Pengukuran Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Metode FMEA dan Framework ISO 27001:2013 pada PT. ABC

Ari Ferdinand*[1], Keysa Naristi[2], Rayhan Abdillah[3], Saffly Diva Walujo[4], Laqma Dica Fitrani[5], Ari Cahaya Puspitaningrum[6]
Program Studi Sistem Informasi, Universitas Hayam Wuruk Perbanas
e-mail: [1]202102021002@mhs.hayamwuruk.ac.id, [2]202102021004@mhs.hayamwuruk.ac.id,
[3]202102021003@mhs.hayamwuruk.ac.id, [4]202102021001@mhs.hayamwuruk.ac.id,
[5]laqma.fitrani@perbanas.ac.id, [6]ari.cahaya@perbanas.ac.id
*Penulis Korespodensi

Diterima: 24 Agustus 2023; Direvisi: 3 Juli 2023; Disetujui: 3 Juli 2024

Abstrak

PT. ABC merupakan perusahaan yang bergerak dibidang jasa pembiayaan seperti peralatan elektronik, rumah tangga, dan kendaraan. Ancaman pada perusahaan sektor jasa pembiayaan juga kerap menjadi perhatian, dikarenakan ancaman yang datang dapat merugikan nasabah maupun stakeholder terkait dan juga merusak citra baik perusahaan salah satu contohnya yaitu tentang kebocoran data digital. Dengan mengangkat isu tentang risiko keamanan aset teknologi informasi mendorong kami untuk melakukan penelitian ini dimana didalamnya menggunakan metode FMEA dan Framework ISO 27001. Penelitian ini bertujuan untuk menganalisis semua risiko keamanan terkait semua aset yang ada diperusahaan dan memberikan rekomendasi tindakan sesuai dengan metode yang digunakan yaitu standar ISO 27001. Dalam penelitian ini terdapat 34 temuan risiko dari beberapa asset IT pada PT. ABC. Beberapa asset yang perlu menjadi fokus perhatian lebih oleh perusahaan antara lain adalah informasi data, server jaringan, hardware berupa computer untuk menghindari risiko dengan level yang tinggi. Hasil penelitian ini diharapkan dapat memberikan panduan praktis bagi PT. ABC dalam mengelola risiko keamanan aset teknologi informasi mereka dengan adanya rekomendasi control ISO 27001 yang telah diberikan.

Kata kunci: *Risiko, Framework ISO 27001, Framework FMEA, CIA*

Abstract

PT. ABC is a company engaged in financing services such as electronic equipment, households and vehicles. Threats to companies in the field of financing services are also often a concern, because threats that come can be detrimental to customers and related stakeholders and damage the company's good image, one example is digital data leaks. By raising the issue of information technology asset security risks, we were encouraged to conduct this research using the FMEA method and ISO 27001 Framework. In this study there were 35 risk findings from several IT assets at PT. ABC. Several assets that need to be the focus of more attention by companies include information data, network servers, hardware computers to avoid high levels of risk. The results of this study are expected to provide practical guidance for PT. ABC in managing the security risk of its information technology assets with the ISO 27001 control recommendations that have been given.

Keywords*: Risk, ISO 27001 Framework, FMEA Framework, CIA*

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat terutama di era industri 4.0 ini dimana banyak dari beberapa perusahaan besar yang menerapkan berbagai macam teknologi informasi untuk membantu mempermudah dan meningkatkan proses bisnis perusahaan supaya perusahaan yang sedang mereka jalankan dapat mengikuti perkembangan saat ini, tetapi dari banyaknya perkembangan teknologi informasi juga tidak menutup kemungkinan banyak risiko yang akan terjadi yang bisa mengancam perusahaan. Jika layanan teknologi tidak tersedia, maka operasional bisnis tidak akan berjalan dengan baik karena peran teknologi sangat penting [1]. Data yang telah dicatat oleh Lembaga Indonesia Secure Incidents Response Team On Internet Infrastructure (ID-SIRTII) pada tahun 2014 sekitar 48,4 juta serangan cyber telah terjadi di Indonesia [2]. Terdapat dua faktor umum penyebab risiko antara lain yaitu faktor *eksternal* dan *internal* [3]. Risiko dari faktor eksternal yaitu risiko yang terkait dengan penyerangan dari pihak luar contohnya seperti pencurian data, serangan virus, *malware*, *hacker*, dan sebagainya. Selain itu, risiko-risiko juga dapat muncul dari faktor internal perusahaan contoh sumber risiko internal salah satunya berasal dari aset *SDM* (Sumber Daya Manusia) didalam perusahaan itu sendiri. Untuk menghindari risiko-risiko yang muncul dari perkembangan teknologi informasi perusahaan juga perlu menerapkan standar manajemen risiko teknologi informasi.

Pentingnya memperhatikan keamanan aset menjadi salah satu hal yang krusial dalam perusahaan atau organisasi. Setiap aset yang ada dapat menimbulkam berbagai risiko bagi perusahaan atau organisasi. Sehingga, asset pada suatu perusahaan harus memenuhi standart keamanan supaya terhindar dari risiko yang dapat menyebabkan kegagalan dan kerugian baik secara finansial maupun produktivitas pada perusahaan atau organisasi. Prinsip keamanan informasi didasarkan pada tiga aspek utama CIA, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Seiring dengan perkembangan teknologi informasi, prinsip-prinsip tersebut telah berkembang menjadi konsep yang lebih komprehensif yang dikenal sebagai CIA+. CIA+ meliputi prinsip-prinsip awal tersebut (kerahasiaan, integritas, dan ketersediaan), serta beberapa prinsip tambahan seperti privasi, identifikasi, otentikasi, otorisasi, dan akuntabilitas [4].

PT. ABC merupakan perusahaan yang bergerak dibidang jasa pembiayaan seperti peralatan elektronik, rumah tangga, dan kendaraan. Perusahaan telah menjalankan kegiatan operasionalnya di 246 lokasi di seluruh Indonesia, yang terdiri dari 191 kantor cabang dan 55 titik layanan. Jumlah total konsumen pada tahun 2009 yang pernah dan sedang mendapatkan pembiayaan dari PT. ABC mencapai lebih dari 4 juta orang dan telah membiayai lebih dari 714 ribu unit kendaraan bermotor baru. Total aset perusahaan pada saat itu melebihi 10 triliun rupiah.

Risiko seringkali menjadi faktor pembatas dalam operasi organisasi untuk mencapai tujuan [5]. Ketika terjadi insiden atau bencana, organisasi umumnya akan mengalami kerugian [6]. Ancaman pada perusahaan sektor jasa pembiayaan juga kerap menjadi perhatian, dikarenakan ancaman yang datang dapat merugikan nasabah maupun *stakeholder* terkait dan juga merusak citra baik perusahaan. Sebagai contoh, pada Mei 2020, telah terjadi insiden kebocoran data di salah satu platform *e-commerce* yang melibatkan 91 juta pengguna. Data yang terdampak mencakup informasi seperti alamat email, nama pengguna, dan kata sandi. Kemudian, data tersebut dijual di pasar dengan nilai sekitar US$ 5000,- atau setara dengan Rp74,5 juta [7]. Selain itu, diungkapkan bahwa kebocoran data Bank Indonesia diduga disebabkan oleh aksi kolaborasi kelompok peretas Conti ransomware. Mereka berhasil meretas data sebanyak 487 MB dari 16 komputer pribadi (PC) pada tanggal 21 Januari 2022. Pada tanggal 24 Januari 2022, jumlah dokumen yang terdampak meningkat menjadi 52.767 dengan total kapasitas data sebesar 74 gigabyte (GB) [8]. Dari beberapa kasus yang telah di paparkan oleh peneliti, terlihat bahwa kebocoran data merupakan ancaman yang sangat membutuhkan perhatian khusus dan harus dihindari. Oleh karena itu aset IT pada PT. ABC yang menyangkut dengan pengelolaan dan penyimpanan data nasabah harus benar-benar dijaga keamanannya.

ISO 27001 memberikan dukungan dalam pengelolaan risiko keamanan dengan menyediakan standar untuk Sistem Manajemen Keamanan Informasi (*Information Security*

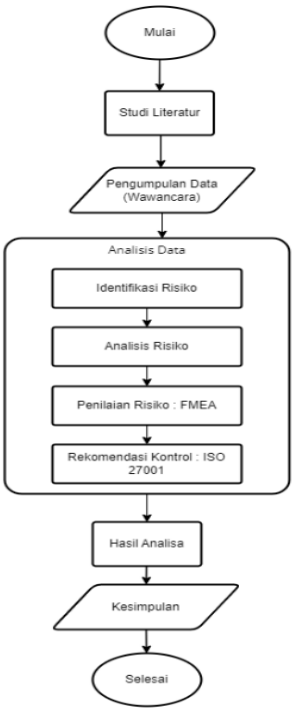
Management System/ISMS). ISO 27001 menyajikan kerangka kerja dan langkah-langkah umum yang harus diikuti oleh sebuah perusahaan atau organisasi dalam hal evaluasi, penerapan, dan pemeliharaan keamanan aset teknologi informasinya berdasarkan praktik terbaik dalam keamanan informasi [9].

Metode *FMEA* dan *Framework ISO 27001* ini sebelumnya sudah pernah diterapkan untuk manajemen risiko teknologi informasi oleh banyak perusahaan. Pada penelitian sebelumnya yang terdapat pada jurnal lain mengatakan bahwa penggunaan *Failure Mode and Effect Analysis* (*FMEA*) bertujuan untuk menilai dampak dari risiko sebagai alat ukur nilai RPN risiko aset kritis [10]. Tidak hanya menggunakan metode FMEA tetapi juga menggunakan kolaborasi dari standar ISO 27001 ini digunakan untuk mengelola, menganalisis, dan mengevaluasi berbagai cara dalam pengendalian ancaman dan risiko [11].

Dengan mengangkat isu tentang risiko keamanan aset teknologi informasi mendorong kami untuk melakukan penelitian ini dimana didalamnya menggunakan metode FMEA dan *Framework* ISO 27001. Penelitian ini bertujuan untuk menganalisis semua risiko keamanan terkait semua aset yang ada diperusahaan dan memberikan rekomendasi tindakan sesuai dengan metode yang digunakan yaitu standar ISO 27001. Penelitian ini diharapkan supaya PT. ABC dapat memiliki pedoman terkait langkah-langkah yang harus dilakukan ketika sewaktu-waktu suatu risiko terjadi pada perusahaan, agar risiko tersebut tidak menimbulkan kerugian yang fatal akibat perusahaan tidak memiliki rencana tindakan yang harus diambil.

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini yaitu dengan pendekatan kualitatif serta menerapkan Framework ISO 27001 dan metode FMEA.



Gambar 1. *Flowchart* Penelitian

Gambar 1 merupakan *flowchart* penelitian dari tahapan saat proses penelitian dilakukan. Tahapan dalam penerapan *Framework* ISO 27001 dan metode FMEA. Tahapan awal dalam penelitian ini yaitu melakukan proses wawancara dengan pihak perusahaan untuk mendapat

bahan penelitian, selanjutnya melakukan studi literatur dengan mengumpulkan data pustaka, mencari dan membaca dari berbagai sumber pustaka, setelah studi literatur dilakukan langkan berikutnya yaitu mengidentifikasi risiko atau masalah untuk mengetahui risiko, ancaman, dan kerentanan yang bisa terjadi pada kegiatan yang berkaitan dengan aset perusahaan, setelah risiko-risiko teridentifikasi dilakukan analisis dari risiko tersebut untuk mengetahui probabilitas risiko terjadi, kemudian melakukan penilaian risiko sesuai dengan metode FMEA untuk mengukur dampak yang akan ditimbulkan suatu risiko, yang terakhir yaitu rekomendasi kontrol berdasarkan pada standar ISO 27001 untuk menentukan pengendalian dan pertimbangan untuk penangan dari semua risiko perusahaan. Berikut tahapan yang dilakukan berdasarkan daripenelitian yang dilakukan.

2.1 Studi Literatur

Studi literatur melibatkan analisis terhadap penelitian sebelumnya yang relevan dengan topik penelitian yang sedang dilakukan [12]. Metode studi literatur ini bertujuan untuk memperoleh pemikiran terkini tentang teori dan metodologi yang sesuai dengan landasan penelitian yang penulis lakukan. Dalam penelitian ini studi literatur dilakukan dengan membaca beberapa referensi penelitian terdahulu, mencari isu-isu terkait dengan permasalahan yang diangkat dan mempelajari kerangka kerja metodologi penelitian terkait dengan manajemen risiko keamanan aset menggunakan *framework* ISO 27001 dan *FMEA*.

2.2 Wawancara

Wanwancara merupakan kegiatan pengumpulan data untuk menunjang kebutuhan informasi dalam penilitian yang sedang dilakukan. Wawancara dalam penelitian ini dilakukan untuk mendapat data penelitian terkait dengan risiko keamanan aset perusahaan yang berkaitan dengan teknologi informasi. Asset perusahaan yang digunakan antara lain aset *database, software, hardware, networ*k dan SDM.

2.3 Analisis Data

Pada tahap ini data yang telah terkumpul dari hasil wawancara selanjutnya dilakukan analisis untuk mendapat hasil dan kesimpulan analisis. Analisis data terdiri dari beberapa tahap antara lain identifikasi risiko, analisis risiko, penilaian risiko dengan *FMEA*, dan rekomendasi kontrol berdasarkan *framework* ISO 27001.

a) Identifikasi Risiko

Identifikasi risiko dilakukan ketika telah mendapatkan data risiko yang diambil dari proses wawancara kemudian risiko-risiko tersebut diidentifikasi ancaman, kerentanan, klasifikasi, dampak dan kecenderungannya.

b) Analisis Risiko CIA

Analisis risiko merupakan pengukuran terkait CIA yaitu : 1) *Confidentaly* yang terkait dengan tingkat kerahasiaan aset dan terkait pengelolaan hak akses [13]; 2) *Integrity* yang terkait dengan penjagaan aset untuk menghindari kegiatan manipulasi dari pihak luar [14]; 3) *Availability* yang terkait dengan ketersediaan informasi [15]

Setiap risiko diberi nilai CIA dengan skala nilai 1-3 dan sesuai dengan parameter CIA. Setelah itu di tentukan aset valuenya dengan mengalikan ketiga pengukuran CIA lalu dibagi dengan 3.

c) Penilaian Risiko FMEA

Setelah mengidentifikasi dan menganalisis risiko, tahapan selanjutnya adalah melakukan penilaian risiko menggunakan *framework FMEA* yang meliputi beberapa tahapan yaitu [16] : 1) Melakukan tinjauan dan identifikasi kegagalan dalam proses; 2) Membuat kriteria dampak keparahan (S), kemungkinan terjadi (O), dan kemungkinan kegagalan deteksi (D); 3) Menetapkan peringkat keparahan (S); 4) Menentukan peringkat kemungkinan terjadi (O); 5) Menentukan

peringkat kemungkinan kegagalan deteksi (D); 6) Menghitung angka prioritas Risiko (Risk Priority Number/RPN); 7) Menyusun urutan prioritas kegagalan berdasarkan hasil perhitungan RPN; 8) Menyusun rencana tindakan penanganan atau pengendalian untuk mengurangi risiko kegagalan

d) Rekomendasi Kontrol ISO 27001

Pada tahapan ini dilakukan rekomendasi kontrol tindakan yag harus dilakukan pada risiko di setiap aset IT yang telah diidentifikasi sebelumnya. Rekomendasi kontrol tindakan yang diberikan berasal dari annex ISO 27001. ISO 27001 adalah sebuah kerangka standar yang di akui secara internasional yang mengatur tentang manajemen keamanan SI/TI [17].

2.4 Kesimpulan

Tahapan terakhir adalah kesimpulan dimana berisi suatu rangkuman atau hasil akhir penelitian yang diperoleh setelah mengolah data-data menjadi suatu informasi terkait dengan manajemen risiko keamanan IT.

3. HASIL DAN PEMBAHASAN

Tabel 1 merupakan tabel identifikasi risiko aset TI PT. ABC yang berisi tentang aset yang ada pada PT. ABC antara lain dapat berupa data, software, network, hardware, SDM. Dari setiap aset tersebut memiliki risiko yang berbeda yang dapat terjadi dengan level risiko 1-10, dalam tabel tersebut juga menjelaskan *current control* yang dapat dilakukan untuk menyelesaikan risiko yang mungkin terjadi.

Tabel 1. Identifikasi risiko

Jenis Aset	Nama *Asset*	Risiko	*Current Control*	Nilai Risiko	Level
Data	Data pelanggan	Kesulitan integrasi data	Memanajemen hak ases sesuai kebutuhan staff	2	*Low*
		Media failure	Memberi informasi ekstensi format file kepada *user*	6	*Medium*
		Corrupt file	Ubah format file, Buka file di program yang berbeda	1	*Low*
		Pencurian data	Memanajemen penyimpanan data, batasi hak akses	9	*High*
	Data karyawan	Pencurian data	Membatasi hak akses data dengan *password*	9	*High*
	Data perusahaan	Pencurian data	Membatasi hak akses data dengan *password*	9	*High*
Software	Sistem Informasi BAF	*Application/Web Crash*	Melakukan pengecekan terhadap *code/syntax* aplikasi secara berkala	9	*High*
	mySQL	Kegagalan mengelola data yang terlalu besar	Memiliki cadangan sistem manajemen *database* selain SQL	3	*Low*
	Xampp	Gagal connect ke phpMyAdmin	Setting ulang hardware, reinstall aplikasi	2	*Low*
	Sublime	Akses fitur terbatas	Membeli aplikasi versi yang berbayar dan resmi	2	*Low*
	Aplikasi desain	Akses fitur terbatas	Membeli aplikasi versi yang berbayar dan resmi	2	*Low*

Jenis Aset	Nama *Asset*	Risiko	*Current Control*	Nilai Risiko	Level
	grafis (adobe/figma, dll)	Memakan banyak storage	Menambah storage device	4	*Low*
	Windows (sistem operasi)	Banyaknya bug	Mengganti versi windows, dan mengurangi jumlah aplikasi dalam device	4	*Low*
		Windows tidak bisa digunakan	Mengaktivasi windows dengan cara membeli lisensi	2	*Low*
		Data lost	Melakukan back up data ke cloud secara berkala, tidak menggunakan internal storage	6	*Medium*
	Server Aplikasi	Server Down	Menyediakan banyak alternatif (jika aplikasi yang down bisa lewat web), banyak melakukan back up data	9	*High*
Network	Server jaringan	Kecepatan akses internet yang lambat	Menaikkan bandwith	9	*High*
Hardware	*Switch*	Port switch rusak	Mengganti port baru	4	*Low*
		Switch hang	Menempatkan pada suhu ruangan dingin agar tidak panas dan hang	4	*Low*
	Router	Router no responses	Mereboot atau merestart router	4	*Low*
	Kabel	Trojan	Membuat prosedur penyimpanan yang aman dan melakukan maintentance	4	*Low*
		Kabel putus	Melakukan perbaikan pada kabel yang terputus	6	*Medium*
	Computer	Serangan Virus	Memasang antivirus Menghindari unduh file dari sumber yang tidak terpercaya	6	*Medium*
		Memori penuh	Mengurangi jumlah software yang terpasang atau mengganti harddisk baru	6	*Medium*
		Kerusakan fisik	Melakukan pemeliharaan hardware dengan menjaga kebersihan hardware secara rutin	4	*Low*
	Server	*Server down*	Menyelidiki penyebab dan mengambil Tindakan untuk memperbaiki	9	*High*
		Server panas	Menyimpan server dalam ruangan yang dingin	6	*Medium*
		Setting server berubah	Pembatasan hak akses setting server dengan password	9	*High*
	CPU	Kerusakan fisik	Membuat prosedur penyimpanan yang aman dan melakukan maintentance hardware	4	*Low*
	Monitor	Kerusakan fisik	Membuat prosedur penyimpanan yang aman dan melakukan maintentance hardware	4	*Low*
	Printer	Kerusakan fisik	Membuat prosedur penyimpanan yang aman dan melakukan maintentance hardware	4	*Low*

Jenis Aset	Nama *Asset*	Risiko	*Current Control*	Nilai Risiko	Level
Sumber Daya Manusia/ people	Staff	Penyalahgunaan hak akses	Memanajemen hak akses staff dengan baik	9	*High*
		Ketidakpahaman staff	Memberikan pelatihan pemahaman staff terhadap fitur-fitur dan kegunaan aplikasi	4	*Low*
	Vendor	Ketidaksempuraan layanan vendor	Bijak dalam memilih vendor, mengganti vendor saat masa kontrak habis	6	*Medium*

Tabel 2 merupakan tabel analisis risiko CIA yang berisi tentang penilaian aset terkait dengan *Confidentiality*, *Integrity* dan *Availability* yang memiliki skala penilaian 1-3. Dari hasil penilaian tersebut diperoleh hasil asset value tertinggi yaitu 9 dan yang terendah yaitu 1.

Tabel 2. Analisis Risiko CIA

No	Aset	*Confidentiality*	*Integrity*	*Availability*	*Aset Value*
1	Data	3 (Informasi sangat rahasia dimana terungkapnya Informasi tersebut secara tidak sah akan mengancam keberlangsungan bisnis)	3 (Kebenaran dan keutuhan Informasi sangat dibutuhkan dimana kekeliruan dan kesalahan akan berdampak signifikan terhadap keberlangsungan bisnis)	3 (Ketersedian Informasi sangat dibutuhkan demi keberlangsungan bisnis)	9
2	Sistem Informasi PT. ABC	2 (Apabila Software /aplikasi digunakan oleh personal secara tidak sah dapat diatasi dengan baik sehingga tidak berdampak secara signifikan pada keberlangsungan bisnis)	3 (Apabila software/ aplikasi dimodifikasi oleh personel yang tidak berwenang dapat berdampak signifikan pada keberlansungan bisnis)	3 (Apabila software/aplikasi tidak tersedia selama jam kerja normal dapat mengganggu keberlangsungan bisnis)	6
3	Server Aplikasi	3 (Apabila Software /aplikasi digunakan oleh personal secara tidak sah akan berdampak negatif pada keberlangsungan bisnis)	3 (Apabila software/ aplikasi dimodifikasi oleh personel yang tidak berwenang dapat berdampak signifikan pada keberlansungan bisnis)	3 (Apabila software/aplikasi tidak tersedia selama jam kerja normal dapat mengganggu keberlangsungan bisnis)	9
4	Server Jaringan	3 (Apabila Software /aplikasi digunakan oleh personal secara tidak sah akan berdampak negatif pada keberlangsungan bisnis	3 (Apabila software/ aplikasi dimodifikasi oleh personel yang tidak berwenang dapat berdampak signifikan pada keberlansungan bisnis)	3 (Apabila software/aplikasi tidak tersedia selama jam kerja normal dapat mengganggu keberlangsungan bisnis	9

No	Aset	*Confidentiality*	*Integrity*	*Availability*	*Aset Value*
5	*Hardware*		2 (Apabila hardware dapat dimodifikasi oleh personel yang tidak berwenang tidak berdampak signifikan pada keberlangsungan bisnis)	2 (Apabila hardware tidak dapat diakses selama jam kerja normal tidak berdampak sangat signifikan terhadap keberlangsungan bisnis)	2
6	Sumber Daya Manusia			3 (Ketersediaan orang sangat dibutuhkan dan apabila ketidaktersediaan/ketidakhadiran orang akan berdampak signifikan pada keberlangsungan bisnis	3

Tabel 3 merupakan tabel penilaian risiko *FMEA* yang berisi tentang penilaian risiko berdasarkan *Security*, *Occurance* dan *Detection* yang memiliki skala penilaian 1-10. Dimana setiap nilai atau ranking memiliki probablitias dan periode waktu risiko yang berbeda-beda. Dari penilaian tersebut diperoleh nilai RPN yang berasal dari hasil perkalian ketiga nilai (*Security*, *Occurance* dan *Detection*) dimana nilai tertinggi diperoleh 180 (*high*) dan nilai terendah yaitu 10 (*very low*).

Penilaian risiko dilakukan dengan menggunakan metode FMEA yaitu memberikan skor *Severity* (S), *Occurrence* (O) dan *Detection* (D) sesuai standar FMEA yang sudah ditetapkan tim analisis dan perhitungan RPN dengan rumus pada persamaan 1 berikut:

$$RPN = (S) \times (O) \times (D) \quad (1)$$

Hasil perhitungan RPN risiko dapat dilihat pada tabel 3 berikut:

Tabel 3. Penilaian risiko *FMEA*

Asset	Nama Aset	Risiko	Sev	Occ	Dec	RPN	*Level*
Data	Data pelanggan	Kesulitan integrasi data	3	2	3	18	*Very Low*
		Media failure	7	1	2	14	*Very Low*
		Corrupt file	7	2	3	42	*Very Low*
		Pencurian data	10	5	3	150	*Medium*
	Data karyawan	Pencurian data	10	5	3	150	*Medium*
	Data perusahaan	Pencurian data	10	5	3	150	*Medium*
Software	Sistem Informasi	Application/Web Crash	10	3	6	180	*High*
	mySQL	Kegagalan mengelola data yang terlalu besar	10	5	2	100	*Low*
	Xampp	Gagal connect ke phpMyAdmin	5	1	2	10	*Very Low*
	Sublime	Akses fitur terbatas	6	2	2	24	*Very Low*
	Aplikasi desain grafis (adobe/figma, dll)	Akses fitur terbatas	5	2	2	20	*Very Low*
	Sistem Operasi	Memakan banyak storage	5	3	2	30	*Very Low*
		Banyaknya bug	6	3	2	36	*Very Low*

Asset	Nama Aset	Risiko	Sev	Occ	Dec	RPN	*Level*
		Windows tidak bisa digunakan	6	3	2	30	*Very Low*
		Data lost	8	3	2	30	*Very Low*
	Server Aplikasi	Server Down	10	5	3	150	*Medium*
Network	Server jaringan	Kecepatan akses internet yang lambat	10	5	2	100	*Low*
Hardware	Switch	Port switch rusak	8	2	5	80	*Low*
		Switch hang	8	2	5	80	*Low*
	Router	Router no responses	10	5	2	100	*Low*
	Kabel	Trojan	8	2	5	80	*Low*
		Kabel putus	8	2	5	80	*Low*
	Computer	Serangan Virus	10	4	4	160	*High*
		Memori penuh	5	3	2	30	*Very Low*
		Kerusakan fisik	8	2	5	80	*Low*
	Komputer	Server down	8	2	5	80	*Low*
	Server	Server panas	8	2	5	80	*Low*
		Setting server berubah	9	3	2	54	*Low*
	CPU	Kerusakan fisik	5	2	2	20	*Very Low*
	Monitor	Kerusakan fisik	5	2	2	20	*Very Low*
	Printer	Kerusakan fisik	5	2	2	20	*Very Low*
Sumber Daya Manusia/ people	Staff	Penyalahgunaan hak akses	9	3	5	135	*Medium*
	Vendor	Ketidakpahaman staff	8	5	2	80	*Low*
		Ketidaksempurnaan layanan vendor	10	3	2	60	*Low*

Tabel 4 merupakan tabel rekomendasi dari klausul ISO 27001 yang berisi tentang rekomendasi kontrol risiko berdasarkan pedoman ISO 27001 yang dipetakan dan disesuaikan di setiap aset yang memiliki risiko *high*. Selain itu terdapat juga keterangan rekomendasi kontrol risiko ISO 27001 yang sudah diterapkan dan belum diterapkan pada PT. ABC.

Tabel 4. Rekomendasi kontrol ISO 27001

Clasificati on Asset	Nama Aset	Risiko	Klausul (berdasarkan ISO 27001)	Mitigasi Risiko dan Adopsi
Software	Sistem Informasi	*Application/ Web Crash*	A.9.4.5 *Access control to program source code* A.13.1.1 *Network control* A.14.2.4 *Restriction on changes to software packages*	1. Memenuhi persyaratan ISO 27001:2013 2. Melakukan *review* hak akses / interval yang diperlukan 3. Membuat mekanisme monitoring hak akses user 4. Mendefinisikan prosedur pengelolaan jaringan 5. Mendefinisikan prosedur pengamanan aplikasi *services* pada network publik dengan instalasi SSL yang akan dilakukan
Hardware	Serangan Virus	Serangan virus	A.12.2.1 *Control against Malware*	1. Mendefinisikan prosedur *backup* 2. Mendefinisikan antivirus dan pergantian *password* 3. Membuat *backup*/cadangan informasi maupun *software* yang disimpan pada sistem harus diambil dan diuji secara

Clasificati on Asset	Nama Aset	Risiko	Klausul (berdasarkan ISO 27001)	Mitigasi Risiko dan Adopsi
				teratur sesuai dengan regulasi terkait kegiatan *backup* yang telah dibuat

4. KESIMPULAN

Berdasarkan penelitian tentang manajemen risiko yang telah dilakukan di PT. ABC dapat disimpulkan bahwa dalam penelitian ini terdapat 34 temuan risiko dari beberapa asset IT pada PT. ABC. Beberapa asset yang perlu menjadi fokus perhatian lebih oleh perusahaan antara lain adalah informasi data, server jaringan, hardware berupa computer untuk menghindari risiko dengan level yang tinggi. Penilaian RPN menggunakan metode FMEA dikelompokkan menjadi empat tingkatan risiko. Hasil penilaian risiko pada penelitian ini teridentifikasi 14 risiko dengan tingkat risiko sangat rendah (very low), 13 risiko dengan tingkat risiko rendah (low), 5 risiko dengan tingkat risiko sedang (medium), 2 risiko dengan tingkat risiko tinggi (high dan tidak ada risiko dengan tingkat risiko sangat tinggi (very high). Adapun rekomendasi mitigasi risiko sesuai dengan *framework* ISO 27001 yang diberikan untuk mencegah kemungkinan terjadinya risiko. Rekomendasi mitigasi risiko sesuai annex ISO 27001 hanya diterapkan pada risiko yang memiliki nilai paling tinggi yaitu pada *software* yaitu adanya *web crash* dan *hardware* adanya serangan virus.

5. SARAN

Berdasarkan hasil dan kesimpulan yang telah diperoleh, peneliti memberikan rekomendasi kepada peneliti yang akan melakukan penelitian serupa di masa mendatang. Rekomendasi tersebut dengan memperluas penelitian dan menambahkan tinjaun terkini sesuai dengan kemajuan teknologi yang sedang terjadi. Rekomendasi yang diberikan bisa untuk diimplementasikan, dilanjutkan, dan bahkan ditambahkan sebagai dasar dalam merumuskan kebijakan dan pengendalian di perusahaan atau organisasi yang sedang dilakukan penelitian.

DAFTAR PUSTAKA

[1] L. D. Fitrani, A. C. Puspitaningrum, U. Hayam, W. Perbanas, J. Timur, and S. I. Akademik, "Utilization of Unified Modeling Language (UML) in the Design of Academic Information Systems based on the OOAD Method," vol. 12, pp. 614–625, 2023.

[2] W. B. M. Setiyawan, E. Churniawan, and F. S. Faried, "Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State," *J. USM Law Rev.*, vol. 3, no. 2, pp. 275–295, 2020.

[3] A. M. Nuris, A. Maharani, and R. N. Rachmadita, "Analisis Risiko Proyek Pengembangan Perangkat Lunak Menggunakan Kerangka Kerja ISO 31000," *J. METRIS*, vol. 22, no. 02, pp. 73–81, 2022, doi: 10.25170/metris.v22i02.2800.

[4] N. U. Handayani, A. Wibowo, D. P. Sari, Y. Satria, and A. R. Gifari, "Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001," *Teknik*, vol. 39, no. 2, pp. 78–85, 2018, doi: 10.14710/teknik.v39n2.15918.

[5] l. D. Fitrani, "Risk Assesment And Business Impact Analysis as a Basis for The Drafting Disaster Recovery Plan AT Upt-Tik of XYZ University," vol. 7, no. Idc, pp. 321–334, 2022.

[6] L. D. Fitrani, "Risk Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013 At XYZ University," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 891–907, 2022, doi: 10.35957/jatisi.v9i2.1643.

[7] A. Dinata, "Hyperconnected, Ancaman Siber, Kebocoran Data Digital," *27 Agustus*, 2020.

[8] V. B. Kusnandar, "Kebocoran Data Bank Indonesia Terus Bertambah, Naik Jadi 74 GB!," *25 Januari*, 2022. .

[9] P. Februari and F. Fitria, "Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung," *POSITIF J. Sist. dan Teknol. Inf.*, vol. 5, no. 2, p. 97, 2019, doi: 10.31961/positif.v5i2.833.

[10] R. J. Gagas, I. Syah, and F. Febryanto, "Analisis, Evaluasi, Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework Octave Dan Fmea (Studi Kasus: Unit Pengelola Teknis Teknologi Informasi Dan Komunikasi Universitas Xyz)," *J. Khatulistiwa Inform.*, vol. 9, no. 2, pp. 121–133, 2021, doi: 10.31294/jki.v9i2.11368.

[11] L. Munaroh, Y. Amrozi, and R. A. Nurdian, "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013," *Technomedia J.*, vol. 5, no. 2, pp. 167–181, 2020, doi: 10.33050/tmj.v5i2.1377.

[12] N. Butarbutar and A. R. Tanaamah, "Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma)," *J. Inf. Syst. Informatics*, vol. 3, no. 3, pp. 352–362, 2021, doi: 10.51519/journalisi.v3i3.155.

[13] J. R. Woda and R. Bisma, "Pembuatan Dokumen Prosedur Keamanan Informasi Yang Mengacu Pada Cobit 5 dan ISO 27001 : 2013 Pada Badan Pengelola Keuangan Dan Aset Daerah Jawa Timur," *JEISBI Vol. 01 Nomor 01, 2020 (Journal Emerg. Inf. Syst. Bus. Intell. Pembuatan*, vol. 01, pp. 51–59, 2020.

[14] I. M. M. Matin, A. Arini, and L. K. Wardhani, "Analisis Keamanan Informasi Data Center Menggunakan Cobit 5," *J. Tek. Inform.*, vol. 10, no. 2, pp. 119–128, 2018, doi: 10.15408/jti.v10i2.7026.

[15] M. Utomo, A. Holil, N. Ali, and I. Affandi, "900-5781-1-Pb," vol. 1, no. 1, pp. 2–7, 2012.

[16] P. Hanifah and J. S.Suroso, "Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA," *J. Komput. Terap.*, vol. 6, no. Vol. 6 No. 2 (2020), pp. 210–221, 2020, doi: 10.35143/jkt.v6i2.3728.

[17] A. N. R. Fitroh, Muhamad Rizaldi Seputra, Ginanjar Ramadhan, Tania Nur Hafizah Hersyaf, "Pentingnya Implementasi Iso 27001 Dalam Manajemen Keamanan : Sistematika Review," *Semin. Nas. Sains dan Teknol. 2017*, no. November, pp. 1–2, 2017.