Jurnal Ilmiah MEDIA SISFO
Vol. 18, No. 2, Oktober 2024

ISSN: 1978-8126
e-ISSN: 2527-7340

Analisis Manajemen Risiko Teknologi Informasi dengan Metode FMEA dan Kontrol ISO 27001:2013 Pada Perusahaan Kontruksi Kapal

Raizsa Noor J.M.N.[1], Sindy Anggraini[2], Sinta Cahyani Putri[3], Saqira Kailatyah[4], Moh.Hadavid[5], Laqma Dica Fitrani[6], Ari Cahaya Puspitaningrum[7]*

Sistem Informasi[1-7], Fakultas Teknik dan Desain, Universitas Hayam Wuruk Perbanas
Jl. Wonorejo Utara No.16, Wonorejo, Rungkut, Surabaya, Indonesia
202202021009@mhs.hayamwuruk.ac.id[1], 202202021004@mhs.hayamwuruk.ac.id [2],
202202021027@mhs.hayamwuruk.ac.id [3], 202202021018@mhs.hayamwuruk.ac.id[4],
202202021025@mhs.hayamwuruk.ac.id [5], laqma.fitrani@hayamwuruk.ac.id [6], ari.cahaya@perbanas.ac.id [7]

Submitted : **14/07/2024**; Reviewed : **26/07/2024**; Accepted : **20/09/2024**; Published : **31/10/2024**

Abstract

PT XYZ is one of the shipping companies in Indonesia that adopts the use of technology in its business processes. The results of the interview show that the company has risk disruptions in electricity, internet networks, communication between users and servers, which can disrupt the course of business processes in the IT department of PT XYZ. In order to develop a better company in the future, the use of technology is needed in the process, but the main challenge that PT XYZ must overcome is finding solutions to every risk that exists in IT. This research uses the FMEA method with ISO 27001: 2013 to find the best solution to overcome the risks that exist in each of the company's assets, with a research flow from interviews and observations, forming a list of potential failures, analyzing risks, calculating RPN, and forming recommendations. The risk that will be recommended in this study is a very high level risk, because it is classified as a problem that is important enough to immediately find a solution so as not to bring losses to the company in the future. Based on the results of the analysis of the identified assets, it was found that the RPN value of 720 was on computer and server assets. Referring to ISO 27001: 2013 controls, control recommendations include physical protection of equipment and the environment, as well as performing regular data backups to ensure data availability.

Keywords : FMEA, information technology, iso 27001:2013, IT risk management, information systems

Abstrak

PT XYZ merupakan salah satu perusahaan pelayaran di Indonesia yang mengadopsi penggunaan teknologi dalam proses bisnisnya. Hasil wawancara menunjukkan bahwa perusahaan memiliki risiko gangguan pada listrik, jaringan internet, komunikasi antar user dan server yang dapat mengganggu jalannya proses bisnis di departemen TI pada PT XYZ. Untuk mengembangkan perusahaan yang lebih baik kedepannya, penggunaan teknologi sangat dibutuhkan dalam prosesnya, namun tantangan utama yang harus diatasi oleh PT XYZ adalah mencari solusi dari setiap risiko yang ada pada TI. Penelitian ini menggunakan metode FMEA dengan ISO 27001:2013 untuk mencari solusi terbaik dalam mengatasi risiko yang ada pada setiap aset perusahaan, dengan alur penelitian dari wawancara dan observasi, membentuk daftar potensi kegagalan, menganalisa risiko, menghitung RPN, dan membentuk rekomendasi. Risiko yang akan direkomendasikan pada penelitian ini adalah risiko yang memiliki tingkat sangat tinggi, karena tergolong masalah yang cukup penting untuk segera dicarikan solusinya agar tidak membawa kerugian bagi perusahaan di masa yang akan datang. Berdasarkan hasil analisis terhadap aset yang teridentifikasi, didapatkan bahwa nilai RPN sebesar 720 berada pada aset komputer dan server. Mengacu pada kontrol ISO 27001:2013, rekomendasi kontrol meliputi perlindungan fisik peralatan dan lingkungan, serta melakukan backup data secara berkala untuk memastikan ketersediaan data.

Kata kunci : FMEA, informasi teknologi, iso 27001:2013, manajemen risiko IT, sistem informasi

1. Pendahuluan

Seiring perkembangan zaman, sistem informasi dan teknologi informasi terus mengalami peningkatan. Hal ini terlihat dari semakin banyaknya perusahaan dan organisasi yang menggunakan teknologi informasi untuk berbagai kebutuhan, terutama dalam lingkungan perusahaan atau organisasi [1]. Penguatan teknologi informasi sangat penting karena sebagian besar bisnis tidak dapat terus beroperasi dengan sukses jika layanan teknologi informasinya tidak tersedia [2]. Hampir semua bidang usaha memerlukan bantuan sistem informasi untuk mempermudah dan mempercepat pekerjaan, termasuk perusahaan perkapalan di Indonesia. PT. XYZ, sebagai salah satu perusahaan yang memproduksi kapal perang dan kapal niaga, serta menyediakan jasa perbaikan, pemeliharaan, dan overhaul kapal, serta produk rekayasa umum, sangat

ISSN: 1978-8126
e-ISSN: 2527-7340

memerlukan analisis manajemen risiko teknologi informasi dalam operasionalnya. Berdasarkan hasil wawancara dengan salah satu pekerja pada perusahaan PT. XYZ, pada departemen IT di perusahaan tersebut ditemukannya risiko-risiko yang menghambat jalannya proses bisnis, diantarnya risiko ganguan arus listrik, ganguan jaringan internet, ganguan komunikasi antar *user* dengan server dan lain sebagainya. Risiko seringkali menjadi faktor pembatas dalam operasional suatu organisasi untuk mencapai tujuan sehingga perlunya dilakukan evaluasi atau analisa terkait manajemen risiko terkait teknologi informasi [3].

Manajemen Risiko adalah proses identifikasi, pengukuran, dan kontrol keuangan dari sebuah risiko yang mengancam aset dan perusahaan atau proyek [4]. Manajemen resiko TI merupakan proses identifikasi resiko, penilaian resiko, dan pengambilan langkah-langkah untuk menurunkan resiko sampai level yang dapat diterima [5]. Penggunaan teknologi informasi mencakup *hardware*, *software*, informasi, people dan jasa, untuk keperluan dalam proses bisnis di PT. XYZ. Risiko aset yang terjadi di PT. XYZ sendiri meliputi adanya ketidakakuratan data, kehilangan data, keterlambatan informasi, kesalahan konfigurasi, *down time*, serta keterlambatan dalam penyelesaian tugas atau *milestone* yang mengakibatkan penundaan proyek. Dengan demikian manajemen risiko sangat diperlukan bagi departemen IT di PT. XYZ [4].

Salah satu cara dalam melakukan identifikasi dan menilai model kegagalan teknologi informasi dari menerapkan aset informasi, dengan menggunakan metode *Failure Mode and Effects Analysis* (FMEA). Metode FMEA, yakni proses terorganisasi untuk kegagalan dengan mencegah terjadinya menganalisis dan mengidentifikasi serta mampu memprioritaskan sumber penyebab masalah kegagalan. Di sisi lain, ISO 27001:2013 digunakan untuk menghasilkan rekomendasi mitigasi untuk perbaikan risiko [6].

Dalam penerapan FMEA, setiap potensi kegagalan dianalisis berdasarkan dampaknya, frekuensi kejadian, dan kemudahan deteksinya. Dari analisis ini, langkah-langkah mitigasi spesifik dapat dirumuskan untuk mengurangi risiko yang terkait dengan teknologi informasi. Pendekatan ini tidak hanya membantu mengidentifikasi risiko, tetapi juga membantu menentukan prioritas tindakan yang diperlukan untuk menjaga keandalan dan integritas aset informasi [6]. Untuk melengkapi analisis FMEA, standar ISO 27001:2013 dapat digunakan sebagai panduan dalam menyusun rekomendasi mitigasi risiko. ISO 27001:2013 menyediakan kerangka kerja yang komprehensif untuk manajemen risiko teknologi informasi [7]. Standar ini membantu organisasi dalam mengidentifikasi, mengelola, dan mengurangi risiko yang berkaitan dengan keamanan informasi, sehingga memastikan perlindungan yang lebih optimal terhadap aset informasi yang kritis [8].

Menggabungkan kedua pendekatan ini—FMEA untuk analisis kegagalan dan ISO 27001:2013 untuk mitigasi risiko—akan memberikan organisasi panduan yang kokoh dalam mengelola risiko teknologi informasi secara efektif [9]. Dengan demikian, organisasi tidak hanya dapat mengidentifikasi dan mengatasi potensi masalah sebelum muncul, tetapi juga dapat membangun kerangka kerja yang kuat untuk perlindungan jangka panjang aset informasi mereka. Pada penelitian ini diawali dengan langkah wawancara dan observasi oleh salah satu pekerja di perusahaan PT. XYZ. Dari hasil pengumpulan data tersebut akan dilakukannya pembentukkan daftar potensi kegagalan dari data yang telah dikumpulkan sebelumnya, yang kemudian akan dilakukan analisis penyebab risiko, dampak, dan frekuensi terjadinya masalah tersebut. Setelah itu, dari hasil pengelompokkan dan analisis tersebut akan dilanjutkan untuk perhitungan RPN dengan menggunakan metode FMEA, sehingga terlihat klasifikasi dari masing-masing masalah sesuai golongan level risiko yang mana nantinya akan dilakukan pembentukkan rekomendasi operasi untuk menanggulangi kegagalan tersebut berdasarkan kontrol ISO 27001:2013. Berdasarkan uraian dari pendahuluan di atas, maka penulis menjadikan topik penelitian berjudul "Analisis Manajemen Risiko Teknologi Informasi dengan Metode FMEA dan Kontrol ISO 27001:2013". Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan informasi dan melindungi aset-aset kritis perusahaan dari berbagai ancaman potensial.

2. Metodologi

Alur penelitian ini menggunakan langkah demi langkah yang dilalui selama proses penelitian. Alur penelitian dimulai dari analisis proses bisnis perusahaan, membentuk daftar potensi kegagalan, analisis penyebab risiko, dampak, dan frekuensi, kemudian dilakukan perhitungan RPN, dan diakhiri membentuk rekomendasi operasi untuk menanggulangi kegagalan seperti yang dapat dilihat pada Gambar 1.

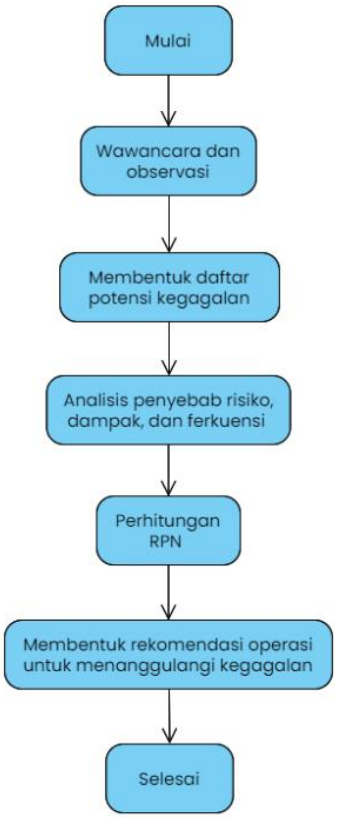
2.1. Wawancara dan Observasi

ISSN: 1978-8126
e-ISSN: 2527-7340

Dalam tahap ini langkah awal dimulai dengan melakukan wawancara dan observasi terkait departemen IT yang ada di PT. XYZ. Hasil wawancara tersebut yang terkumpul akan menghasilkan informasi-informasi, baik berupa aset, proses bisnis, maupun masalah yang terjadi di departemen IT perusahaan tersebut. Kemudian, dilanjutkan dengan menganalisis proses bisnis yang terjadi dan masih digunakan departemen tersebut yang nantinya akan dilanjutkan pada langkah berikutnya dengan menggunakan hasil wawancara yang membantu mengidentifikasi aset-aset yang dimiliki oleh departemen IT, seperti *hardware*, *software*, dan infrastruktur pendukung. Informasi ini penting untuk memahami sumber daya yang tersedia dan bagaimana mereka digunakan dalam mendukung operasional perusahaan [10].

2.2. Membentuk Daftar Potensi Kegagalan

Setelah menganalisis proses bisnis departemen IT tersebut, langkah selanjutnya yakni membuat daftar potensi terjadinya kegagalan berdasarkan tingkat keparahan, kejadian, dan deteksi kegagalan pada masing-masing aset yang digunakan di departemen IT [11]. Daftar yang dibuat meliputi dari potensi kegagalan yang terjadi pada asset bidang data, *hardware*, *software*, dan sumber daya manusia, seperti halnya ketidak akuratan data, kebocoran data, *downtime*, sampai kecelakaan kerja.



Gambar 1. *Alur Penelitian*

2.3. Analisis Penyebab Risiko, Dampak, dan Frekuensi

Tahap ini melanjutkan dari tahap sebelumnya, yang mana setelah terbentuk daftar potensi kegagalan setiap aset yang ada, maka dianalisis penyebab risiko yang terjadi pada aset tersebut, kemudian dianalisis dampak apa yang nantinya berimbas jika risiko tersebut tidak diselesaikan, dan terakhir dianalisis banyak frekuensi terjadinya risiko tersebut.

2.4. Perhitungan RPN

Setelah menyelesaikan tahap-tahap sebelumnya, akan dilakukan perhitungan Risk Priority Number (RPN) yang dilihat berdasarkan 3 aspek, yaitu *Severity* (Sev), *Occurrence* (Occ), dan *Detectability* (Dec). Hasil

ISSN: 1978-8126
e-ISSN: 2527-7340

dari perhitungan nilai RPN tersebutlah yang nantinya dapat menunjukkan level risiko dari permasalahan aset tersebut, apakah ada pada level *Very Low, Low, Medium, High,* atau *Very High* [11] .

Tabel 2. *Tabel Indikator Severity*

Dampak	Kriteria	Ranking
Berbahaya: Tanpa Peringatan	Melukai pekerja/pihak ketiga/*customer*	10
Berbahaya: Tanpa peringatan	Kegiatan yang tidak diperbolehkan oleh perusahaan	9
Sangat tinggi	Kesalahan dalam penggunaan alat yang ada	8
Tinggi	Menyebabkan *complain* dari pihak ketiga/*customer*	7
Sedang	Menyebabkan kerugian untuk perusahaan	6
Rendah	Menyebabkan penurunan kinerja dari pekerja	5
Sangat rendah	Menyebabkan sedikit kerugian	4
Minor	Menyebabkan gangguan kecil yang dapat diatasi tanpa kehilangan sesuatu	3
Sangat minor	Tanpa disadari dan memberikan dampak kecil pada kinerja	2
Tidak terdampak	Tanpa disadari dan tidak mempengaruhi kinerja	1

Tabel 3. *Tabel Indikator Occurrence*

Probabilitas Risiko	Periode Waktu	Ranking
Sangat tinggi	Lebih dari satu tiap harinya	10
Failure is almost inevitable	Satu kali dalam 4 hari	9
Tinggi: secara umum terkait dengan proses yang sebelumnya sering kali gagal	Satu kali dalam seminggu	8
Proses yang sering kali gagal	Satu kali dalam sebulan	7
Moderate: secara umum terkait dengan proses yang sebelumnya sering kali gagal	Satu kali setiap 3 bulan	6
Proses sebelumnya yang memiliki	Satu kali setiap 6 bulan	5
Kegagalan yang pernah terjadi, tapi tidak dalam proporsi yang besar	Satu kali dalam setahun	4
Rendah: Kegaglan hanya terisola terkait dengan proses serupa	Satu kali dalam 1-3 tahun	3
Sangat rendah: Kegagalan hanya terisolasi terkait dengan proses yang hamper sama	Satu kali dalam 3-6 tahun	2
Remote: Kegagalan tidak mungkan terjadi, tidak ada kegagalan yang terkait dengan proses yang hampir serupa	Satu kali dalam 6-100 tahun	1

Tabel 4. *Tabel Indikator Detectability*

Effect	*Detection effect for FMEA*	*Ranking*
Hampir tidak mungkin	Alat control hampir tidak dapat melaksanakan deteksi yang menyebabkan kegagalan	10
Sangat jarang	Inspektor tidak dapat mendeteksi kegagalan	9
Jarang	Pengendali sangat sulit terdeteksi sebab kegagalan	8
Sangat rendah	Performa pengendalian sangat lemah	7
Rendah	Kemampuan pengendalian deteksi kegagalan lemah	6
Sedang	Pengendalian deteksi sedang	5
Agak tinggi	Kesalahan pengontrol menyebabkan kemampuan deteksi cukup tinggi	4
Tinggi	Kemampuan alat control melaksanakan deteksi sebab kegagalan tinggi	3
Sangat tinggi	Tinggi kesalahan pengontrol menyebabkan kemampuan deteksi sangat tinggi	2

ISSN: 1978-8126
e-ISSN: 2527-7340

Effect	*Detection effect for FMEA*	*Ranking*
Hampir pasti	Alat control saat ini hampir pasti mampu mendeteksi penyebab kegagalan	1

Tabel 5. *Tabel Skala RPN*

RPN	Level Risiko
200>	*Very high*
151- 200	*High*
101 – 150	*Medium*
51 – 100	*Low*
0 – 50	*Very low*

2.5. Membentuk Rekomendasi Operasi Untuk Menanggulangi Kegagalan

Dari hasil analisis dan perhitungan RPN, dapat diusulkan beberapa rekomendasi untuk mengatasi risiko yang terjadi pada aset di departemen IT perusahaan PT. XYZ, dengan mengacu pada standar ISO 27001:2013. Standar ini menekankan pentingnya penerapan manajemen resiko TI yang mencakup langkah-langkah untuk mengidentifikasi, menilai, dan mengelola risiko teknologi informasi secara sistematis dalam konteks manajemen risiko TI [12]. Pendekatan ini tidak hanya memastikan perlindungan yang memadai terhadap aset-aset kritis, tetapi juga membantu dalam mencapai kepatuhan terhadap standar internasional yang diatur dalam ISO 27001:2013, yang mencakup persyaratan untuk keamanan data, mitigasi risiko, dan kontinuitas bisnis dalam manajemen risiko TI.

3. Hasil dan Pembahasan

Hasil penelitian ini digambarkan dalam bentuk beberapa tabel di bawah ini. Adapun pada tabel 3.1 menjelaskan mengenai perhitungan risiko dengan metode FMEA dari aset-aset perusahaan PT. XYZ departement IT yang ada.

Tabel 6. *Perhitungan FMEA pasa Risiko Aset Perusahaan*

Jenis Aset	**Nama Aset**	***No. Cause Failure***	**Risiko**	***Potential Cause***	**Sev**	**Occ**	**Dec**	**RPN**	**Level Risiko**
Hardware	Print, *Fotocopy*, Scan	1	Kebocoran tinta saat mencetak/print dalam *fotocopy*	Pengelolaan mesin cetak yang tidak dirawat, diperhatikan, dan dipelihara secara teratur	6	7	6	252	*Very High*
	Komputer	2	Kegagalan komponen seperti *hard disk*, RAM, atau *motherboard* yang dapat menyebabkan hilangnya data	Durasi kegiatan untuk *maintance* perangkat yang tidak teratur	10	9	8	720	*Very High*
	CPU	3	Kerusakan komponen internal yang mengakibatkan CPU tidak berfungsi	Waktu pemeliharaan dan perbaikan yang tidak teratur, serta ada indikasi ukuran suhu ruang yang kurang kondusif untuk perangkat	10	3	6	180	*High*
	Keyboard	4	Tumpahan cairan, tekanan berlebih, atau kotoran yang masuk ke dalam *keyboard*	Kurangnya perlindungan pada perangkat, baik dari sisi peraturan penggunaan maupun	8	3	6	144	*Medium*

ISSN: 1978-8126
e-ISSN: 2527-7340

Jenis Aset	Nama Aset	*No. Cause Failure*	Risiko	*Potential Cause*	Sev	Occ	Dec	RPN	Level Risiko
				perlindungan fisik perangkat					
	Mouse	5	Terjatuh, terkena cairan, atau penggunaan yang kasar	Kurangnya perlindungan perangkat secara fisik maupun peraturan penggunaan	7	3	5	105	*Medium*
	Server	6	Kerusakan pada komponen seperti *hard disk*, RAM, atau *power supply*	Durasi kegiatan untuk *maintance* perangkat yang tidak teratur, ada kemungkinan suhu ruang yang kurang kondusif untuk perangkat	10	9	8	720	*Very High*
	Access Point	7	Interferensi dari perangkat lain atau hambatan fisik yang mengurangi jangkauan sinyal.	Pemasangan perangkat yang kurang akurat yang menyebabkan ganguan pancaran sinyal	10	2	5	100	*Low*
	Switch	8	Terlalu banyak perangkat yang terhubung dapat menyebabkan *switch* menjadi *overload* dan kinerjanya menurun	Kurangnya kebijakan pemasangan perangkat yang baik dan efisien	9	3	4	108	*Medium*
	Router	*9*	*Router* yang tidak diamankan dapat menjadi sasaran serangan yang mengakibatkan akses tidak sah ke jaringan	Kurangnya kebijakan perlindungan keamanan saat konfigurasi perangkat	8	4	5	160	*High*
	Extender	10	Jaringan yang diperluas oleh extender dapat lebih rentan terhadap serangan jika tidak dikonfigurasi dengan benar	Kebijakan konfigurasi perangkat kurang diperhatikan dan diamankan	8	3	4	96	*Low*
	Kabel LAN	11	Kabel berkualitas rendah atau yang rusak dapat menyebabkan koneksi tidak stabil	Belum ditetapkannya standarisasi kualitas perangkat yang baik, aman, dan minim risiko	7	3	2	42	*Very Low*
Software	IM4	12	Perangkat lunak rentan terhadap serangan peretas (*hacker*)	Kebijakan keamanan perangkat kurang ditingkatkan secara berkala	10	5	7	350	*Very High*
	React.js	13	Permintaan yang tidak sah dapat dikirim dari situs lain	Peningkatan kemanan kurang diterapkan secara rutin	8	4	5	160	*High*
	Node.js	14	Kurangnya logging yang memadai dapat menyulitkan dalam debugging dan pemantauan aplikasi	Pemantau aplikasi kurang ditetapkan secara jelas dan tetap	8	3	3	72	*Low*

ISSN: 1978-8126
e-ISSN: 2527-7340

Jenis Aset	Nama Aset	*No. Cause Failure*	Risiko	*Potential Cause*	Sev	Occ	Dec	RPN	Level Risiko
	MySQL	15	Data sensitif dapat bocor karena kelemahan dalam keamanan basis data atau aplikasi yang mengaksesnya	Keamanan pada basis data kurang diperhatikan dan di-*maintance* secara rutin	9	4	4	144	*Medium*
	Jest	*16*	*Mocking* yang tidak tepat dapat menyebabkan pengujian yang tidak akurat dan sulit untuk dipelihara	Belum adanya kebijakan persiapan sebelum *mocking* dilakukan agar mengurangi terjadinya risiko	6	5	3	90	*Low*
	Postman	17	Postman dapat menyimpan data sensitif seperti API keys, tokens, dan credentials yang bisa diekspos jika tidak dikelola dengan baik	Kurang jelasnya kebijakan, standar SOP, terkait pengelolaan data sensitif	8	3	4	96	*Low*
	IFS	18	IFS menyimpan banyak data sensitif yang bisa menjadi target bagi serangan siber, jika terjadi kegagalan sistem atau gangguan	Lemahnya keamanan perangkat, baik dari sisi peningkatan keamanan atau sistem keamanan yang telah diterapkan	10	5	7	350	*Very High*
	Phyton	19	Python tidak memiliki dukungan bawaan untuk pengembangan aplikasi mobile, yang bisa menyulitkan pengembang yang ingin membuat aplikasi mobile menggunakan Python	Belum ada kebijakan alternatif terkait solusi lain untuk pengembangan aplikasi mobile	8	4	3	96	*Low*
	OUTLOOK, EXCEL	20	Tidak tersimpannya data perusahaan	Kurangnya *maintance* perangkat	2	5	2	20	*Very Low*
	E-OFFICE.	21	Tidak tersimpannya data perusahaan	Kurangnya *maintance* perangkat	3	5	6	90	*Low*
Sumber Daya Manusia	Kepala Divisi	22	Tanggung jawab atas reputasi divisi yang dipimpinnya	Komunikasi yang Tidak Efektif	8	7	6	336	*Very High*
		23	Bertanggung jawab atas keputusan strategis	Analisis Data yang Tidak Memadai	8	7	6	336	*Very High*
		24	Tidak mencapai target operasional	Perencanaan dan Penganggaran yang Buruk	8	7	6	336	*Very High*
	Tenaga Ahli TI	25	Adanya kecelakaan kerja	Kurangnya kebijakan pada SOP kerja yang jelas terkait keamanan dan peraturan kerja	9	2	4	72	*Low*

ISSN: 1978-8126
e-ISSN: 2527-7340

Jenis Aset	Nama Aset	*No. Cause Failure*	Risiko	*Potential Cause*	Sev	Occ	Dec	RPN	Level Risiko
	MSDM	26	Kualitas SDM yang tidak memadai dengan jobdes kerja	Perekrutan pegawai yang kurang menyesuaikan standar yang dibutuhkan perusahaan	7	3	6	126	*Medium*
	Helpdesk	27	Kinerja kerja yang tidak bagus	Kurang dilakukannya evaluasi rutin untuk semua aktivitas kerja yang sudah terlaksana	8	3	6	144	*Medium*
Informasi	*Database Material of List*	28	Ketidakakuratan Data	Kurangnya kebijakan standar pengelolaan data	5	9	4	180	*High*
	Database Biweekly Report	29	Keterlambatan Laporan	Kurangnya *maintenance* terkait proses bisnis dari sistem	4	3	7	84	*Low*
	Database Manajemen Logistik	30	Keterlambatan Informasi	Kurangnya maintenance terkait proses bisnis dari sistem	6	6	5	180	*High*
	Database Schedule tube bundle	31	Kehilangan data	Lemahnya keamanan dan perlindungan data	10	4	5	200	*High*
	Database Document and Archive	32	Kehilangan data	Lemahnya keamanan dan perlindungan data	9	3	6	162	*High*
	Database Project and Construction	33	Ketidakakuratan data	Kurangnya kebijakan standar pengelolaan data	9	3	7	189	*High*
	Database Maintenance and Repair	34	Kehilangan data	Lemahnya keamanan dan perlindungan data	10	2	6	120	*Medium*
	Database Management Information System (MIS)	35	Kehilangan data	Lemahnya keamanan dan perlindungan data	10	3	5	150	*Medium*
Jasa	Penyedia jasa keamanan *cyber*	36	Biaya Pelayanan yang terus meningkat tanpa bisa diukur	Informasi dan data perusahaan yang terus bertambah	8	6	4	192	*High*
	Penyedia jasa layanan *cloud*	37	Satu karyawan hanya memiliki satu akun penyimpanan, yang mana terhubung dengan email karyawan masing-masing	Adanya kebijakan dari jasa layanan sesuai dengan kontrak kerja sama dengan perusahaan	7	4	3	84	*Low*
	Penyedia layanan server	38	Biaya pelayanan server tidak termasuk dengan cara mengatasi penanggulangan bencana alam ataupun kebijakan-kebijakan untuk mengamankan server	Kebijakan perusahaan yang memilih biaya layanan yang terjangkau tanpa memperhatikan risiko ke depannya	9	3	4	108	*Medium*

Setelah perhitungan FMEA dan penentuan level risiko selesai, maka informasi aset-aset tersebut akan dilakukan *shorting* untuk level risiko *very high*. Tingkat risiko paling tinggi itulah yang akan dilakukan

ISSN: 1978-8126
e-ISSN: 2527-7340

rekomendasi solusi berdasarkan kontrol ISO 27001:2013, karena risiko permasalahan aset tersebut sangat penting dan mendesak untuk diatasi demi keberlangsungan perusahaan terutama di departement IT-nya.

Tabel 7. *Shorting Nilai RPN Level Very High*

Nama Aset	No. Cause Failure	Sev	Occ	Dec	RPN	Level Risiko
Print, *Fotocopy*, Scan	1	6	7	6	252	*Very High*
Komputer	2	10	9	8	720	*Very High*
Server	6	10	9	8	720	*Very High*
IM4	12	10	5	7	350	*Very High*
IFS	18	10	5	7	350	*Very High*
Kepala Divisi	22	8	7	6	336	*Very High*
	23	8	7	6	336	*Very High*
	24	8	7	6	336	*Very High*

Di sisi lain, hasil perhitungan FMEA pada table 3.1 sebelumnya akan dikelompokkan berdasarkan kategori matriks level permaslahannya, yaitu *very low*, *low*, *medium*, *high*, dan *very high*. Berikut adalah penggambaran matriks level sesuai dengan level risiko yang terhitung pada metode FMEA.

Tabel 8. *Matrik Level*

		***Occurrence*/Kemungkinan**				
		Very Low	**Low**	**Medium**	**High**	**Very High**
***Severity*/ Dampak**	*Very High*	7, 25, 34	3, 9, 15, 31, 32, 33, 35, 38			2, 6
	High		4, 5, 8, 9, 10, 11, 13, 14, 17, 19, 26, 27, 37	36,	22, 23, 24	
	Medium			16, 30	1	12, 18, 28,
	Low		29	21		
	Very Low			20		

Permasalahan yang tejadi pada aset-aset perusahaan dijabarkan dalam tabel 3.1, yang kemudian dilakukan *shorting* berdasarkan level risiko paling tinggi pada tabel 3.2, berdasarkan kontrol ISO 27001:2013 maka para peneliti menggambarkan point-point penting terkait rekomendasi solusi, annex ISO 27001:2013, hingga informasi kontrol yang ada pada tabel di bawah ini.

Tabel 9. *Rekomendasi Solusi Risiko Dengan ISO 27001:2013*

Nama Aset	No. Kasus Masalah	Risiko	Rekomendasi Solusi	Annex ISO 27001:2013	Kontrol
Print, *Fotocopy*, Scan	1	Kebocoran tinta saat mencetak/print dalam *fotocopy*	Perbaikan pada kerusakan komponen elektronik	A.11.2.1 A.11.2.4	Peralatan perusahaan harus ditempatkan dan dilindungi dari bahaya lingkungan dan peralatan harus dipelihara untuk memastikan ketersediaan.
Komputer	2	Kegagalan komponen seperti hard disk, RAM, atau motherboard yang dapat menyebabkan hilangnya data.	Melakukan *backup* data secara berkala ke media penyimpanan eksternal atau cloud.	A.11.2.4 A.11.1.1 A.11.1.4	Perlindungan fisik terhadap serangan dan peralatan perusahaan harus ditempatkan dan dilindungi dari bahaya lingkungan, peralatan harus dipelihara untuk memastikan ketersediaan.
Server	6	Kerusakan pada komponen seperti hard disk, RAM, atau power supply.	Melakukan *backup* data secara rutin untuk memastikan data dapat dipulihkan jika terjadi kegagalan.	A.11.2.4 A.11.1.1 A.11.1.4 A.12.3.1	Perlindungan fisik terhadap serangan dan peralatan perusahaan harus ditempatkan dan dilindungi dari bahaya lingkungan, peralatan harus dipelihara untuk memastikan ketersediaan dan melakukan cadangan informasi sekala berkala
IM4	12	Perangkat lunak rentan terhadap serangan peretas (*hacker*).	Adanya kontrol deteksi, pencegahan, dan pemulihan dari serangan malware,	A.9.3.1 A.12.2.1	Mengikuti penggunaan informasi dan melindungi terhadap malware dan pengguna yang sesuai kesadaran

ISSN: 1978-8126
e-ISSN: 2527-7340

Nama Aset	No. Kasus Masalah	Risiko	Rekomendasi Solusi	Annex ISO 27001:2013	Kontrol
			baik saat sebelum terjadi, saat terjadi, dan sesudah terjadi serangan.		
IFS	18	IFS menyimpan banyak data sensitif yang bisa menjadi target bagi serangan siber, jika terjadi kegagalan sistem atau gangguan.	Lakukan audit keamanan secara berkala untuk memastikan kepatuhan terhadap standar keamanan yang berlaku. ketersediaan data dan layanan jika terjadi kegagalan.	A.9.3.1 A.12.2.1	Mengikuti penggunaan informasi dan melindungi terhadap malware dan pengguna yang sesuai kesadaran
Kepala Divisi	22	Tanggung jawab atas reputasi divisi yang dipimpinnya.	Posisi ini haruslah ditempati oleh orang yang sudah dipilih secara hati-hati.	A.7.1.1 A.7.2.1	Penempatan sebagai jabatan kepala divisi harus memiliki pertimbangan beberapa aspek, abik dari segi Pendidikan, pengalaman, dan kesesuaian dengan jobdesk di perusahaan.
	23	Bertanggung jawab atas keputusan strategis.	Adanya kemampuan yang memadai sejak awal pemilihan posisi ini.	A.7.2.1	Kepala Divisi juga harus memiliki pengalamn dalam pengambilan Keputusan dari beberapa pertimbangan yang telah ditetapkan oleh Perusahaan dengan cepat dan akurat.
	24	Tidak mencapai target operasional.	Adanya evaluasi setiap kegiatan/proyek, dan pelatihan.	A.7.2.2 A.7.2.3	Melihat informasi-informasi evaluasi terhadap kesalahan lalu untuk merencanakan strategi yang lebih minim risiko

4. Kesimpulan

Mengidentifikasi dan menilai risiko teknologi informasi dalam operasionalnya, PT. XYZ menggunakan metode *Failure Mode and Effects Analysis* (FMEA) yang menemukan level risiko tertinggi pada aset print, *fotocopy*, scan, komputer, server, IM4, IFS, serta kepala divisi. Dari aset-aset tersebut yang memiliki nilai RPN sebesar 720 yaitu ada pada aset komputer dan server. Mengacu pada kontrol ISO 27001:2013, rekomendasi kontrol meliputi perlindungan fisik terhadap peralatan dan lingkungan, serta melakukan *backup* data secara berkala untuk memastikan ketersediaan data. Pendekatan ini tidak hanya membantu mengidentifikasi risiko tetapi juga menentukan prioritas tindakan untuk menjaga keandalan dan integritas aset informasi perusahaan.

Daftar Pustaka

[1] D. R. Nurfadilah, W. N. H. Putra, and A. Rachmadi, "Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001 : 2013 (Studi Kasus : Aplikasi E-Kinerja)," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer, Univ. Brawijaya*, vol. 4, no. 9, pp. 3014–3020, 2020.

[2] 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.

[3] 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.

[4] M. Kartika, S. A1, Y. Saintika, and W. A. Prabowo, "Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto," vol. 10, no. 4, pp. 423–428, 2022, doi: 10.26418/justin.v10i4.48977.

[5] I. Maliki, "Manajemen Resiko Teknologi Informasi I Untuk Keberlangsungan Layanan Publik Menggunakan Framework Information Technology Infrastructure Library (Itil Versi 3)," *Semin. Nas. Apl. Teknol. Inf.*, vol. 2010, no. Snati, pp. 1907–5022, 2010.

[6] Tutik, N. Mutiah, and I. Rusi, "Analisis Dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis (FMEA) Dan ISO/IEC 27001:2013," *Coding J. Komput. dan Apl.*, vol. 10, no. 02, pp. 249–261, 2022.

ISSN: 1978-8126
e-ISSN: 2527-7340

[7] N. Badariah, D. Surjasa, and Y. Trinugraha, "Analisa Supply Chain Risk Management Berdasarkan Metode Failure Mode and Effects Analysis (Fmea)," *J. Tek. Ind.*, vol. 2, no. 2, pp. 110–118, 2012, doi: 10.25105/jti.v2i2.7021.

[8] K. P. Ningsih, U. Tunnisa, and N. Erviana, "Manajemen Resiko Redesign Sistem Penjajaran Rekam Medis dengan Metode Failure Mode and Effect Analysis (FMEA)," *Indones. Heal. Manag. J.*, vol. 8, no. 1, pp. 8–20, 2020.

[9] A. Kusnandar, "Evaluasi Keamanan Sistem Informasi Menggunakan Fuzzy FMEA Berbasis Framework ISO/IEC 27001:2013 untuk Meningkatkan Keamanan Informasi," *J. Sist. Inf. Bisnis*, vol. 14, no. 2, pp. 181–190, 2024, doi: 10.21456/vol14iss2pp181-190.

[10] R. F. Putra, A. Adiyanto, and M. Asbari, "Penerapan Metode Fuzzy Fmea (Failure Mode and Effect Analysis) Untuk Penjadwalan Maintenance Mesin Produksi Berbasis Web Di Pt Victory Ching Luh Indonesia," *Insa. Pembang. Sist. Inf. dan Komput.*, vol. 10, no. 2, pp. 27–34, 2022, doi: 10.58217/ipsikom.v10i2.220.

[11] D. C. Pangestuti, H. Nastiti, and R. Husniaty, "Analisis Risiko Operasional Dengan Metode FMEA," *J. AKUNTANSI, Ekon. dan Manaj. BISNIS*, vol. 10, no. 2, pp. 177–186, 2022, doi: 10.30871/jaemb.v10i2.3235.

[12] C. S. Saputri *et al.*, "Dampak Teknologi Informasi Mengenai Proses Audit : Teknologi Informasi Carina Serly Saputri Zulkarnain Zulkarnain Universitas Internasional Batam Korespondensi Penulis : 2242006.carina@uib.edu memperkuat sistem pengendalian internal . Melalui integrasi te," *J. Tek. Mesin, Ind. Elektro Dan Inform.*, vol. 3, no. 1, 2024.