Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer
Vol. 15, No. 3, Mei 2025, pp. 433 – 441
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

RISK ASSESMENT PENGENDALIAN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001:2013 MENGGUNAKAN METODE *FAILURE MODE AND EFFECTS ANALYSIS* (FMEA) STUDI KASUS: TIM BRINESIA PT. BRI ASURANSI INDONESIA

Winni Indah Kurnia Sari*[1], Syakur Khoiri[2], Fajar Masya[3]
[1,2,3]Ilmu Komputer, Sistem Informasi, Universitas Mercu Buana

Email: winniindahks20@gmail.com[1], syakurkhoiri@gmail.com[2], fajar.masya@mercubuana.ac.id[3]

Abstrak

Implementasi teknologi informasi tidak lepas dari risiko (*Information Technology Risk*) yang dapat berdampak pada pencapaian tujuan organisasi. Mengingat keterkaitannya yang tinggi dengan kemajuan teknologi, tim BRINESIA memiliki kewajiban untuk menjadi unit yang memerlukan perlindungan keamanan informasi guna menjaga kualitas keamanan data, termasuk aset-aset yang dimiliki. Untuk meminimalkan kemungkinan terjadinya kebocoran data, kerusakan, ketidakakuratan, ketidaktersediaan, atau gangguan lain terhadap informasi, penting untuk melakukan penilaian terhadap risiko. Terdapat berbagai metode yang dapat digunakan untuk menganalisis kemungkinan terjadinya kegagalan atau risiko. Salah satu metode yang banyak digunakan adalah FMEA (*Failure Mode & Effect Analysis*), yang merupakan pendekatan terstruktur untuk mendeteksi dan memberi peringkat pada mode kegagalan dengan cara menilai *severity*, *occurrence*, dan *detection*, sehingga menghasilkan *Risk Priority Number* (RPN). Metode ini juga memberikan saran untuk mitigasi risiko sesuai dengan standar ISO/IEC 27001:2013. Penelitian ini mengidentifikasi level potensi mode *failure mode* pada informasi yang diurus oleh tim BRINESIA, menentukan prioritas risiko, serta menyediakan pedoman mitigasi risiko yang bermanfaat bagi tim BRINESIA dalam menerapkan kontrol keamanan informasi.

Kata Kunci: *FMEA (Failure Mode & Effect Analysis), Risk Priority Number, ISO/IEC 27001:2013, mitigasi risiko.*

Abstract

The implementation of information technology is inherently associated with risks (Information Technology Risk), which can impact the achievement of organizational goals. Given its strong connection to technological advancements, the BRINESIA team has a responsibility to function as a unit that requires robust information security protection to maintain the integrity and security of data, including its assets. To minimize the risk of data leakage, damage, inaccuracies, unavailability, or other disruptions, conducting a thorough risk assessment is essential. Various methods can be employed to analyze the likelihood of failures or risks, one of the most widely used being Failure Mode and Effects Analysis (FMEA). This structured approach identifies and ranks failure modes by assessing severity, occurrence, and detection, ultimately generating a Risk Priority Number (RPN). Additionally, FMEA provides recommendations for risk mitigation in alignment with the ISO/IEC 27001:2013 standard. This study identifies the potential failure modes in the information assets managed by the BRINESIA team, determines risk priorities, and provides actionable risk mitigation guidelines to enhance the team's information security controls.

Keywords: *FMEA (Failure Mode & Effect Analysis), Risk Priority Number, ISO/IEC 27001:2013, risk mitigation.*

p-ISSN 2089-0265
e-ISSN 2598-3016

1. Pendahuluan

Teknologi informasi saat ini adalah keperluan utama bagi sebuah organisasi dalam mendukung operasi serta membantu meningkatkan efisiensi dan efektivitas proses di dalamnya. Pengelolaan yang baik terhadap teknologi informasi juga berperan penting untuk memastikan bahwa penggunaan teknologi ini selaras dengan Visi, Misi, dan Tujuan dari organisasi. Maka, penerapan teknologi informasi tidak terlepas dari risiko (Information Technology Risk) yang dapat memengaruhi pencapaian target organisasi. Banyak organisasi masih sering menghadapi masalah seperti kebocoran data, kerusakan, ketidakakuratan, ketidaktersediaan, atau gangguan lain pada informasi.

PT. BRI Asuransi Indonesia, yang selanjutnya akan disebut BRI Insurance, adalah sebuah perusahaan asuransi umum yang merupakan bagian dari BRI Group. BRI Insurance tentu saja mempunyai rencana untuk menghadapi tantangan dalam melindungi keamanan informasi dari berbagai ancaman yang mungkin muncul, dengan tujuan untuk memastikan kelangsungan usaha, mengurangi risiko bisnis, serta meningkatkan peluang dalam dunia usaha.

BRINESIA merupakan kependekan dari BRI *Insurance Enterprise Application* yaitu tim yang diperuntukkan untuk merevitalisasi proses bisnis, digitalisasi dan peningkatan teknologi untuk meningkatkan layanan baik internal maupun eksternal perusahaan. Oleh karena itu dalam menjalankan operasionalnya BRINESIA tidak terlepas dari proses pengembangan aplikasi baik website maupun mobile, pengelolaan *database*, penggunaan server serta pemeliharaan aset seperti laptop, handphone tester serta *license software*.

Mengingat pentingnya peranan BRINESIA dalam penerapan teknologi informasi, maka harus dikelola secara efektif agar pengelolaannya menjadi optimal dan risiko yang timbul dapat dimitigasi. Maka mengharuskan BRINESIA menjadi unit yang membutuhkan perlindungan keamanan sebagai upaya menjaga kualitas keamanan informasi termasuk aset-aset yang dimiliki.

Berdasarkan penjelasan sebelumnya, diperlukan suatu solusi, yaitu penilaian risiko. Penilaian risiko ini bertujuan untuk mempersiapkan diri menghadapi berbagai potensi serta peluang risiko yang bisa muncul. Proses penilaian risiko dilakukan dengan menggunakan metode Failure Mode And Effects Analysis (FMEA), yang hasilnya dapat memberikan saran mitigasi sesuai dengan hasil identifikasi risiko dari Control Annex A pada ISO 27001:2013, sehingga dapat meningkatkan layanan dengan cepat dan memenuhi kebutuhan para pemangku kepentingan.

2. Tinjauan Pustaka

Berikut adalah teori-teori maupun konsep terkait yang menjadi landasan teori dalam penelitian ini:

2.1 Risiko Teknologi Informasi

Teknologi Informasi merupakan salah satu sumber daya yang sangat berharga, dan jika keamanan aset ini terancam, hal itu bisa mengganggu operasi suatu organisasi. Risiko yang terkait dengan Teknologi Informasi adalah sebuah ancaman yang mampu memanfaatkan kelemahan pada aspek keamanan teknologi informasi dan berpotensi menyebabkan kerugian bagi organisasi tersebut.

2.2 Mitigasi Risiko

Mitigasi Risiko merupakan upaya yang dilakukan untuk mengurangi atau meminimalisir adanya kemungkinan terjadinya risiko. Tindakan mitigasi dilakukan tergantung dari risiko apa yang dihadapi. Respon atau tanggapan tersebut bisa dalam bentuk menghindari risiko (*avoidance*), mengurangi risiko (*reduction*), memindahkan risiko (*sharing*), menerima risiko (*acceptance*), aktivitas pengendalian.

2.3 Aset Informasi

Aset adalah salah satu komponen penting yang harus dilindungi dan dikelola dengan baik dalam suatu instansi atau organisasi. Aset informasi adalah sumber daya yang sangat berharga dalam

mendukung proses operasional perusahaan dan perlu dikelola secara efektif untuk dimanfaatkan dengan optimal. Aset informasi terdiri dari beberapa elemen, yaitu *software*, *hardware*, *people*, data dan *network*

2.4 Manajemen Risiko

Manajemen Risiko adalah suatu cara untuk menemukan dan menganalisis risiko serta melakukan tindakan untuk mengurangi risiko dan pengaruhnya terhadap proses bisnis dalam sebuah organisasi hingga mencapai batas yang bisa diterima. Aktivitas yang terlibat dalam manajemen risiko meliputi pengumpulan informasi, pengenalan ancaman dan kelemahan, analisis dampak terhadap bisnis, dan penilaian risiko. Dalam konteks Sistem Manajemen Keamanan Informasi (SMKI), risiko merujuk pada pengaruh yang muncul ketika ada sesuatu yang mengancam keamanan informasi dari tiga aspeknya, yaitu yaitu *confidentiality, integrity* dan *availability* pada suatu organisasi.

2.5 Failure Mode and Effect Analysis (FMEA)

Failure Mode and E ffect Analysis (FMEA) adalah cara yang terorganisir yang bisa digunakan untuk menemukan dan memberi peringkat pada jenis-jenis kegagalan, lalu mencegahnya sebanyak mungkin (Budiarto, 2017).

Langkah-langkah yang dilakukan dalam metode *Failure Mode and Effect Analysis* (FMEA) adalah:

1. Mengidentifikasi risiko yang mungkin terjadi melalui diskusi dengan semua pihak terkait.
2. Memberikan tingkat keparahan (severity).

Berikut merupakan bagan tingkatan risiko dalam penentuan nilai keparahan(*severity*).

TABEL 1.
SKOR TINGKAT SEVERITY

Skor	*Severity*	Keterangan
1	Tidak ada akibat (*none*)	Tidak ada dampak atau tidak mempengaruhi terhadap kinerja.
2	Akibat sangat ringan (*very minor*)	Tidak terganggu. Sangat sedikit berpengaruh pada kinerja sistem atau memberikan dampak kecil terhadap kinerja.
3	Akibat ringan (*minor*)	Menyebabkan sedikit terjadinya gangguan maupun menyebabkan sedikit masalah yang bisa di perbaiki tanpa adanya kehilangan sesuatu.
4	Sangat rendah (*very low*)	Menimbukan gangguan yang cukup berpengaruh/ menyebabkan sedikit kerugian.
5	Rendah (*low*)	Menimbulkan komplain.
6	Sedang (*moderate*)	Menyebabkan layanan gagal berfungsi sebagaimana mestinya.
7	Tinggi (*high*)	Menimbulkan proses organisasi terhenti dalam waktu 1 hari.
8	Sangat tinggi (*very high*)	Menimbulkan proses organisasi terhenti dalam waktu yang sebentar <1 hari.
9	Akibat serius / Berbahaya; Dengan peringatan	Potensial kegagalan atau risiko mempengaruhi keamanan sistem dengan peringatan atau Dapat menimbulkan proses pengorganisasian terhenti selama waktu yang cukup lama > 1 hari.
10	Akibat berbahaya; Tanpa peringatan	Potensial kegagalan atau risiko mempengaruhi keamanan sistem tanpa peringatan dan mengakibatkan proses organisasi berhenti dalam jangka waktu yang lama > 1 minggu.

3. Menentukan tingkat frekuensi kejadian (*occurrence*)

Berikut merupakan bagan tingkatan risiko dalam penentuan nilai frekuensi kejadian (*occurrence*).

TABEL 2.
SKOR TINGKAT OCCURENCE

Skor	*Occurrence*	Keterangan
1	*Almost never*. Kegagalan hampir/tidak pernah terjadi	Satu kali dalam 6 – 50 tahun
2	*Remote*. Kegagalan terjadi relatif kecil dan sangat jarang	Satu kali dalam 3 – 6 tahun
3	*Very slight*. Kegagalan terjadi relatif kecil	Satu kali dalam 1 – 3 tahun
4	*Slight*. Kegagalan jarang terjadi	Satu kali dalam setahun
5	*Low*. Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan
6	*Medium*. Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan
7	*Moderatly high*. Kegagalan sering terjadi	Satu kali dalam sebulan
8	*High*. Kegagalan terjadi berulang kali	Satu kali dalam seminggu
9	*Very high*. Kegagalan selalu terjadi	Satu kali setiap 3 – 4 hari
10	*Almost certain*. Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya

4. Menentukan tingkat deteksi kejadian (*detection*)

Berikut merupakan bagan tingkatan risiko dalam penentuan nilai deteksi (*detection*)

TABEL 3.
SKOR TINGKAT DETECTION.

Skor	*Detection*	Keterangan
1	Hampir pasti	Hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi
2	Sangat tinggi	Sangat tinggi dapat dideteksi dengan kontrol yang ada saat ini. Semua produk secara otomatis diperiksa
3	Tinggi	Memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan
4	Cukup tinggi	Memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan
5	Sedang	Memiliki tingkat efektifitas yang rata-rata
6	Rendah	Memiliki tingkat efektifitas yang rendah
7	Sangat rendah	Tidak handal dalam mendeteksi tepat waktu
8	Kecil	Tidak terbukti untuk mendeteksi tepat waktu
9	Sangat kecil	Tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi
10	Hampir tidak mungkin	Kekurangan tidak dapat di deteksi penyebabnya. Tidak adanya metode deteksi

5. Perhitungan Nilai Risk Priority Number (RPN)

Risk Priority Number adalah hasil dari mengalikan tingkat *severity*, *occurrence*, dan *detection* yang sudah dihitung. Dengan perhitungan RPN, kita bisa mendapatkan daftar prioritas dari risiko kegagalan yang ada, di mana nilai RPN yang didapat hanya digunakan untuk menentukan urutan dari risiko yang paling mungkin terjadi hingga yang paling tidak mungkin. Rumus untuk menghitung nilai RPN adalah sebagai berikut:.

RPN = *severity X occurrence X detection*

Keterangan:

RPN : Risk Priority Number
Severity : tingkat keparahan kegagalan
Occurrence : frekuensi terjadinya kegagalan
Detection : tingkat deteksi kejadian

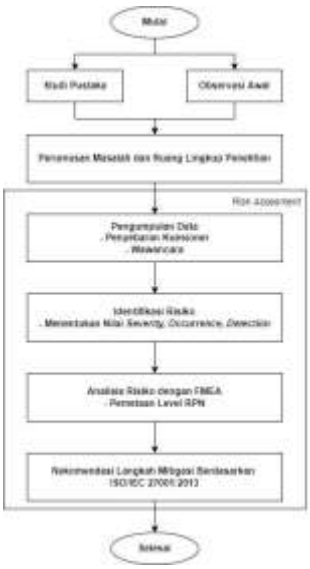
p-ISSN 2089-0265
e-ISSN 2598-3016

2.6 ISO/IEC 27001:2013

ISO/IEC 27001:2013 adalah dokumen yang menjadi acuan untuk Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS). Dokumen ini menawarkan panduan untuk menerapkan prinsip-prinsip keamanan informasi dalam suatu organisasi dengan mengikuti praktik terbaik. ISO/IEC 27001:2013 merinci hal-hal yang dibutuhkan untuk sistem manajemen keamanan informasi yang efektif. Tujuannya adalah untuk menjaga dan melindungi aktivitas bisnis dari gangguan serta memberikan perlindungan terhadap masalah keamanan informasi yang dapat menyebabkan kerugian.

3. Metode Penelitian

Bagian ini menjelaskan proses penelitian yang menyajikan rincian mengenai urutan langkah-langkah yang disusun dengan sistematis dan logis. Tujuannya adalah untuk menjadi pedoman yang jelas dan mudah dalam menyelesaikan masalah, menganalisis hasil, serta mengatasi kendala yang muncul. Penelitian ini difokuskan pada tim pengembang BRINESIA di PT. BRI Asuransi Indonesia. Gambar 1 menunjukkan urutan langkah-langkah yang digunakan dalam penelitian ini untuk menyelesaikan masalah. .



Gambar 1. Metode Penelitian

4. Hasil dan Pembahasan

4.1 Klasifikasi Aset

Berdasarkan hasil pengamatan selama proses yang sudah dilakukan yaitu pengumpulan data dan informasi sebagai bahan yang mendukung kebenaran acuan referensi. Untuk mengetahui tindakan mitigasi terhadap potensi risiko pada aset-aset keamanan informasi pada tim BRINESIA maka diperlukan beberapa tahap yang harus dilakukan.

TABEL 4.
KLASIFIKASI ASET

No	Aset	Keterangan
A1	Hardware	Perangkat keras yang digunakan oleh semua anggota tim BRINESIA yang dapat menimbulkan potensi risiko keamanan informasi, seperti: laptop, handphone dan tablet tester.
A2	Software	Perangkat lunak yang digunakan oleh semua anggota tim BRINESIA yang dapat menimbulkan potensi risiko keamanan informasi, seperti: aplikasi dan server.
A3	Informasi Dokumentasi	Dokumen-dokumen yang dikelola oleh tim BRINESIA yang dapat menimbulkan potensi risiko keamanan informasi, seperti: dokumen internal, eksternal, publik maupun rahasia/*credential*.
A4	*People*/Orang	Sumber Daya Manusia yang tergabung dalam tim BRINESIA yang dapat menimbulkan potensi risiko keamanan informasi, seperti: pemalsuan data/informasi, *spionase* (mata-mata).

p-ISSN 2089-0265
e-ISSN 2598-3016

4.2 *Brainstorming* Risiko

Dalam tahap ini, dilakukan brainstorm mengenai risiko yang mungkin terjadi, dengan tujuan untuk memahami kemungkinan kegagalan yang bisa muncul dalam fungsi sistem yang digunakan. Hasil yang didapat adalah daftar dampak dari risiko atau mode kegagalan potensial pada aset-aset yang telah dikenali sebelumnya.

TABEL 5.
IDENTIFIKASI RISIKO

Aset	No. Cause Failure	Potential Failure Mode
A1	CF1	Laptop terserang malware
	CF2	Kerusakan laptop dikarenakan malfungsi
	CF3	Laptop hilang/dicuri di ruang kerja
	CF4	Laptop hilang/dicuri di luar lingkungan kerja (ruang publik)
	CF5	Laptop diakses oleh pihak yang tidak berkepentingan
	CF6	Handphone terserang malware
	CF7	Kerusakan handphone dikarenakan malfungsi
	CF8	Handphone hilang/dicuri di ruang kerja
	CF9	Handphone hilang/dicuri di luar lingkungan kerja (ruang publik)
	CF10	Handphone diakses oleh pihak yang tidak berkepentingan
A2	CF11	Server terserang malware
	CF12	Server down system
	CF13	Server diakses oleh pihak yang tidak berkepentingan
	CF14	Penyalahgunaan hak akses
	CF15	*Software error*
	CF16	Lisensi illegal atau *expired*
A3	CF17	Kerusakan atau *corrupt* dokumen
	CF18	Dokumen tidak dapat diakses
A4	CF19	Pengungkapan data/informasi oleh pihak tidak berkepentingan

4.3 Menentukan Nilai Severity, Occurrence, Detection

Setelah melakukan daftar identifikasi risiko, langkah selanjutnya adalah menentukan tingkat keparahan atau dampak yang ditimbulkan (*severity*), frekuensi kejadian (*occurrence*) dari masing-masing daftar potensi risiko serta pengukuran terhadap kemampuan mengendalikan kegagalan yang terjadi (*detection*).

Kemudian di waktu yang bersamaan dapat dilakukan perhitungan Level Risk Priority Number (RPN). Perhitungan ini dilakukan dengan cara pengkalian dari nilai severity, occurrence dan detection. Dari proses penilaian tersebut akan dipetakan nilai RPN yang merupakan skor potensi tertinggi hingga terendah yang telah diidentifikasi tersebut.

TABEL 6.
PERHITUNGAN RPN

Aset	No. Cause Failure	Potential Failure Mode	S	O	D	RPN
A1	CF1	Laptop terserang malware	6	2	5	60
	CF2	Kerusakan laptop dikarenakan malfungsi	6	3	5	90
	CF3	Laptop hilang/dicuri di ruang kerja	6	1	5	30
	CF4	Laptop hilang/dicuri di luar lingkungan kerja (ruang publik)	7	2	6	84

p-ISSN 2089-0265
e-ISSN 2598-3016

	CF5	Laptop diakses oleh pihak yang tidak berkepentingan	6	3	5	90
	CF6	Handphone terserang malware	6	3	5	90
	CF7	Kerusakan handphone dikarenakan malfungsi	6	3	6	108
	CF8	Handphone hilang/dicuri di ruang kerja	6	2	6	72
	CF9	Handphone hilang/dicuri di luar lingkungan kerja (ruang publik)	6	3	6	108
	CF10	Handphone diakses oleh pihak yang tidak berkepentingan	6	3	5	90
	CF11	Server terserang malware	7	3	6	126
	CF12	Server down system	7	4	6	168
A2	CF13	Server diakses oleh pihak yang tidak berkepentingan	6	2	6	72
	CF14	Penyalahgunaan hak akses	6	2	5	60
	CF15	Software error	6	2	5	60
	CF16	Lisensi illegal atau *expired*	6	2	5	60
A3	CF17	Kerusakan atau *corrupt* dokumen	6	2	5	60
	CF18	Dokumen tidak dapat diakses	6	2	5	60
A4	CF19	Pengungkapan data/informasi oleh pihak tidak berkepentingan	6	2	4	48

4.4 Menentukan Prioritas Risiko

Pada tahap ini setelah risiko-risiko tersebut diukur tingkat *severity*, *occurrence* dan *detection* hingga menghasilkan nilai RPN, selanjutnya dilakukan susunan urutan prioritas berdasarkan nilai RPN tertinggi sampai dengan nilai RPN risiko yang terendah.

TABEL 7.
PERHITUNGAN RPN

No. Cause Failure	Potential Failure Mode	S	O	D	RPN	Level
CF12	Server down system	7	4	6	168	*High*
CF11	Server terserang malware	7	3	6	126	*High*
CF7	Kerusakan handphone dikarenakan malfungsi	6	3	6	108	*Medium*
CF9	Handphone hilang/dicuri di luar lingkungan kerja (ruang publik)	6	3	6	108	*Medium*
CF2	Kerusakan laptop dikarenakan malfungsi	6	3	5	90	*Medium*
CF5	Laptop diakses oleh pihak yang tidak berkepentingan	6	3	5	90	*Medium*
CF6	Handphone terserang malware	6	3	5	90	*Medium*
CF10	Handphone diakses oleh pihak yang tidak berkepentingan	6	3	5	90	*Medium*
CF4	Laptop hilang/dicuri di luar lingkungan kerja (ruang publik)	7	2	6	84	*Medium*
CF8	Handphone hilang/dicuri di ruang kerja	6	2	6	72	*Low*
CF13	Server diakses oleh pihak yang tidak berkepentingan	6	2	6	72	*Low*
CF1	Laptop terserang malware	6	2	5	60	*Low*
CF14	Penyalahgunaan hak akses	6	2	5	60	*Low*
CF15	software error	6	2	5	60	*Low*
CF16	Lisensi illegal atau expired	6	2	5	60	*Low*
CF17	Kerusakan atau corrupt dokumen	6	2	5	60	*Low*

p-ISSN 2089-0265
e-ISSN 2598-3016

CF18	Dokumen tidak dapat diakses	6	2	5	60	*Low*
CF19	Pengungkapan data/informasi oleh pihak tidak berkepentingan	6	2	4	48	*Low*
CF3	Laptop hilang/dicuri di ruang kerja	6	1	5	30	*Low*

4.5 Rekomendasi Mitigasi Risiko Berdasarkan ISO/IEC 27001:2013

Mitigasi risiko adalah tahap penanganan risiko yang dilakukan berdasarkan hasil penilaian dari prioritas risiko yang telah ditentukan. Dalam pemetaan yang terlihat pada Tabel 4.4, terdapat dua langkah mitigasi yang harus diambil, yaitu untuk cause failure nomor CF12 dan CF11, karena keduanya dikategorikan sebagai level tinggi. Langkah ini bertujuan untuk mengurangi kemungkinan terjadinya risiko, dan saran yang diberikan bisa diterapkan jika risiko tersebut muncul. Tabel 4.5 berisi rekomendasi tindakan mitigasi yang diambil sesuai dengan standar ISO/IEC 27001:2013.

TABEL 8.
REKOMENDASI TINDAKAN MITIGASI RISIKO

No. Cause Failure	**Tindakan Mitigasi berdasarkan ISO/IEC 27001:2013**		
	Klausul	**Kontrol**	**Tindakan**
CF12	A.12.3.1	*Information Backup*	Merencanakan proses *fail over* (Pemindahan ke server cadangan ketika server utama down)
CF11	A.12.2.1	*Controls Against Malware*	Penggunaan aplikasi antivirus mengikuti matriks aplikasi BRINESIA yang tertera pada lampir 3.

5. Kesimpulan

Berdasarkan tujuan dan hasil penelitian maka dapat disimpulkan beberapa hal berikut:

1. Terdapat 19 potential cause failure yang akan menyebabkan terjadinya risiko pada keamanan aset TI pada tim BRINESIA. Diantaranya terdapat 2 cause failure dengan level high, 7 cause failure dengan level medium dan 10 cause failure dengan level low.

2. Penilaian risiko menggunakan metode FMEA dilakukan dalam beberapa langkah. Pertama, proses akan direview, lalu diadakan sesi brainstorming untuk mengidentifikasi potensi risiko. Setelah itu, tingkat severity, occurrence, dan detection akan ditentukan. Selanjutnya, RPN atau Risk Priority Number akan dihitung, dan berdasarkan itu, risiko akan diprioritaskan, diikuti dengan rekomendasi untuk mitigasi risiko, yang merupakan langkah-langkah yang bisa diambil untuk mencegah atau mengurangi kemungkinan terjadinya kegagalan atau dampak pada sistem. Melalui proses penilaian risiko dengan metode FMEA, diperoleh daftar risiko yang diurutkan dari yang tertinggi hingga terendah berdasarkan skornya. Salah satu risiko yang termasuk kategori tinggi memiliki RPN sebesar 168, yang terkait dengan risiko perangkat lunak. Risiko ini diidentifikasi sebagai kemungkinan terjadinya server down system, yang dapat menyebabkan terhentinya proses di organisasi.

3. Dari risiko dan ancaman yang ada, dihasilkan rekomendasi yaitu berdasarkan Kontrol Annex A.12.3.1 Information Backup yang berguna sebagai acuan tindakan mitigasi untuk mencegah risiko server down system. Kontrol Annex A.11.2.9 Clear Desk & Clear Screen Policy yang berguna sebagai SOP untuk mencegah risiko keamanan informasi apabila aset hardware seperti laptop, handphone tester diakses oleh pihak yang tidak berkepentingan.

Daftar Pustaka

FITRIANI, L.D. 2022. Risk Assessment And

p-ISSN 2089-0265
e-ISSN 2598-3016

Development Of Access Control Information Security Governance Based On ISO/IEC 27001:2013 At XYZ University. Jurnal Teknik Informatika dan Sistem Informasi Hal. 891-907.

BAKRI, M., IRMAYANA, N., 2017. Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001. Jurnal TEKNOKOMPAK, Vol. 11 Hal 41-44 .

WIJAYA, Y.D., 2021. Evaluasi Keamanan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013. Jurnal Sistem Informasi dan Informatika (SIMIKA), Vol 4 No 2.

SASRTIKA, I.F., BISMA, R., 2021. Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001:2013 (Sistem Manajemen Keamanan Informasi). JEISBI: Volume 02 Number 03.

INDRASARI, A., WAHYUDI, A.T. 2018. Analisis Manajemen Resiko berbasis ISO 9001:2015 dan ISO 31010:2009 pada Pelayanan Sistem Informasi Akademik "EduManage" di Universitas Setia Budi. Jurnal Ilmiah Teknik Industri dan Informasi, Hal. 47.

PRAMONO, P.P., FAHRIANTO, F., 2019.

`Pendeteksian Dini Tingkat Kemanan Informasi Berbasis ISO 27001:2013 Menggunakan Metode AHP (Analytical Hierarchy Process). CyberSecurity dan Forensik Digital Vol. 2, No. 2 hlm. 57-64.

WOWOR, N.E., SENTINUWO, S.R., dkk., 2018.

Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks KAMI. Jurnal Teknik Informatika Vol 13, No.4.

HANDAYANI, N.U., WIBOWO.M.A., SARI, D.P., dkk., 2018. Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001. TEKNIK, 39 (2), hal. 78-85.

PANJAITAN, B., ABDURRAHMAN, L., MULYANA, R. 2021. Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis ISO 27001:2013 Menggunakan Kontrol Annex : Studi Kasus Data Center PT. XYZ. e- Proceeding of Engineering : Vol.8, No.2, Page 2813.

SURYANA, D.Y., VINOLIA., IBRAHIM.A. 2017. Evaluasi Celah Keamanan Sistem Webserver Dengan Metode Failure Mode And Effects Analysis (Studi Kasus: Tiket.com). Computer Science and ICT Vol. 3 No. 1.

RAMAYANI, Y., OKTARINA, T. 2022. Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA). JURNAL INOVTEK POLBENG - SERI INFORMATIKA, VOL. 7, NO. 2.