Jurnal Sistem Informasi Bisnis 04(2024)
Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/63516

Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO/IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi

Aris Kusnandar*, Adian Fatchur Rochim, Vincensius Gunawan

Magister Sistem Informasi, Sekolah Pasca Sarjana, Universitas Diponegoro

Naskah masuk: 4 Mei 2024; Diterima untuk publikasi: 22 Juli 2024
DOI: 10.21456/vol14iss4pp375-384

Abstract

The more information stored in an organization, the higher the risks that may arise, such as damage, loss, or the exposure of personal information to irresponsible parties. XYZ Institution faces information security threats from various sources, including data theft, damage, and computer hacking. It is essential for the organization to understand the level of information security risk to ensure information remains secure. Therefore, this study proposes measuring information security risk using the FMEA method and analyzing information security risks based on ISO/IEC 27001:2013. The aim of this study is to identify and assess the level of information security risk at XYZ Institution to provide recommendations for information security. The study's results revealed 4 high-risk information security threats, 9 medium-risk threats, and 16 low-risk threats. The findings demonstrate that the organization needs to pay more attention to information security to ensure its smooth operation in the future.

Keywords: Information Security; FMEA; ISO 27001; Risk Measurement

Abstrak

Semakin banyak informasi yang disimpan di sebuah organisasi maka semakin banyak juga risiko yang akan terjadi seperti kerusakan, kehilangan, atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab. Instansi XYZ menghadapi ancaman keamanan informasi yang berasal dari berbagai sumber, seperti pencurian data, perusakan dan peretasan komputer. Tingkat risiko keamanan informasi perlu diketahui oleh organisasi guna memastikan keamanan informasi dalam batas yang aman, untuk itu penelitian ini mengusulkan pengukuran risiko keamanan informasi menggunakan metode FMEA dan menggunakan ISO/IEC 27001:2013 untuk analisis risiko keamanan informasi. Tujuan penelitian ini adalah mengetahui dan menilai tingkat risiko keamanan informasi pada Instansi XYZ sehingga bisa memberikan rekomendasi keamanan informasi. Hasil penelitian berisi penilaian risiko keamanan sistem informasi dan mitigasi risiko keamanan sistem informasi berdasarkan ISO/IEC 27001:2013. Penilaian risiko keamanan sistem informasi menggunakan metode FMEA didapatkan 4 prioritas risiko keamanan dengan tingkat tinggi, 9 prioritas keamanan dengan tingkat sedang, dan 16 prioritas risiko keamanan dengan tingkat kecil. Hasil penilaian menunjukkan bahwa organisasi perlu meningkatkan keamanan sistem informasi supaya organisasi berjalan dengan baik kedepanya.

Kata kunci: Keamanan Informasi; FMEA; ISO 2700; Pengukuran Risiko

1. Pendahuluan

Tantangan keamanan informasi terus berkembang seiring dengan kemajuan teknologi dan meningkatnya ancaman dari pihak internal maupun eksternal. Informasi merupakan aset yang sangat penting bagi organisasi (Kristanto *et al.*, 2019). Namun, tidak sedikit organisasi yang tidak menyadari akan pentingnya keamanan informasi. Semakin banyak informasi yang disimpan di sebuah organisasi/lembaga maka semakin banyak juga risiko yang akan terjadi seperti kerusakan, kehilangan, atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab (Safitri *et al*., 2020). Instansi XYZ adalah sebuah lembaga yang mengelola data kependudukan dengan menjamin kerahasiaan, integritas, dan ketersediaan informasi. Instansi XYZ menghadapi ancaman keamanan informasi yang berasal dari berbagai sumber, seperti pencurian data, perusakan dan peretasan komputer. Terkait ancaman tersebut, Instansi XYZ belum pernah melakukan analisis risiko keamanan. Tingkat risiko keamanan informasi perlu diketahui oleh instansi guna memastikan keamanan informasi dalam batas yang aman.

Keamanan informasi, baik secara langsung maupun tidak langsung dapat mendukung kelangsungan operasional bisnis, mengurangi risiko, dan meningkatkan efisiensi proses bisnis. Standar yang populer untuk meminimalisir ancaman dan risiko terkait keamanan informasi yang timbul akibat

*) *Corresponding author*: aries130797@gmail.com

kegiatan pengelolaan dan pemeliharaan informasi adalah ISO 27001(Anggraini *and* Bisma, 2021). ISO 27001 merupakan *framework* yang dipakai untuk menilai spesifikasi sistem dan menilai kinerja sistem dalam keandalan dan keakuratan sistem dalam melindungi informasi (Eskaluspita, 2020).

ISO 27001 membantu organisasi dalam mengembangkan dan memelihara sistem manajemen keamanan informasi (SMKI) di tingkat organisasi dan tetap menjadi salah satu alat manajemen risiko paling efektif (Mirtsch *et al.*, 2021; Culot *et al.*, 2021). ISO 27001:2013 merupakan sebuah standar yang bersifat independen terhadap produk teknologi informasi, pendekatan yang digunakan yakni manajemen risiko, dibuat dapat menjamin dan memberi keyakinan terhadap perusahaan yang memilih kontrol keamanan untuk melindungi aset informasi (Anggraini *and* Bisma, 2021; Herkules *et al.*, 2023). Standar ini menggunakan pendekatan manajemen yang berbasis kontrol berdasarkan analisis risiko (Paradise *et al.*, 2020).

Failure Mode and Effect Analysis (FMEA) adalah alat dan metode untuk menganalisis penyebab kegagalan dan memperkirakan dampak berbagai faktor (Nuchpho *et al.*, 2019). FMEA juga merupakan metode yang tepat untuk menentukan kemungkinan penyebab kerusakan dan dampaknya pada sistem yang kompleks (Balaraju *et al.*, 2019). Proses FMEA adalah mendeteksi potensi kegagalan dengan mengidentifikasi risiko dari suatu sistem, kemudian menilai setiap potensi kegagalan berdasarkan tiga kriteria: *severity* (S), *occurrence* (O), dan *detection* (D). S merupakan tingkat keparahan dampak yang disebabkan oleh *potential cause*, O merupakan kemungkinan terjadinya *potential failure* dengan melihat *potential cause*, dan D adalah tingkat efektivitas prosedur deteksi yang bertujuan untuk mencegah *potential failure* (Hartanti *et al.*, 2022) .

Penelitian sebelumnya tentang keamanan informasi adalah Analisis Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2005 oleh Kristanto *et al.*, (2019), ISO 27001:2013 untuk Sistem Informasi Manajemen Laboratorium oleh Eskaluspita, (2020), Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis ISO 27001:2013 Menggunakan Kontrol *Annex* oleh Panjaitan *et al.*, (2021) dan Penerapan Standar Sistem Manajemen Keamanan Informasi Internasional ISO/IEC 27001: Analisis Berbasis *Web Mining* oleh Mirtsch *et al.*, (2021). Sedangkan penelitian ini mengukur tingkat risiko keamanan informasi menggunakan metode FMEA berbasis ISO/IEC 27001 pada Instansi XYZ.

Setiap ancaman keamanan seperti pencurian informasi, penipuan, vandalisme, dan peretasan komputer akan mempengaruhi organisasi dalam berbagai cara seperti merusak reputasi organisasi, merusak data, kehilangan kepercayaan pelanggan, dan gangguan pada bisnis (Kristanto *et al.*, 2019). Untuk menghindari adanya pencurian dan hilangnya informasi baik disengaja maupun tidak, maka diperlukan keamanan informasi. Karena instansi pemerintah memiliki peran dalam pengelolaan data dan informasi, tata kelola harus memiliki keamanan informasi yang baik (Kamil *et al.*, 2023).

Pentingnya perlindungan terhadap keamanan informasi yang dimiliki Instansi XYZ, maka penelitian ini bertujuan untuk melakukan pengukuran risiko dan keamanan sistem informasi menggunakan metode FMEA sehingga menghasilkan rekomendasi untuk meningkatkan keamanan informasi berdasarkan analisis risiko yang dilakukan.

2. Kerangka Teori

2.1. Keamanan Informasi

Keamanan informasi adalah perlindungan terhadap informasi termasuk sistem dan perangkat yang digunakan untuk menyimpan dan mengirim informasi. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisir kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi, dan peluang usaha (Triantono, 2007). Keamanan informasi adalah upaya untuk mengamankan aset informasi dari segala ancaman yang mungkin terjadi untuk mengurangi risiko negatif yang diterima. Semakin banyak informasi yang disimpan di sebuah organisasi maka semakin banyak juga risiko yang akan terjadi seperti kerusakan, kehilangan, atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab (Safitri *et al.*, 2020). Organisasi perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupun produktivitas.

2.2. ISO 27001:2013

ISO/IEC 27001 saat ini telah menjadi standar paling menonjol di bidang keamanan informasi (Podrecca *and* Sartor, 2023). Standar keamanan informasi menggunakan ISO/IEC 27001 direkomendasikan karena pada penerapan standar tersebut telah berbasis risiko sehingga dianggap mampu dalam mengurangi ancaman keamanan informasi dengan tepat (Musyarofah *and* Bisma, 2021).

ISO/IEC 27001 memberikan pandangan terkait SMKI, yaitu keseluruhan sistem manajemen melalui pendekatan risiko bisnis dengan maksud untuk menetapkan, menerapkan, mengoperasikan, memantau, dan memelihara SMKI (Culot *et al.*, 2021). Secara umum ada 14 klausul mencakup 113 kontrol yang harus ada setiap organisasi dalam mengimplementasi konsep keamanan informasi. Pada Tabel 1 adalah 14 klausul ISO/IEC 27001:2013.

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/63516

Tabel 1. Klausul ISO/IEC 27001

No	Klausul ISO/IEC 27001:2013
1	A.5 Kebijakan keamanan informasi
2	A.6 Organisasi keamanan informasi
3	A.7 Keamanan sumber daya manusia
4	A.8 Manajemen Aset
5	A.9 Kontrol akses
6	A.10 Kriptografi
7	A.11 Keamanan fisik dan lingkungan
8	A.12 Operasi keamanan
9	A.13 Komunikasi keamanan
10	A.14 Sistem akuisisi dari sistem informasi
11	A.15 Hubungan dengan pemasok
12	A.16 Pengelolaan insiden keamanan informasi
13	A.17Aspek keamanan informasi manajemen kelangsungan hidup
14	A.18 Kepatuhan

2.3. Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) adalah teknologi yang dirancang untuk mengidentifikasi mode kegagalan potensial pada suatu proses sebelum terjadi, dengan mempertimbangkan risiko yang berkaitan dengan mode kegagalan tersebut serta efeknya (Nurkertamanda, 2019). Tujuan utama dari FMEA adalah untuk mengidentifikasi kegagalan yang potensial, mengevaluasi penyebab dan dampaknya serta menentukan hal apa yang dapat mengurangi potensi terjadinya kegagalan yang berisiko tinggi (Hakim *and* Wijaya, 2020).

Hasil dari identifikasi bahaya menggunakan metode FMEA yaitu berupa nilai *Risk Priority Number* (RPN), kemudian akan diketahui komponen mana yang memiliki nilai RPN paling tinggi (Pribadi *and* Ernastuti, 2020). Nilai RPN didapatkan dengan mengalikan nilai tingkat keparahan (*Severity*), probabilitas kegagalan (*Occurrence*), dan deteksi kegagalan (*Detection*) (Wicaksono *et al.*, 2022).

3. Metode Penelitian

3.1. Metode Penelitian

Standar ISO 27001 menyatakan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan manajemen keamanan informasi, model PDCA merupakan konsep yang tepat untuk mencapai persyaratan tersebut dalam penerapannya (Achmadi *et al.*, 2018; Ruiz *et al.*, 2022). Standar ISO/IEC 27001 menunjukkan bahwa pengoperasiannya mengikuti siklus perbaikan PDCA yang berupaya membuat proses manajemen lebih gesit, jelas, dan obyektif (Carvalho *and* Marques, 2019; Roy, 2020). PDCA memiliki 4 tahapan yaitu:

1) Tahap perencanaan yaitu melakukan wawancara dengan pihak organisasi untuk mengetahui informasi risiko keamanan berdasarkan ISO/IEC 27001:2013 dan observasi untuk meninjau secara langsung untuk mendapatkan data yang akurat dan jelas. Studi pustaka dilakukan untuk mengumpulkan informasi terkait penelitian. Hasil dari Tahap perencanaan yaitu kemungkinan risiko dan dampak dari risiko kemanan informasi;
2) Tahap pelaksanaan yaitu pra-pengolahan data yaitu melakukan uji validitas dan reliabilitas kuesioner risiko keamanan informasi. Setelah itu melakukan analisis risiko FMEA yakni mendapatkan nilai *severity*, *occurrence*, dan *detection* dari kuesioner yang disebarkan;
3) Tahap Pemeriksaan yaitu melakukan perhitungan FMEA untuk menentukan prioritas risiko keamanan informasi pada instansi XYZ;
4) Tahap penyesuaian adalah pemberian rekomendasi penganan keamanan sistem informasi berdasarkan prioritas risiko keamanan. Rekomendasi didapatkan dari mitigasi dengan ISO/IEC 27001. ISO 27001 juga mendefinisikan keperluan-keperluan untuk Sistem Manajemen Keamanan Informasi (SMKI) dan memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam implementasi konsep keamanan informasi di organisasi (Yuwono *et al.*, 2022).

3.2. Pengumpulan data

Pada tahap pengumpulan data, penulis melakukan dengan menyebarkan kuesioner terkait risiko keamanan informasi yang telah dianalisis sebelumnya untuk dilakukan uji validasi dan reliabilitas dengan jumlah 40 responden. Instrumen yang *valid* dan reliabel kemudian dilakukan penilaian risiko FMEA.

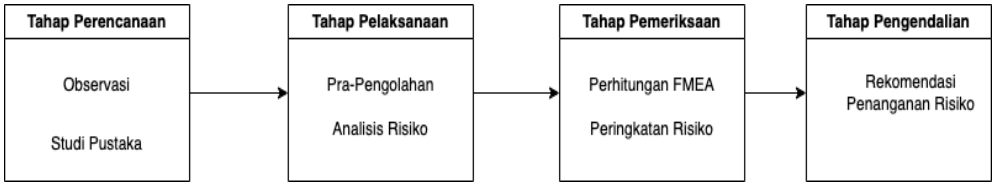
Uji validitas dilakukan dengan cara membandingkan nilai r hitung dengan nilai r tabel. Menentukan layak dan tidaknya suatu *item* yang akan digunakan, biasanya dilakukan uji signifikasi koefisien korelasi pada taraf signifikansi 0.05 yang artinya suatu *item* dianggap *valid* jika berkorelasi signifikan terhadap skor total. Jika r hitung lebih besar dari r tabel dan nilai positif maka butir atau pertanyaan atau variabel tersebut dinyatakan *valid* dan dapat lanjut ke tahap berikutnya. Persamaan 1 merupakan persamaan *pearson* untuk uji validasi.

$$r_{xy} = \frac{n\Sigma y_i - (\Sigma x_i)(\Sigma y_i)}{\sqrt{(n\Sigma x_i^2 - (\Sigma x_i)^2)(n(\Sigma y_i^2 - (\Sigma y_i)^2)}} \quad (1)$$

dengan:
r_{xy} : korelasi antara variabel x dan y
x_i : nilai x ke-i
y_i : nilai y ke-i
n : banyaknya nilai

Flowchart Metode Penelitian ini seperti ditunjukkan pada Gambar 1.

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/63516



Gambar 1. *Flowchart* Metode Penelitian

Uji reliabilitas merupakan pengujian untuk mengukur konsistensi kuesioner yang merupakan indikator dari variabel. Suatu data kuesioner dikatakan reliabel atau andal jika jawaban seseorang terhadap pertanyaan adalah konsisten atau stabil dari waktu ke waktu. Kriteria pengambilan keputusan sebagaimana dinyatakan oleh Suwarsono *et al.*, (2022), yaitu jika koefisien *Cronbach Alpha* > 0.70 maka pertanyaan dinyatakan andal atau suatu variabel dinyatakan reliabel. Sebaliknya, jika koefisien *Cronbach Alpha* < 0.70 maka pertanyaan dinyatakan tidak reliabel. Pengujian reliabilitas menggunakan rumus *Alpha Cronbach* pada persamaan 2.

$$r_n = \left(\frac{n}{n-1}\right)\left(1 - \frac{\sum \sigma b^2}{\sigma_t^2}\right) \quad (2)$$

dengan:
r_n : reliabilitas yang dicari
n : jumlah *item* pertanyaan yang diuji
$\sum \sigma b^2$: jumlah varian skor setiap *item*
σ_t^2 : varian total

3.3. Pengolahan dan Analisis Data

Tahap analisis yaitu melakukan penilaian risiko bertujuan untuk memahami seberapa besar risiko apa yang akan diterima oleh organisasi atau perusahaan jika informasi yang dikelola mendapatkan ancaman atau gangguan keamanan informasi. Metode FMEA adalah suatu metodologi yang digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan risiko dari kegagalan dan skala prioritas untuk mengambil tindakan yang diperlukan. Kuesioner yang *valid* dan reliabel pada tahap pra-pengolahan selanjutnya dapat dilakukan pengambilan nilai *severity*, *occcurrance*, dan *detection. Severity* yaitu seberapa besar efek/dampak dari risiko keamanan informasi. Nilai *severity* mulai skala 1 sampai 10, dimana 1 merupakan dampak paling kecil dari risiko kegagalan dan 10 merupakan dampak paling besar seperti yang ditunjukkan pada Tabel 2. Dampak dari kegagalan yang parah akan mendapat penilaian tertinggi dalam variabel *severity*.

Tabel 2. Nilai Tingkat Risiko (*Severity*)

Nilai	Efek	Deskripsi
10	Berbahaya tanpa peringatan	Mengakibatkan proses organisasi berhenti dalam jangka waktu yang lama > 1 minggu.
9	Berbahaya dengan peringatan	Dapat menimbulkan proses pengorganisasian terhenti selama waktu yang cukup lama > 1 hari.
8	Sangat tinggi	Proses organisasi terhenti dalam waktu yang sebentar <1 hari.
7	Tinggi	Menimbulkan proses organisasi terhenti dalam waktu 1 hari.
6	Sedang	Menimbulkan komplain. Menyebabkan layanan gagal berfungsi sebagaimana mestinya.
5	Rendah	Menimbulkan komplain. Layanan masih berjalan
4	Sangat rendah	Menimbulkan gangguan yang cukup berpengaruh/ menyebabkan sedikit kerugian.
3	Kecil	Menyebabkan sedikit terjadinya gangguan maupun menyebabkan sedikit masalah yang bisa diperbaiki tanpa adanya kehilangan sesuatu.
2	Sangat kecil	Tidak diperhatikan, namun memberikan dampak kecil terhadap kinerja.
1	Tidak ada	Tidak ada efek

Variabel *occurrence* menentukan penilaian berdasarkan pada potensi kegagalan yang terjadi dan seberapa sering kegagalan tersebut akan terjadi lagi selama proses tersebut berjalan (Aprianto *et al.*, 2021). Rincian penilaian *occurrence* seperti pada Tabel 3.

Tabel 3. Nilai Tingkat Probabilitas Risiko (*Occurrence*)

Nilai	Kemungkinan	Deskripsi
10	Lebih dari satu kali setiap hari	Kegagalan hampir/ tidak dapat dihindari
9	Satu kali dalam 3-4 hari	Kegagalan sering terjadi
8	Satu kali dalam 1 minggu	Kegagalan terjadi berulang kali
7	Satu kali dalam 1 bulan	Kegagalan sering terjadi
6	Satu kali dalam 3 bulan	Kegagalan terjadi waktu tertentu
5	Satu kali dalam 6 bulan	Kegagalan sesekali terjadi
4	Satu kali dalam 1 tahun	Kegagalan jarang terjadi
3	Satu kali dalam 1-3 tahun	Kegagalan relatif kecil
2	Satu kali dalam 3-6 tahun	Kegagalan relatif kecil dan sangat jarang terjadi
1	Satu kali dalam 6-9 tahun	Kegagalan hampir/tidak pernah terjadi

Variabel *detection*, fokus penilaian berdasarkan pada kemampuan pengendalian dan deteksi yang dilakukan organisasi terhadap kegagalan yang terjadi. Semakin baik pengendalian terhadap kegagalan, maka penilaian semakin tinggi. Tabel 4. merupakan rincian penilaian *detection*.

Tabel 4. Nilai Tingkat Kontrol Risiko (*Detection*)

Nilai	Deteksi	Deskripsi
10	Hampir tidak mungkin	Pasti tidak dapat terdeteksi/ tidak dapat terkontrol
9	Sangat susah	Sangat susah untuk mendeteksi risiko, sangat susah dikendalikan
8	Susah	Susah dideteksi, susah dikendalikan
7	Cukup susah	Cukup susah dideteksi, cukup susah kendalikan
6	Normal	Dapat dideteksi dengan usaha ekstra, dapat dikendalikan dengan usaha ekstra
5	Sedang	Dapat dideteksi, dapat dikendalikan
4	Cukup mudah	Cukup mudah dideteksi, dapat dikendalikan
3	Mudah	Mudah dideteksi, mudah dikendalikan
2	Sangat mudah	Sangat mudah dideteksi, mudah dikendalikan
1	Hampir pasti	Terlihat jelas, sangat mudah pengendalian

Setelah mendapatkan nilai selanjutnya yaitu penentuan tingkat risiko keamanan sistem informasi pada Intansi XYZ. Penentuan risiko keamanan informasi dilakukan dengan perhitungan perkalian *severity*, *occurance*, dan *detection* untuk menghasilkan *Risk Priority Number* (RPN) sehingga dapat mengetahui tingkat risiko keamanan sistem informasi. Perhitungan RPN ditunjukkan pada persamaan 3.

$$RPN = S \times O \times D \quad (3)$$

dengan
RPN : *Risk Priority Number*
S : *severity* (tingkat risiko)
O : *occurrence* (probabilitas risiko)
D : *detection* (deteksi/penanganan risiko)

Dari proses penilaian tersebut akan dibobotkan sehingga didapatkan RPN yang merupakan skor potensi dari risiko-risiko yang telah diidentifikasi tersebut. Kemudian dilakukan pengurutan berdasarkan nilai RPN tertinggi sampai yang terendah. Setelah itu, hasil dari penilaian RPN tersebut diurutkan sesuai level. Hasil dari RPN kemudian dilakukan pengurutan nilai RPN dari tertinggi sampai terendah. Nilai RPN memiliki level risiko yang berbeda-beda, seperti yang ditunjukkan pada Tabel 5.

Tabel 5. Level Risiko

Nilai RPN	Level Risiko
<20	Sangat Kecil
<80	Kecil
<120	Sedang
<170	Tinggi
>200	Sangat Tinggi

4. Hasil dan Pembahasan

4.1. Hasil

Hasil identifikasi risiko dan dampak keamanan informasi yang dilakukan melalui wawancara dengan manajerial didapatkan 3 klausul dari 14 klausul keamanan informasi ISO/IEC 27001:2013 yang menjadi kemungkinan risiko keamanan informasi untuk dilakukan penilaian risiko keamanan informasi, antara lain keamanan sumber daya manusia, manajemen aset, dan keamanan fisik dan lingkungan.

Berikut rincian kemungkinan risiko ancaman keamanan informasi. Tabel 6. menunjukkan risiko dari klausul keamanan sumber daya manusia.

Tabel 6. Keamanan Sumber Daya Manusia

ID	Kemungkinan Risiko	Dampak
A1	Verifikasi latar belakang calon pegawai tidak dilaksanakan dengan baik sesuai dengan peraturan	Pegawai tidak kompeten, Efek negatif ke pegawai lain
A2	Pegawai tidak membuat perjanjian tertulis tentang ketentuan pegawai dalam keamanan informasi organisasi	Tidak ada pertanggung jawaban dan organisasi yang akan terjadi bilamana ada ancaman keamanan informasi
A3	Organisasi tidak mewajibkan pegawai menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang diterapkan	Kemungkinan risiko ancaman keamanan informasi tinggi Keamanan informasi mudah diretas, adanya penyalahgunaan data
A4	Pegawai tidak menerima pemberitahuan secara berkala terkait kebijakan dan prosedur organisasi sesuai *jobdesk* pegawai	Pelanggaran pegawai akan terjadi Penyalahgunaan wewenang
A5	Tidak ada proses hukuman yang jelas dan terkomunikasi kepada pegawai mengenai pelanggaran	Pelanggaran akan terjadi lagi, Menurunkan kualitas pegawai
A6	Setelah pemberhentian atau perubahan pegawai dalam tugas. Keamanan informasi tidak di informasikan dan dikomunikasikan dengan pegawai pengganti	Adanya penyalahgunaan kewenangan Pelanggaran akan terjadi

Klausul manajemen aset berisi 10 kemungkinan risiko yang dapat dilihat pada Tabel 7.

Tabel 7. Manajemen Aset

ID	Kemungkinan Risiko	Dampak
B1	Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi tidak diidentifikasi dan inventaris dari aset-aset ini tidak dicatat dan kurang dipelihara.	Kerusakan aset yang akan terjadi tidak dapat dimnimalisir, tidak ada pemeliharaan aset, inventaris tidak terorganisir.
B2	Tidak ada pegawai yang bertanggung jawab atas aset yang ada	Aset menjadi rusak, tidak ada pemeliharaan aset
B3	Aturan untuk penggunaan tidak diidentifikasi, tidak didokumentasi dan tidak diimplementasikan.	Aset menjadi rusak, hilangnya aset, penyalahgunaan aset
B4	Semua pegawai dan pengguna pihak eksternal tidak mengembalikan semua	Bocornya informasi organisasi, hilangnya aset organisasi.

ID	Kemungkinan Risiko	Dampak
	aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.	
B5	Informasi tidak diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.	Informasi tidak tertata dengan baik, sulit untuk pencarian informasi,
B6	Seperangkat prosedur yang tepat untuk pelabelan informasi tidak dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.	Informasi tidak tertata dengan baik, sulit untuk pencarian informasi
B7	Prosedur penanganan aset tidak dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi organisasi.	Informasi tidak tertata dengan baik, sulit untuk pencarian informasi
B8	Prosedur tidak diimplementasikan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi.	Media informasi rusak, bocornya informasi organisasi
B9	Media tidak dihancurkan dengan aman saat tidak lagi dibutuhkan	Media dapat disalahgunakan
B10	Media yang mengandung informasi tidak dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah selama dipindahkan.	Bocornya informasi organisasi, penyalahgunaan informasi, hilangnya kepercayaan terhadap organisasi

Klausul keamanan fisik dan lingkungan berisi 15 kemungkinan risiko yang ditunjukkan pada Tabel 8.

Tabel 8. Keamanan Fisik dan Lingkungan

ID	Kemungkinan Risiko	Dampak
C1	Batas fisik keamanan tidak ditetapkan dan tidak digunakan untuk melindungi area yang mengandung informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.	Perangkat informasi mudah rusak, diretas dan rusak, bocornya informasi organisasi
C2	Tidak ada yang menjaga akses keluar masuk ruang sistem informasi organisasi	Informasi dan perangkat bisa diretas dan dicuri, Dapat terjadi kebocoran informasi
C3	Keamanan fisik untuk kantor, ruangan dan fasilitas tidak dirancang dan tidak diterapkan.	Mudahnya pencurian, kebocoran informasi, dan kerusakan informasi
C4	Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan tidak dirancang dan diterapkan.	Mudahnya kebocoran data, pencurian dan hilangnya informasi
C5	Prosedur untuk bekerja dalam daerah aman tidak dirancang dan diterapkan.	Mudahnya kerusakan informasi, pencurian informasi.
C6	Titik akses seperti area bongkar muat dan titik lain yang dapat dimasuki orang yang tidak berwenang tidak dikendalikan dan tidak dipisahkan dari fasilitas pengolahan informasi.	Informasi dapat bocor, Kehilangan informasi Kehilangan perangkat informasi
C7	Peralatan tidak ditempatkan dan dilindungi dari bahaya lingkungan dan mudah diakses oleh pihak tidak berwenang	Kerusakan peralatan, hilangnya peralatan, dan bocornya informasi
C8	Peralatan tidak dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung.	Informasi data tidak tersimpan, Kehilangan informasi data, kerusakan perangkat informasi
C9	Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung tidak dilindungi dari pencegatan, interferensi atau kerusakan.	Dapat terjadi kebocoran data, rusaknya peralatan dan hilangnya informasi
C10	Peralatan tidak dipelihara secara tepat untuk menjamin ketersediaan yang berkelanjutan dan integritas	kerusakan peralatan Penyalahgunaan data, integritas organisasi menurun
C11	Peralatan, informasi atau perangkat lunak boleh dibawa keluar lokasi tanpa izin yang berwenang	Penyalahgunaan informasi, kerusakan peralatan informasi, bocornya informasi
C12	Keamanan tidak diterapkan untuk aset di luar kantor dengan memperhitungkan risiko yang berbeda akibat bekerja di luar lokasi organisasi.	Kerusakan peralatan dan kehilangan dan penyalahgunaan informasi
C13	Semua peralatan yang mengandung media penyimpanan tidak diverifikasi untuk menjamin bahwa data rahasia dan perangkat lunak berlisensi apapun sudah dihapus atau ditimpa secara aman sebelumnya untuk dibuang atau dipergunakan kembali.	Dapat terjadi kobocoran informasi, penyalahgunaan informasi

Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/63516

ID	Kemungkinan Risiko	Dampak
C14	Pengguna tidak menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak.	Dapat terjadi kebocoran data, penyalahgunaan informasi.
C15	Kebijakan mengosongkan meja dari kertas dan media penyimpanan yang dapat dipindah dan kebijakan mengosongkan layar dari fasilitas pengolahan informasi tidak diadopsi.	Kerusakan peralatan dan Risiko kehilangan dan penyalahgunaan data tidak dapat diminimalisir

Berdasarkan hasil uji validitas kuesioner terkait risiko ancaman keamanan informasi dari 31 instrumen ditemukan 29 kemungkinan instrumen *valid* dengan hasil r hitung diatas r tabel dan 2 instrumen tidak *valid* yaitu ID B10 dan ID C2. Adapun uji reliabilitas dengan 29 instrumen penelitian *valid* menggunakan rumus *Cronbach Alpha*. Berdasarkan rumus persamaan uji reliabilitas variabel diperoleh hasil pengujian *Cronbach Alpha* dengan nilai 0.969 yang berarti memiliki nila reliabilitas tinggi. Kuesioner dikatakan reliabel jika *Cronbach Alpa* > 0.6 (Suwarsono *et al.*, 2022). Selanjutnya Analisis risiko dalam penelitian ini menggunakan metode FMEA. Pada Tabel 9 merupakan hasil perhitungan FMEA.

Tabel 9. Hasil Perhitungan FMEA

ID	*Severity*	*Occurrence*	*Detection*	RPN	Peringkat
A1	8	4	3	96	4
A2	8	4	2	64	7
A3	9	2	2	36	13
A4	7	2	2	28	15
A5	9	3	2	54	10
A6	8	3	3	72	6
B1	7	4	3	84	5
B2	8	3	4	96	4
B3	8	4	4	128	2
B4	9	4	4	144	1
B5	8	4	4	128	2
B6	9	4	4	144	1
B7	8	4	3	96	5
B8	9	3	4	108	4
B9	9	4	3	108	4
C1	7	4	2	56	9
C3	7	3	2	42	12
C4	7	4	4	112	3
C5	8	2	2	32	14
C6	7	2	2	28	15
C7	8	4	3	96	5
C8	8	3	2	48	11
C9	8	3	2	48	11
C10	8	3	3	72	6
C11	7	3	2	42	12
C12	7	4	4	112	3
C13	8	2	2	32	14
C14	7	2	2	28	15

Pada Tabel 10 berisi pengendalian keamanan Informasi yang diurutkan berdasarkan tingkat risiko keamanan informasi.

Tabel 10. Pengendalian Keamanan Informasi

ID	Pengendalian Keamanan Informasi
B4	Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.
B6	Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
B3	Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi, didokumentasi dan diimplementasikan.
B5	Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.
C4	Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan.
C12	Keamanan harus diterapkan untuk aset di luar kantor dengan memperhitungkan risiko yang berbeda akibat bekerja di luar lokasi organisasi.
A1	Verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan hukum, regulasi dan etika terkait dan harus proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.
B2	Aset yang dipelihara dalam inventaris harus dimiliki (ada personel yang bertanggung jawab).
B8	Prosedur harus diimplementasikan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi.
B9	Media harus dihancurkan dengan aman saat tidak lagi dibutuhkan, dengan menggunakan prosedur baku.
B1	Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan inventaris dari aset-aset ini harus dicatat dan dipelihara.
B7	Prosedur penanganan aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi organisasi.
C7	Peralatan harus ditempatkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan peluang untuk akses oleh pihak yang tidak berwenang.
A6	Setelah penghentian atau perubahan kepegawaian, tugas dan tanggung jawab keamanan informasi yang masih berlaku harus ditetapkan, dikomunikasikan kepada pegawai atau kontraktor, dan ditegakkan.
C10	Peralatan harus dipelihara secara tepat untuk menjamin ketersediaan yang berkelanjutan dan integritas
A2	Semua pegawai organisasi dan kontraktor (jika relevan) harus menerima kepedulian, pendidikan, dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka.
C1	Batas fisik keamanan harus ditetapkan dan digunakan untuk melindungi area yang mengandung informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.
A5	Harus ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi.
C8	Peralatan harus dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung.
C9	Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari pencegatan, interferensi atau kerusakan.
C3	Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.
C11	Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin yang berwenang

ID	Pengendalian Keamanan Informasi
A3	Manajemen harus mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan.
C5	Prosedur untuk bekerja dalam daerah aman harus dirancang dan diterapkan.
C13	Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk menjamin bahwa data rahasia dan perangkat lunak berlisensi apapun sudah dihapus atau ditimpa secara aman sebelumnya untuk dibuang atau dipergunakan kembali.
A4	Semua pegawai organisasi dan kontraktor (jika relevan) harus menerima kepedulian, pendidikan, dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka.
C6	Titik akses seperti area bongkar muat dan titik lain yang dapat dimasuki orang yang tidak berwenang harus dikendalikan dan, jika mungkin, dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses oleh pihak yang tidak berwenang
C14	Pengguna harus menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak.

4.2. Pembahasan

Penilaian tingkat risiko keamanan informasi perlu dilakukan dan diketahui karena organisasi perlu mengetahui batas yang aman untuk keamanan informasi dan jika level risiko tidak pada batas aman perlu dilakukannya pengendalian risiko. Dengan mengikuti langkah-langkah evaluasi, organisasi dapat mengidentifikasi area yang memerlukan perbaikan dan mengambil tindakan yang sesuai (Rahayu *et al.*, 2021). Dengan melakukan penilaian risiko keamanan informasi Instansi/Organisasi akan lebih mudah melakukan persiapan dan penanganan keamanan informasi untuk meminimalisir risiko keamanan informasi. Salah satu standar yang popular digunakan untuk persiapan keamanan informasi adalah ISO/IEC 27001:2013. Standar ISO/IEC 27001:2013 bertujuan menentukan persiapan keamanan informasi untuk menetapkan, menerapkan, memelihara dan terus meningkatkan keamanan informasi yang diintegrasikan kedalaman tata kelola sistem informasi dengan tujuan mengamankan sumber informasi (Carvalho *and* Marques, 2019).

Salah satu metode untuk penilaian risiko adalah FMEA, Metode FMEA merupakan salah satu metode penilaian risiko proaktif yang paling dikenal dan banyak digunakan (Hisprastin *and* Musfiroh, 2020). FMEA adalah metode terstruktur yang dapat digunakan untuk mengidentifikasi dan memprioritaskan risiko untuk meningkatkan kualitas dan keamanan informasi (Aldenny *et al.*, 2022; Zilfianah *et al.*, 2022). Manfaat dalam menggunakan metode FMEA yaitu bisa menentukan prioritas untuk setiap tindakan perbaikan, menyediakan dokumen yang lengkap tentang perubahan proses dimana untuk membantu perkembangan selanjutnya, meningkatkan kualitas, keandalan, dan keamanan (Zilfianah *et al.*, 2022).

Berdasarkan hasil perhitungan dengan metode FMEA, level tertinggi risiko keamanan informasi pada level tinggi dengan nilai RPN 144. Risiko tersebut pada ID B4 yaitu semua pegawai dan pengguna pihak eksternal tidak mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka, dan ID B6 yaitu Seperangkat prosedur yang tepat untuk pelabelan informasi tidak dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi. Sedangkan level terendah risiko yaitu level kecil dengan nilai RPN 28 yaitu pada ID C14 yaitu Pengguna tidak menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak.

Penelitian yang dilakukan oleh Jauhary *et al.*, (2022) didapatkan bahwa dengan menerapkan standar ISO/IEC 27001 organisasi menjadi tidak rentan terhadap risiko keamanan informasi. Penelitian yang dilakukan oleh Yuwono *et al.*, (2022) menjelaskan jika organisasi telah standar ISO/IEC 27001:2013 *stackholders* akan lebih nyaman melakukan bisnis. Dari kedua penelitian tersebut bisa simpulkan bahwa dengan menerapkan keamanan informasi, Instansi XYZ akan mendapatkan kepercayaan publik untuk menjaga keamanan data dan Instansi XYZ akan tidak rentan terhadap ancaman keamanan informasi.

5. Kesimpulan

Berdasarkan penelitian pengukuran risiko dan keamanan informasi menggunakan metode FMEA, ditemukan 4 ancaman keamanan informasi dengan tingkar risiko tinggi, 9 ancaman keamanan informasi dengan tingkat risiko sedang, dan 16 ancaman keamanan informasi dengan tingkat risiko kecil. Instansi XZY perlu melakukan pengendalian terhadap prioritas risiko keamanan informasi berdasarkan rekomendasi ISO/IEC 27001:2013.

Saran untuk penelitian selanjutnya adalah analisis risiko keamanan informasi berbasis ISO/IEC 27001:2013 disarankan menganalisis risiko dari semua klausul ISO 27001 yakni 14 klausul untuk menilai keseluruhan sistem tata kelola. Selain itu juga metode FMEA dapat dikombinasikan dengan metode lainya seperti *Naïve Bayes.*

Daftar Pustaka

Achmadi, D., Suryanto, Y., Ramli, K., 2018. On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *2018 International Workshop on Big Data and Information Security, IWBIS 2018*, 149-157. https://doi.org/10.1109/IWBIS.2018.8471700

Aldenny, M., Kristian, H., Gaol, F.L., Matsuo, T., Nugroho, A., 2022. The Implementation of Failure Mode and Effects Analysis (FMEA) of the Information System Security on the Government

Electronic Procurement Service (LPSE) System. *Lecture Notes in Networks and Systems*, 317, 1-12. http://dx.doi.org/10.1007/978-981-16-5640-8_1

Anggraini, D., Bisma, R., 2021. Perencanaan Tata Kelola Keamanan Informasi dalam Penerapan Cloud Computing Menggunakan ISO 27001:2013 pada PT.SPINDO,Tbk. *Journal of Informatics and Computer Science (JINACS)*, 3(1), 46-54. https://doi.org/10.26740/jinacs.v3n01.p46-54

Aprianto, T., Setiawan, I., Purba, H.H., 2021. Implementasi Metode Failure Mode and Effect Analysis pada Industri di Asia – Kajian Literature. *Matrik*, 21(2), 165-174. http://dx.doi.org/10.30587/matrik.v21i2.2084

Balaraju, J., Raj, M.G., Murthy, C.S., 2019. Fuzzy-FMEA Risk Evaluation Approach for LHD Machine-A Case Study', *Journal of Sustainable Mining*, 18(4), 257-268. https://doi.org/10.1016/j.jsm.2019.08.002

Carvalho, C., Marques, E., 2019. Adapting ISO 27001 to a Public Institution. *Iberian Conference on Information Systems and Technologies (CISTI)*, 19-22. https://doi.org/10.23919/CISTI.2019.8760870

Culot, G., Nassimbeni, G., Podrecca, M., Sartor, M., 2021. The ISO/IEC 27001 information security Management Standard: Literature Review and Theory-Based Research Agenda. *TQM Journal*, 33(7), 76-105. https://doi.org/10.1108/TQM-09-2020-0202

Eskaluspita, A.Y., 2020. ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. *IOP Conf. Ser.: Mater. Sci. Eng.*, 879, 012074. http://dx.doi.org/10.1088/1757-899X/879/1/012074

Hakim, A.R., Wijaya, R.A.P., 2020. Perancangan Perangkat Audit Internal untuk Sistem Keamanan Informasi pada Organisasi XYZ. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 7(3), 435-442 https://doi.org/10.25126/jtiik.2020701940

Hartanti, L.P.S., Mulyono, J., Mayang, V., 2022. Penerapan FMEA dan Fuzzy FMEA dalam Penilaian Risiko Lean Waste di Industri Manufaktur. *JST (Jurnal Sains dan Teknologi)*, 11(2), 293-304. http://dx.doi.org/10.23887/jstundiksha.v11i2.50552

Herkules, Putra, C., Hadi, A., 2023. Tata Kelola Data Center Berbasis ISO 27001 dan ISO 20000 pada DISKOMINFOSANTIK Kalimantan Tengah. Jurnal Sistem Informasi, Manajemen dan Teknologi Informasi, 1(2), 203-219. https://doi.org/10.33020/jsimtek.v1i2.429

Hisprastin, Y., Musfiroh, I., 2020. Ishikawa Diagram dan Failure Mode Effect Analysis (FMEA) sebagai Metode yang Sering Digunakan dalam Manajemen Risiko Mutu di Industri. *Majalah Farmasetika*, 6(1), 1-9. http://dx.doi.org/10.24198/mfarmasetika.v6i1.27106

Jauhary, H., Pratiwi, G.E., Salim, A.Z., Fitroh, 2022. Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review'. *Media Jurnal Informatika*, 14(1), 43-49. https://doi.org/10.35194/mji.v14i1.1581

Kamil, Y., Lund, S., Islam, M.S., 2023. Information Security Objectives and the Output Legitimacy of ISO/IEC 27001: Stakeholders' Perspective on Expectations in Private Organizations in Sweden. *Inf Syst E-Bus Manage*, 21, 699-722. https://doi.org/10.1007/s10257-023-00646-y

Kristanto, T., Sholik, M., Rahmawati, D., Nasrullah, M., 2019. Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 pada Staff IT Support di Instansi XYZ. *JISA(Jurnal Informatika dan Sains)*, 2(2), 30-33. https://doi.org/10.31326/jisa.v2i2.497

Mirtsch, M., Kinne, J., Blind, K., 2021. Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, 68(1), 87-100. https://doi.org/10.1109/TEM.2020.2977815

Musyarofah, S.R., Bisma, R., 2021. Analisis Kesenjangan Sistem Manajemen Keamanan Informasi (SMKI) Sebagai Persiapan Sertifikasi ISO/IEC 27001:2013 pada Institusi Pemerintah. *Teknologi*, 11(1), 1-15. https://doi.org/10.26594/teknologi.v11i1.2152

Nuchpho, P., Nansaarng, S., Pongpullponsak, A., 2019. Modified Fuzzy FMEA Application in the Reduction of Defective Poultry Products. *Engineering Journal*, 23(1), 171-190. https://doi.org/10.4186/ej.2019.23.1.171

Nurkertamanda, D., Wulandari, F.T., 2019. Analisa Moda dan Efek Kegagalan (Failure Mode and Effect Analysis/FMEA) pada Produk Kursi Lipat Chitose Yamamoto HAA', *J@ti Undip: Jurnal Teknik Industri*, 4(1), 49-64. https://doi.org/10.12777/jati.4.1.49-64

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*, 8(2), 2813-2825.

Paradise, Kusrini, K., Nasiri, A., 2020. Audit Keamanan Aplikasi E-Cash Menggunakan Iso 27001. *Creative Information Technology Journal*, 5(4), 243-253. https://doi.org/10.24076/citec.2018v5i4.209

Podrecca, M., Sartor, M., 2023. Forecasting the Diffusion of ISO/IEC 27001: a Grey Model Approach. *TQM Journal*, 35(9), 123-151. https://doi.org/10.1108/TQM-07-2022-0220

Pribadi, H.I., Ernastuti, 2020. Manajemen Risiko

Teknologi Informasi pada Penerapan E-Recruitment Berbasis ISO 31000:2018 dengan FMEA (Studi Kasus PT Pertamina). *Jurnal Sistem Informasi Bisnis*, 10(1), 28-35. https://doi.org/10.21456/vol10iss1pp28-35

Rahayu, S.F., Prawira, D., Rusi, I., 2021. Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks Kami (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak. *Coding : Jurnal Komputer dan Aplikasi*, 09(3), 468-477. https://dx.doi.org/10.26418/coding.v9i03.51126

Roy, P.P., 2020. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications(NCETSTEA)*, 53, 27001-27003. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Ruiz, L.C., Amado, M.L., Carrasco, J.R., Arenas, L.A., 2022. Implementation of Information Security Audit for the Sales System in a Peruvian Company. *International Journal on Advanced Science, Engineering and Information Technology*, 12(3), 1189–1195. https://doi.org/10.18517/ijaseit.12.3.13969

Safitri, E.M., Sesha, P.S.K., Ningtias, J.P., 2020. Analisis Penilaian Risiko pada Keamanan Sistem Informasi: Studi Literatur. *Jurnal Informatika dan Sistem Informasi (JIFoSI)*, 1(2), 601-607.

Suwarsono, L. W., Aisha, A. N., Nugraha, F.N., 2022. The Role of E-Learning Readiness on Workload: Perspective Engineering and non-Engineering Students. *International Journal of Innovation in Enterprise System*, 6(1), 85-94. https://doi.org/10.25124/ijies.v6i01.165

Triantono, H.B., 2007. Kebijakan Keamanan dengan Standar BS 7799/ISO 17799 pada Sistem Manajemen Keamanan Informasi Organisasi. *Seminar Nasional Aplikasi Teknologi Informasi*, 2007(SNATI), 1907-5022.

Wicaksono, A. C., Prabowo, S., Oktaria, D., 2022. Risk and Security Measurement Based on ISO 27001 using FMEA Methodology Case Study: National Government Agency. *2022 1st International Conference on Software Engineering and Information Technology, ICoSEIT 2022*, (95), 6-11. https://doi.org/10.1109/ICoSEIT55604.2022.10029988

Yuwono, S.T., Pratama, N., Afifah, V., 2022. Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001: 2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK. *Jurnal IKRAITH-Informatika*, 6(2), 21-28.

Zilfianah, K., Ismiyah, E., Rizqi, AW., 2022. Quality Control Analysis on Steel Construction Projects Using the Method Statistical Quality Control and Failure Mode and Effects Analysis. *MOTIVECTION : Journal of Mechanical, Electrical and Industrial Engineering*, 5(1), 13-32. https://doi.org/10.46574/motivection.v5i1.174