jieet.v3n2.p51-56.

[15] 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, doi: 10.33105/itrev.v3i1.20.

[16] H. Himayadi and J. F. Andry, "TATA KELOLA TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT 4.1 PADA PT. DUNIA SAFTINDO," Jurnal SISTEMASI, vol. 8, no. 3, pp. 329–340, 2019.

[17] *International Organization for Standardization, ISO/IEC 27005 : 2008 Information technology-Security techniques-Information security risk management*. UK: International Organization for Standarization, 2008.

[18] *International Organization for Standardization, ISO/IEC 27005 : 2011 Information technology-Security techniques-Information security risk management*. UK: SAI GLOBAL-ILI Publishing, 2011.