Jurnal Sistem Informasi Bisnis 02(2024)
Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/61481

Evaluasi Keamanan Sistem Informasi Menggunakan *Fuzzy* FMEA Berbasis *Framework* ISO/IEC 27001:2013 untuk Meningkatkan Keamanan Informasi

Aris Kusnandar*

Magister Sistem Informasi, Sekolah Pascasarjana, Universitas Diponegoro, Semarang

Naskah masuk: 14 Januari 2024; Diterima untuk publikasi: 15 Maret 2024
DOI: 10.21456/vol14iss2pp181-190

Abstract

Very few organizations are not aware of the importance of information security, even though information security is important to the running of an organization. Dinas Kependudukan XYZ faces a number of information security threats from various sources. Every security threat such as information theft, fraud, vandalism, and computer hacking will affect the organization. This research uses the ISO/IEC 27001:2013 framework as a method for. analyze risks. The risk value calculation uses the FMEA method which is integrated with the fuzzy method to determine the risk level of information security threats based on ISO/IEC 27001:2013. The research results are in the form of a risk processing report containing a list of risk priorities and control plans according to the ISO/IEC 27001:2013 standard. The information security risk priorities obtained in this research were 13 very high priority and 10 high priority. This proves that the organization has not complied with standard security/information procedures so it needs to document security policies based on ISO/IEC 27001:2013 to provide a sense of security and increase trust in the public.

Keywords: FMEA; Fuzzy; ISO 27001; Information Security

Abstrak

Sangat sedikit organisasi yang tidak menyadari akan pentingnya keamanan informasi, padahal keamanan informasi menjadi hal yang penting terhadap jalanya suatu organisasi. Dinas Kependudukan XYZ dihadapkan pada sejumlah ancaman keamanan informasi dari berbagai sumber. Setiap ancaman keamanan seperti pencurian informasi, penipuan, vandalisme, dan peretasan komputer akan mempengaruhi organisasi .Penelitian ini menggunakan kerangka kerja ISO/IEC 27001:2013 sebagai metode untuk menganalisis risiko. Perhitungan nilai risiko menggunakan metode FMEA diintegrasikan dengan metode *fuzzy* untuk mengetahui tingkat risiko ancaman keamanan informasi berdasarkan ISO/IEC 27001:2013. Hasil Penelitian berupa laporan hasil pengolahan risiko yang berisikan daftar prioritas risiko dan rencana pengendalian sesuai standar ISO/IEC 27001:2013. Prioritas risiko keamanan informasi yang didapatkan pada penelitian ini sebanyak 13 prioritas sangat tinggi dan 10 prioritas tinggi. Hal ini membuktikan bahwa organisasi belum mematuhi prosedur standar keamanan/informasi sehingga perlu mendokumentasikan kebijakan keamanan berdasarkan ISO/IEC 27001:2013 supaya memberikan rasa aman dan meningkatkan kepercayaan kepada publik.

Kata kunci: FMEA; *Fuzzy*; ISO 27001; Keamanan Informasi.

1. Pendahuluan

Meningkatnya kebutuhan dan pengguna Teknologi Informasi (TI) dalam menunjang kegiatan suatu organisasi akan meningkatkan risiko ancaman terhadap keamanan informasi. Informasi merupakan aset yang bernilai bagi sebuah organisasi yang perlu dilindungi dari ancaman yang mungkin terjadi, baik dari pihak luar maupun pihak dalam organisasi (Yoseviano *and* Retnowardhani, 2018). Keamanan informasi didefinisikan sebagai terjaganya kerahasiaan, integritas, dan ketersediaan informasi (Mirtsch *et al.*, 2021).

Keamanan informasi menjadi hal yang penting terhadap berjalanya suatu organisasi yang memanfaatkan TI sebagai pendukung proses bisnisnya (Musyarofah *and* Bisma, 2021). Namun demikian, tidak sedikit organisasi yang masih belum menyadari akan pentingnya keamanan informasi. Kebocoran, kerusakan, ketidakakuratan, ketersediaan atau gangguan lain terhadap informasi masih sering dialami organisasi. Kebocoran, kerusakan atau hilangnya suatu informasi dapat menimbulkan kerugian baik secara finansial maupun produktivitas bagi organisasi dan perusahaan (Handayani *et al.*, 2018).

Dinas kependudukan XYZ memiliki fungsi yaitu melakukan pencatatan, mobilitas, pengendalian data penduduk. Dinas Kependudukan XYZ dihadapkan pada sejumlah ancaman keamanan informasi dari berbagai sumber. Setiap ancaman keamanan seperti

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

pencurian informasi, penipuan, vandalisme, dan peretasan komputer akan mempengaruhi organisasi dalam berbagai cara seperti merusak reputasi organisasi, merusak data, kehilangan kepercayaan publik, dan gangguan bisnis (Achmadi *et al.*, 2018). Manfaat keamanan Informasi yaitu memberikan rasa aman dan meningkatkan kepercayaan publik. Untuk Menghindari adanya pencurian dan hilangnya informasi baik disengaja maupun tidak, maka diperlukan penerapan keamanan informasi. Karena instansi pemerintah memiliki peran dalam pengelolaan data dan informasi, tata kelola harus memiliki keamanan informasi yang baik (Kamil, 2023).

Manajemen risiko merupakan serangkaian proses dalam mengidentifikasi risiko, melakukan penilaian risiko, dan menyusun serangkaian tindakan untuk menurunkan risiko tersebut sampai level yang dapat diterima oleh organisasi (Nugraha *et al.*, 2020). Penerapan manajemen risiko memungkinkan organisasi untuk mengevaluasi keamanan informasi dan menerapkan prosedur yang menjaga integritas, kerahasiaan, dan ketersediaan informasi (Carvalho *and* Marques 2019).

Standar keamanan yang sering digunakan pada organisasi di dunia sebagai manajemen kebijakan dan pelaksanaan keamanan informasi organisasi yaitu ISO/IEC 27001. ISO/IEC 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 untuk melawan miliaran serangan yang terjadi setiap tahun (Podrecca *and* Sartor 2023). ISO/EIC 27001 merupakan standar Internasional yang dipersiapkan untuk mengimplementasikan, membangun, memonitor, mengoperasikan serta merawat sistem manajemen keamanan informasi (SMKI) (Fathurohman *and* Witjaksono 2020). Standar ISO/IEC 27001 memiliki kelebihan yaitu dapat dikembangkan tergantung kebutuhan organisasi, tujuan organisasi. Standar ini tidak tergantung pada produk IT, membutuhkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk memastikan bahwa kontrol keamanan yang dipilih mampu untuk melindungi aset informasi dari berbagai risiko (Sulistyowati *and* Ginardi 2019).

Secara umum ISO/IEC 27001:2013 memiliki 34 kontrol dan pada pelaksanaannya organisasi dapat memilih kontrol mana yang relevan dengan kondisi di lapangan. ISO/IEC 27001 ini fokus pada efektivitas dan proses perbaikan yang berkelanjutan dengan menggunakan pola pikir PDCA (*Plan-Do-Check-Action*). Setiap proses PDCA dilakukan dengan perancangan yang matang, implementasi terstruktur dan jelas, dilakukan evaluasi dan analisis data yang akurat, serta tindakan perbaikan yang sesuai dengan monitoring pelaksanaannya supaya dapat menyelesaikan masalah yang terjadi di organisasi.

Failure Mode and Effect Analysis (FMEA) sebagai sarana untuk melakukan analisis manajemen risiko dapat diadopsi untuk mencegah kejadian yang tidak diinginkan untuk menghindari kekecewaan terhadap kepuasan pelanggan (Syreyshchikova *et al*., 2019; Filz *et al*., 2021). Proses FMEA adalah mengidentifikasi potensi kegagalan dan penyebabnya sebelum terjadi dan menganalisis potensi penyebab kegagalan yang diprioritaskan untuk diatasi (Ardyansyah *and* Handayani 2023).

Metode FMEA digunakan untuk mengambil data angka dan penentuan kegagalan mana yang diprioritaskan. Namun, FMEA banyak mendapat kritik dari beberapa penelitian sebelumnya mengenai konsistensi penilaian risiko, karena adanya kesulitan dalam menemukan akar penyebab potensi risiko, mengevaluasi faktor risiko secara akurat dan menentukan kriteria skala (Balaraju *et al.*, 2019). Karena itu, pada penelitian ini metode FMEA diintegrasikan dengan metode fuzzy untuk mengatasi kelemahan tersebut. Pendekatan fuzzy FMEA adalah pondasi terbaik untuk mendapatkan hasil yang akurat (Calache *et al*., 2021).Penelitian yang menggunakan logika *fuzzy* yang dipadukan dengan FMEA memiliki pengaruh yang besar dalam penilaian risiko dan nilai risiko kegagalan yang diperoleh memberikan hasil yang lebih tepat *(Yaqin et al*., 2020).

Tujuan evaluasi keamanan sistem informasi pada penelitian ini adalah untuk mengetahui ancaman dan prioritas risiko keamanan informasi, sebagai pertimbangan pengambilan kebijakan pada level manajemen organisasi dalam penerapan sistem informasi supaya tujuan keamanan informasi tercapai dan tingkat kepercayaan publik meningkat.

2. Kerangka Teori

2.1. Keamanan Informasi

Keamanan informasi merupakan suatu bentuk perlindungan terhadap informasi dan unsur-unsur penting yang ada didalamnya seperti kerahasiaan, integritas, dan ketersediaan. Keamanan Sistem Informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau mendeteksi adanya penipuan disebuah sistem informasi (Nurul *et al*, 2022)

Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan *return of investment* (ROI) serta peluang bisnis (Yusnanto *et al*., 2021). Sistem keamanan sistem informasi terdapat tiga aspek keamanan informasi yang perlu di perhatikan. Aspek-aspek tersebut antara lain (Desy *et al*, 2014)

2.2. ISO/IEC 27001:2013

ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi (SMKI), sering kali digunakan oleh perusahaan untuk

menerapkan keamanan sistem informasi, dengan menerapkan standar ISO/IEC 27001 perusahaan dapat melindungi, memelihara kerahasiaan, integritas dan ketersediaan informasi serta untuk mengelola dan mengendalikan risiko keamanan informasi pada organisasi perusahaan.

Keamanan informasi dicapai dengan menerapkan sebuah kontrol terintegrasi, mulai dari kebijakan, proses, prosedur, struktur organisasi, serta perangkat lunak dan perangkat keras. 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). ISO/IEC 27001 merupakan salah satu standar SMKI yang banyak diadopsi organisasi. Standar ini mengadopsi pendekatan proses model *Plan-Do-Check-Action* untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan SMKI suatu organisasi.

2.3. Failure Mode and Effect Analyis (FMEA)

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 *and* Wulandari, 2019).

Ada dua fase utama dalam metode FMEA. Fase pertama berkaitan dengan identifikasi mode kegagalan potensial dan pengaruhnya. Hal ini termasuk dalam menentukan potensi kegagalan komponen produk, sub-rakitan, perakitan akhir dan proses manufakturnya. Fase kedua berkaitan dengan melakukan analisis kekritisan untuk menentukan tingkat keparahan mode kegagalan dengan mengevaluasi dan memberi peringkat disetiap kegagalan sesuatu dengan tingkat kekritisan suatu kegagalan.

Ada 3 bagian penilaian yaitu *severity* (tingkat keparahan), *occurrence* (kemungkinan terjadi ancaman), dan *detection* (deteksi tiap ancaman) yang nantinya ketiga penilaian tersebut digunakan untuk menghitung RPN (*Risk Priority Number*).

2.4. Fuzzy FMEA

Terjadi tren yang berkembang pada literatur FMEA dengan menggunakan istilah fuzzy linguistik untuk menggambarkan tiga faktor resiko *severity*, *occurence*, dan *detection* (Kang *et al*., 2017). Sebagian besar studi yang ada mengenai fuzzy FMEA berhubumgam degan pendekatan *rule base fuzzy* dengan menggunakan aturan "*if-then*". Ada tiga tahapan utama dalam fuzzy FMEA, yaitu:

1) *Fuzzification*, proses menggunakan variabel linguistik untuk mengonversi tiga faktor risiko *severity*, *occurrence*, *dan detection* kedalam *fuzzy*. Menggunakan variabel linguistik beserta definisi, kemudian membuat peringkat tiga faktor tersebut pada skala dasar, dengan tujuan untuk memperoleh derajat keanggotaan pada setiap kelas;
2) Mesin inferensi berisi pengetahuan dari para ahli mengenai interaksi mode kesalahan dan efek yang ditimbulkan dalam bentuk aturan fuzzy "*if then".* Aturan tersebut lebih mudah dirumuskan dalam aturan lingusitik dibanding dengan numerik;
3) *Difuzzification*, proses menciptakan peringkat dari Fuzzy RPN untuk memberikan tingkat prioritas mode kesalahan. Proses defuzzifikasi menggunakan metode *centroid*.

3. Metode

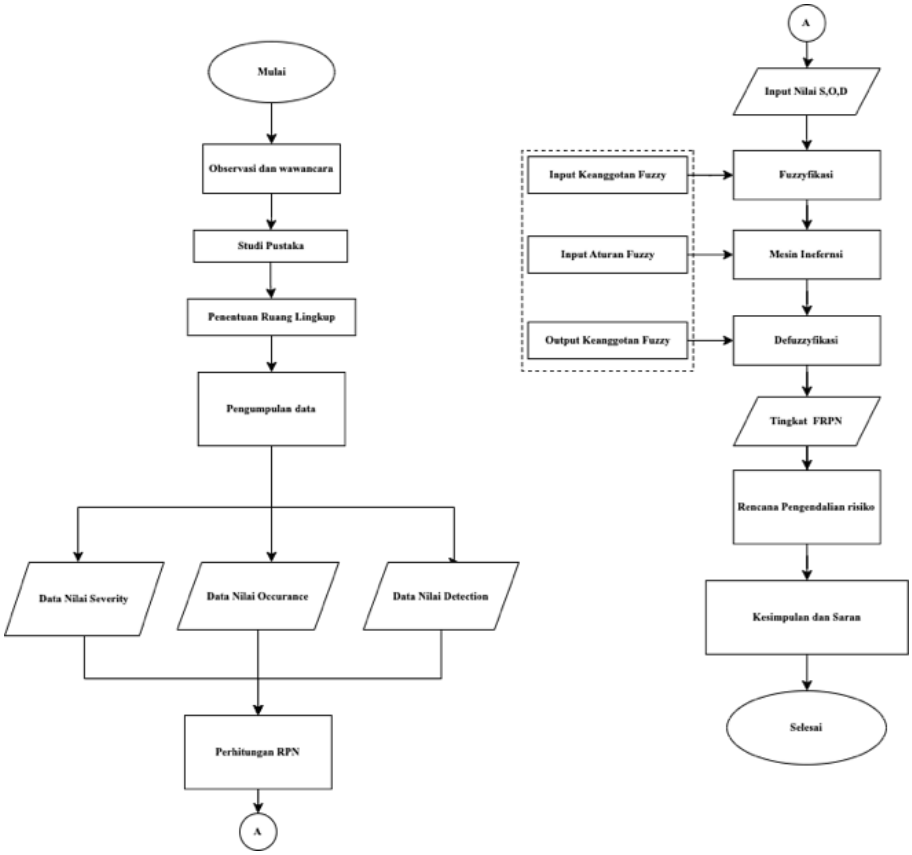
3.1. Prosedur Penelitian

Prosedur penelitian menggunakan prinsip pengembangan model PDCA untuk mewujudkan sistem yang selalu berkembang menjadi lebih baik secara kualitas, efektivitas, maupun efisiensi. Model PDCA ada 4 Fase yaitu:

1) Fase perencanaan yaitu melakukan tahapan Observasi ke objek penelitian dengan secara langsung untuk meninjau dokumen sehingga mendapatkan informasi yang akurat dan jelas kapabilitasnya. Wawancara dilakukan untuk mengetahui masalah yang ada di objek penelitian. studi Pustaka yaitu mengumpulkan informasi yang relevan untuk penelitian dan pemilihan ruang lingkup dengan menetapkan cakupan yang dinilai keamanan informasi;
2) Fase pelaksanaan yaitu melakukan pengumpulan data dengan memberikan kuesioner berisi risiko-risiko keamanan informasi untuk mendapatkan nilai *severity*, nilai *occurance*, dan nilai *detection* berdasarkan parameter nilai yang sudah ditentukan;
3) Fase pengendalian yaitu melakukan perhitungan fuzzy FMEA dengan melakukan tiga Langkah yakni fuzzyfikasi, mesin inferensi dan defuzzyfikasi untuk mendapatkan nilai *Fuzzy Risk Priority Number* (FRPN).
4) Fase penyesuaian yaitu perbaikan dan pengembangan keamanan informasi dengan memberikan rekomendasi terhadap objektif kontrol mengacu pada ISO/IEC 27001:2013.

Flowchart Prosedur penelitian tampak pada Gambar 1.

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/61481



Gambar 1. Prosedur Penelitian

3.2. Pengumpulan Data

Tahap pengumpulan data, penulis melakukan penyebaran kuesioner terkait ancaman keamanan informasi berbasis ISO/IEC 27001:2013 yang sebelumnya telah dilakukan analisis masalah untuk selanjutnya dilakukan pengujian validitas dan reliabilitas. Instrumen yang *valid* dan reliabel maka dilakukan pembobotan risiko dengan metode *Fuzzy* FMEA.

Skala pengukuran merupakan acuan untuk menentukan interval yang terdapat dalam satuan alat ukur guna menghasilkan data kuantitatif, adapun penelitian ini menggunakan pengukuran nominal dari kategori responden seperti kepala dinas, sekretaris dinas, dan kepala bidang dengan ukuran pernyataan pada Tabel 1.

Tabel 1. Skala Pengukuran

Ukuran Pernyataan	Bobot Nilai
Tidak Dilaksanakan	1
Dalam perencanaan	2
Penerapan/Diterapkan sebagian	3
Diterapkan menyeluruh	4

3.3. Analisis Data

Pada tahap analisis dengan FMEA dilakukan identifikasi penilaian risiko terhadap sistem informasi Dinas Kependudukan XYZ bertujuan untuk memahami seberapa besar risiko apa yang akan diterima oleh organisasi atau perusahaan jika informasi yang dikelola mendapatkan ancaman atau gangguan keamanan yang menyebabkan gagalnya penjagaan aspek keamanan informasi dan dapat menganggu tercapainya sasaran dan tujuan organisasi. FMEA mengevaluai kegagalan dengan pemberian skor masing-masing moda kegagalan berdasarkan atas tingkat keparahan (*severity*), kejadian (*occurrence*), dan deteksi (*detection*). Berikut Tabel 2. merupakan acuan nilai dalam menentukan keparahan ancaman.

Tabel 2. Nilai *Severity*

Nilai	Severity	Deskripsi
10	Berbahaya tanpa peringatan	Keparahan sangat tinggi. Mode kegagalan potensial mempengaruhi operasi sistem tanpa peringatan
9	Berbahaya dengan peringatan	Keparahan sangat tinggi. Mode kegagalan potensial mempengaruhi operasi sistem dengan peringatan
8	Sangat tinggi	Sistem tidak dapat dioperasikan dengan kegagalan yang merusak tanpa mengorbankan keamanan
7	Tinggi	Sistem tidak dapat dioperasikan dengan kerugian atau kerusakan peralatan
6	Sedang	Sistem tidak dapat dioperasikan. Ada kerusakan kecil

Nilai	Severity	Deskripsi
5	Rendah	Sistem tidak dapat dioperasikan. Tidak ada kerugian
4	Sangat rendah	Sistem dapat dioperasikan dengan beberapa penurunan kinerja yang sangat signifikan
3	Kecil	Sistem dapat dioperasikan dengan beberapa penurunan kinerja
2	Sangat kecil	Sistem dapat dioperasikan dengan gangguan minimal
1	Tidak ada	Tidak ada efek

Apabila sudah ditentukan nilai *severity*, maka tahap selanjutnya adalah menentukan rating terhadap nilai *occurrence*. *Occurrence* adalah suatu penilaian mengenai peluang (probabilitas) frekuensi penyebab mekanisme kegagalan yangakan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat saat ancaman terjadi. Nilai o*ccurance* tampak pada Tabel 3.

Tabel 3. Nilai *Occurrence*

Nilai	*Occurance*	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 kal dalam 6-9 tahun	Kegagalan hampir/tidak pernah terjadi

Setelah diperoleh nilai *occurrence*, selanjutnya adalah menentukan nilai. Nilai *detection* diasosiasikan dengan pengendalian saat ini. *Detection* adalah pengukuran terhadap kemampuan mengendalikan/mengontrol kegagalan yang dapat terjadi. Nilai *detection* tampak pada Tabel 4.

Tabel 4. Nilai *Detection*

Nilai	*Detection*	Deskripsi
10	Hampir tidak mungkin	Pasti tidak dapat terdeteksi/ tidak dapat terkontrol
9	Sangat susah	Sangat susah untuk mendeteksi risiko, sangat sudengsah 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

4. Hasil dan Pembahasan

4.1. Identifikasi Risiko

Identifikasi ririko sebagai variable penelitian adalah dengan menggunakan standarisasi ISO/IEC 27001:2013. Terkait identifikasi risiko ancaman keamanan informasi dilakukan analisis masalah dengan melakukan wawancara dengan manajerial Dinas Kependukan XYZ yakni Kepala Dinas, Sekretaris Dinas, dan Kepala Bidang. Berdasarkan hasil analis masalah ditemukan 4 klausul dari 14 klausul yang menjadi kemungkinan risiko ancaman. Klasul tersbut yaitu (1) kebijakan keamanan informasi, (2) organisasi keamanan informasi, (3) keamanan sumber daya manusia dan (4) manajemen aset. Berikut rincian kemungkinan risiko ancaman keamanan sistem informasi Dinas Kependudukan XYZ. Berikut Tabel 5. yang berisi dari ancaman dari klausul kebijakan keamanan informasi.

Tabel 5. Klausul Kebijakan Keamanan Informasi

ID	Kemungkinan Ancaman
R1.1	Kebijakan untuk keamanan informasi tidak terimplementasikan dengan baik.
R1.2	Kebijakan untuk keamanan informasi tidak di evaluasi secara terencana.

Sedangakan ancaman dari klausul organisasi keamanan informasi tampak pada Tabel 6. yang berisi 7 ancaman.

Tabel 6. Klausul Organisasi Keamanan Informasi

ID	Kemungkinan Ancaman
R2.1	Tanggung jawab keamanan informasikan tidak didefinisikan dan dialokasikan dengan kurang tepat
R2.2	Tugas dan area tanggung jawab yang bertentangan tidak dipisahkan (dijabat oleh personil yang sama)
R2.3	Hubungan baik dengan pihak berwenang terkait kurang dipelihara dengan baik
R2.4	Hubungan baik dengan komunitas, forum, dan asosiasi profesional spesialis keamanan kurang dipelihara.
R2.5	Keamanan informasi tidak diterapkan ke dalam manajemen proyek.
R2.6	Kebijakan dan tindakan keamanan yang mendukung perangkat bergerak tidak diadopsi dengan baik.
R2.7	Kebijakan dan tindakan keamanan yang mendukung tidak diimplementasikan untuk melindungi informasi yang diakses, diproses atau disimpan di dalam situs.

Adapun ancaman klausul keamanan sumber daya manusia tampak pada Tabel 7., yang berisi 6 ancaman keamanan.

Tabel 7. Klausul Keamanan Sumber Daya Manusia

ID	Kemungkinan Ancaman
R3.1	Verifikasi latar belakang dari semua calon pegawai tidak dilaksanakan berdasarkan hukum, regulasi dan etika terkait dan tidak proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.
R3.2	pegawai dan kontraktor tidak menyatakan perjanjian tertulis (syarat dan ketentuan pegawai) tentang keamanan informasi dan organisasi
R3.3	Organisasi tidak mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan.
R3.4	Semua pegawai dan kontraktor (jika relevan) kurang menerima kepedulian, pendidikan, dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka.
R3.5	tidak ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap n pegawai yang melakukan pelanggaran keamanan informasi.
R3.6	Setelah penghentian atau perubahan kepegawaian, tugas dan tanggung jawab keamanan informasi yang masih berlaku. tidak ditetapkan, dikomunikasikan kepada pegawai atau kontraktor, dan ditegakkan.

Sedangkan ancaman pada klausul manajemen aset tampak pada Tabel 8., yang berisi 10 ancaman keamanan.

Tabel 8. Klausul Manajemen Aset

ID	Kemungkinan Ancaman
R4.1	Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi tidak diidentifikasi dan inventaris dari aset-aset ini tidak dicatat dan kurang dipelihara.
R4.2	Tidak ada pegawai yang bertanggung jawab atas aset yang ada
R4.3	Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi tidak diidentifikasi, tidak didokumentasi dan tidak diimplementasikan.
R4.4	Semua pegawai dan pengguna pihak eksternal tidak mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.
R4.5	Informasi tidak diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.
R4.6	Seperangkat prosedur yang tepat untuk pelabelan informasi tidak dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
R4.7	Prosedur penanganan aset tidak dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi organisasi.
R4.8	prosedur tidak diimplementasikan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi.
R4.9	Media tidak dihancurkan dengan aman saat tidak lagi dibutuhkan, dengan menggunakan prosedur baku.
R4.10	Media yang mengandung informasi tidak dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah selama dipindahkan.

4.2. Hasil Validitas dan Reliabilitas

Pengujian validitas instrument penelitian ini dilakukan pada setiap kemungkinan risiko ancaman dengan 43 responden. Pengujian menggunakan persamaan pearson seperti pada Persamaan (1).

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

dengan:

r_{xy} : Korelasi antara variabel x dan y
x_i : Nilai x ke-i
y_i : Nilai y ke-i
n : Banyaknya nilai

Validitas digunakan untuk melihat sejauh mana ketepatan dan kecermatan suatu alat ukur dalam melakukan fungsi ukurnya. Berikut Tabel 9. adalah hasil dari pengolahan kuesioner. Nilai kesalahan (signifikansi) hasil dari perhitungan dibandingkan dengan probabilitas kesalahan yang ditetapkan dan disimbolkan dengan alpha (α). Jika nilai signifikansi < 0.05, maka suatu *item* instrumet yang diuji korelasinya adalah *valid*.

Tabel 9. Hasil Uji Validitas

ID	r hitung	r variabel	Keterangan
R1.1	0,789	0,301	*Valid*
R1.2	0,218	0,301	Tidak *Valid*
R2.1	0,835	0,301	*Valid*
R2.2	0,743	0,301	*Valid*
R2.3	0,908	0,301	*Valid*
R2.4	0,967	0,301	*Valid*
R2.5	0,935	0,301	*Valid*
R2.6	0,944	0,301	*Valid*
R2.7	0,834	0,301	*Valid*
R3.1	0,889	0,301	*Valid*
R3.2	0,775	0,301	*Valid*
R3.3	0,819	0,301	*Valid*
R3.4	0,798	0,301	*Valid*
R3.5	0,901	0,301	*Valid*
R3.6	0,758	0,301	*Valid*
R4.1	0,787	0,301	*Valid*
R4.2	0,686	0,301	*Valid*
R4.3	0,774	0,301	*Valid*
R4.4	0,815	0,301	*Valid*
R4.5	0,691	0,301	*Valid*
R4.6	0,687	0,301	*Valid*
R4.7	0,782	0,301	*Valid*
R4.8	0,723	0,301	*Valid*
R4.9	0,127	0,301	Tidak *Valid*
R4.10	0,581	0,301	*Valid*

Berdasarkan hasil validitas kuesioner terkait keumgkinan risiko pada sistem informasi Dinas Kependukan XYZ ditemukan 2 kemungkinan risiko tidak *valid*, dengan demikian kemungkinan risiko

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/61481

adalah 23 kemungkinan risiko. Uji reliabilitas dengan menggunakan rumus *Cronbach Alpha* 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 tiap-tiap item
σ_t^2 : Varian total

Berdasarkan rumus uji reliabilitas variabel penelitian diperoleh hasil pengujian *Cronbach Alpha* sebesar 0.969 yang berarti memiliki nilai reliabilitas tinggi . Kuesioner dikatakan *reliable* jika nilai *cronbach alpha* >0.6 (Suwarsono et *al.*, 2022).

4.3. Analisi Fuzzy FMEA

Berdasarkan penelitian sebelumnya dimana penilaian risiko sistem informasi pada Fakultas Teknik Universitas Diponegoro menggunakan metode FMEA (Handayani *et al*., 2018), sedangkan pada penelitian ini menggunakan Fuzzy FMEA sehingga hasil prioritas risiko lebih akurat.FMEA memiliki kelemahan yaitu ketiga kriteria FMEA (S, O, D) memiliki kepentingan yang sama namun dalam kenyataanya memiliki kepentingan yang berbeda.

Fuzzy FMEA memiliki beberapa tahapan yakni fuzzyfikasi, mesin inferensi, dan defuzzyfikasi. Fuzzifikasi adalah proses yang digunakan untuk mengubah parameter masukan menjadi besaran derajat keanggotaan, yang menyatakan parameter masukan dalam bentuk istilah linguistik kualitatif (Balaraju *et al.*, 2019). Variabel linguistik untuk mengonversi tiga faktor risiko *severity*, *occurence*, dan *detection* kedalam *input fuzzy*. Menggunakan variabel linguistik beserta definisi, kemudian membuat peringkat tiga faktor tersebut pada skala dasar, dengan tujuan untuk memperoleh derajat keanggotaan pada setiap kelas, istilah linguistik untuk menggambarkannya adalah *None*, *Low*, *Medium*, *High*, *Very High* (Balaraju *et al.*, 2019). Tabel 10. menunjukan *variable input fuzzy*.

Tabel 10. Variabel *Input Fuzzy* FMEA

Input	*None*	*Low*	*Medium*	*High*	*Very High*
Severity	1-2	1-4	3-7	6-9	8-10
Occurance	1-2	1-4	3-7	6-9	8-10
Detection	1-2	1-4	3-7	6-9	8-10

Mesin Inferensi, berisi pengetahuan dari para ahli mengenai interaksi mode kesalahan dan efekyang ditimbulkan dalam bentuk aturan *fuzzy* "*if then*." Aturan yang terdapat didalam fuzzy FMEA ini merupakan kombinasi dari tiga variabel *input* yaitu *severity*, *occurrence*, dan *detection* serta ditambah *output* dari *fuzzy* RPN itu sendiri dengan menggunakan *if-then rules*. *Rules* yang terbentuk dari tiga variabel *input* tersebut terdiri dari S sebanyak 5 kategori, O sebanyak 5 kategori, dan D sebanyak 5 kategori, sehingga diperoleh total sebanyak 125 *rules* (5x5x5). Tabel 11. beberapa aturan Fuzzy FMEA.

Tabel 11. Aturan *Fuzzy* FMEA

Severity	*Occurance*	*Detection*	*Output*
None	*Medium*	*Low*	Rendah
Low	*High*	*Low*	Tinggi
Medium	*High*	*Medium*	Sangat Tinggi

Defuzzyfikasi adalah kesimpulan *fuzzy* dapat dikonversi menjadi representasi risiko yang memiliki keluaran angka. Angka tersebut disebut juga dengan *Fuzzy Risk Priority Number* (FRPN). Keanggotaan untuk output himpunan fuzzy berdasarkan nilai skala *severity*, *occurrence* dan *detection* dengan rentan antara 1-10. Sedangkan keluaranya memiliki rentan nilai 1-200, nilai parameter keluaran memiliki kategori dan tipe kurva yang berbeda seperti tampak pada Tabel 12.

Tabel 12. Kategori Prioritas Risiko

Rentan	Kategori
1-60	Rendah
40-120	Sedang
80-180	Tinggi
140-200	Sangat Tinggi

Analis Risiko menggunakan metode *Fuzzy* FMEA diperoleh dengan melakukan langkah-langkah pada sebelumnya. Berikut Tabel 13. merupakan hasil perbandingan perhitungan RPN dan *Fuzzy* RPN.

Tabel 13. Hasil *Fuzzy* FMEA dan FMEA

ID	S	O	D	FRPN	RANK FRPN	RPN	RANK RPN
R1.1	9	4	2	180	1	72	6
R2.1	8	2	3	137	2	48	10
R2.2	8	3	2	137	2	48	10
R2.3	7	2	2	137	2	28	12
R2.4	8	3	3	137	2	72	6
R2.5	9	2	4	180	1	72	6
R2.6	7	4	2	137	2	56	8
R2.7	8	3	4	180	1	96	4
R3.1	8	4	3	180	1	96	4
R3.2	8	4	2	180	1	64	7
R3.3	9	2	2	137	2	36	11
R3.4	7	2	2	137	2	28	12
R3.5	9	3	2	137	2	54	9
R3.6	8	3	3	137	2	72	6
R4.1	7	4	3	137	2	84	5
R4.2	8	3	4	180	1	96	4
R4.3	8	4	4	180	1	128	2
R4.4	9	4	4	180	1	144	1
R4.5	8	4	4	180	1	128	2

ID	S	O	D	FRPN	RANK FRPN	RPN	RANK RPN
R4.6	9	4	4	180	1	144	1
R4.7	8	4	3	180	1	96	4
R4.8	9	3	4	180	1	108	3
R4.10	9	4	3	180	1	108	3

4.4. Pengendalian Risiko

Berdasarkan perhitungan antara FMEA dengan *Fuzzy* FMEA pada Tabel 13., FMEA sudah bisa memberi peringkat risiko dan mengevaluasi ancaman keamanan informasi, namun FMEA memiliki beberapa kelemahan sehingga dinilai kurang akurat dalam mengevaluasi ancaman keamanan informasi. Kelemahan FMEA yaitu ketiga kriteria yakni *severity*, *occurance*, dan *detection* memiliki tingkat kepentingan yang sama, namun dalam praktiknya ketiga kriteria tersebut memiliki tingkat kepentingan yang berbeda. ID R2.4 yaitu Hubungan baik dengan komunitas, forum, dan asosiasi profesional spesialis keamanan kurang dipelihara. dan R2.5 yaitu Keamanan informasi tidak diterapkan ke dalam manajemen proyek, memiliki hasil nilai RPN yang sama, namun dalam perhitungan dengan *fuzzy* FMEA didapatkan hasil nilai yang berbeda. Terdapat nilai yang sama dalam perkalian S, O, D yang menghasilkan nilai RPN, sementara tingkat kepentingan mengartikan representasi risiko yang berbeda. *Fuzzy* FMEA merupakan ekspansi dari pendekatan FMEA yang memberikan fleksibilitas terhadap ketidakpastian akibat samarnya suatu informasi yang diterima maupun unsur alternatif yang subjektif yang digunakan dalam penilaian terhadap mode kegagalan yang terjadi (Nuchpho *et al.*, 2019). Hasil perhitungan FMEA dan *fuzzy* FMEA menunjukkan hasil yang relatif sama, terutama pada rangking RPN. R4.4 dan R4.6 contohnya pada perhitungan FMEA pada peringkat 1 dan pada perhitungan *fuzzy* FMEA juga pada peringkat 1, maka perhitungan *fuzzy* FMEA tidak bertentangan dengan FMEA meskipun ada sedikit perbedaan. Penelitian membuktikan bahwa perhitungan *fuzzy* FMEA memperkuat hasil dari perhitungan metode FMEA, sehingga hasil lebih dapat diandalkan. Hasil perhitungan ini bermanfaat dalam merumuskan rekomendasi perbaikan.

Prioritas risiko yang mendesak untuk ditindaklajuti adalah R4.4 yaitu pegawai dan pengguna pihak eksternal tidak mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka, dan R4.6 yaitu prosedur yang tepat untuk pelabelan informasi tidak dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi. . Usualan pengendalian risiko R4.4 adalah semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka (ISO/IEC 27001:2013). Dinas Kependudukan telah memiliki kebijakan untuk mengembalikan aset organisasi yang telah dikuasai ketika menjadi pegawai, namun kebijakan tersebut belum dilaksanakan dengan baik. Pembaharuan kebijakan tentang pengembalian aset harus ditetapkan secara tertulis yang menetapkan aturan yang jelas dan segera tujuanya adalah untuk melindungi aset organisasi sebagai bagian dari proses perubahan atau pemutusan hubungan kerja, kontrak atau perjanjian.

Sedangkan usulan pengendalian risiko R4.6 adalah Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.(ISO/IEC 27001:2013). Aset informasi diberi label dengan menambahkan metadata, sehingga pengelola metadata harus bertanggung jawab dalam menerapkan proses pelabelan dengan benar. Semua aset data harus diberi label yang sesuai, dan pemilik aset melakukan modifikasi apapun pada pelabelan harus dengan izin akses. Berdasarkan perhitungan *fuzzy* FMEA masih banyak kontrol keamanan yang memiliki prioritas sangat tinggi dan tinggi Berikut Tabel 14. merupakan rencana pengendalian risiko untuk meminimalisir ancaman keamanan informasi berdasarkan ISO/IEC 27001:2013.

Tabel 14. Pengendalian Risiko

ID	Prioritas	Pengendalian
R1.1	Sangat Tinggi	Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.
R2.5	Sangat Tinggi	Keamanan informasi harus diterapkan ke dalam manajemen proyek, tanpa memperhatikan tipe proyeknya.
R2.7	Sangat Tinggi	Kebijakan dan tindakan keamanan yang mendukung harus diadopsi untuk mengelola risiko yang terjadi akibat dari penggunaan perangkat bergerak.
R3.1	Sangat Tinggi	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.
R3.2	Sangat Tinggi	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.
R4.2	Sangat Tinggi	Aset yang dipelihara dalam inventaris harus dimiliki (ada personil yang bertanggung jawab).
R4.3	Sangat Tinggi	Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi, dokumentasi dan diimplementasikan.

ID	Prioritas	Pengendalian
R4.4	Sangat Tinggi	Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.
R4.5	Sangat Tinggi	Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.
R4.6	Sangat Tinggi	Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
R4.7	Sangat Tinggi	Prosedur penanganan aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi organisasi.
R4.8	Sangat Tinggi	Prosedur harus diimplementasikan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi.
R4.9	Sangat Tinggi	Media harus dihancurkan dengan aman saat tidak lagi dibutuhkan, dengan menggunakan prosedur baku.
R2.1	Tinggi	Semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan.
R2.2	Tinggi	Tugas dan area tanggung jawab yang bertentangan harus dipisahkan (dijabat oleh personel yang berbeda) untuk mengurangi kemungkinan dari modifikasi yang tidak sah atau tidak sengaja atau penyalahgunaan aset organisasi.
R2.3	Tinggi	Hubungan baik dengan pihak berwenang terkait harus dipelihara.
R2.4	Tinggi	Hubungan baik dengan komunitas, forum, dan asosiasi profesional spesialis keamanan harus dipelihara.
R2.6	Tinggi	Kebijakan dan tindakan keamanan yang mendukung harus diadopsi untuk mengelola risiko yang terjadi akibat dari penggunaan perangkat bergerak.
R3.3	Tinggi	Manajemen harus mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan.
R3.4	Tinggi	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.
R3.5	Tinggi	Harus ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi.
R3.6	Tinggi	Setelah penghentian atau perubahan kepegawaian, tugas dan tanggung jawab keamanan informasi yang masih berlaku harus ditetapkan, dikomunikasikan kepada pegawai atau kontraktor, dan ditegakkan.
R4.1	Tinggi	Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan inventaris dari aset-aset ini harus dicatat dan dipelihara.

5. Kesimpulan

Jumlah prioritas risiko keamanan informasi yang ditemukan dengan metode *fuzzy* FMEA yaitu 13 risiko sangat tinggi dan 10 risiko tinggi. Oleh karena, itu Dinas Kependudukan XYZ harus memperbaiki segera risiko-risiko keamanan informasi berdasarkan ISO/IEC 27001:2013 sehingga dapat meminimalisir risiko keamanan informasi. Evaluasi Keamanan Sistem Informasi Menggunakan *Fuzzy* FMEA Berbasis Framework ISO/IEC 27001:2013 terbukti dapat menjadi acuan untuk meningkatkan keamanan informasi sehingga tujuan organisasi dapat tercapai.

Saran bagi penelitian selanjutnya metode FMEA dan *fuzzy* FMEA yang digunakan dalam penelitian ini dapat dikombinasikan dengan metode lainnya, misalnya *Fault Tree Analysis*, agar didapatkan hasil analisis yang lebih komprehensif.

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)*. https://doi.org/10.1109/IWBIS.2018.8471700

Ardyansyah, H.R., Handayani, N.U., 2023. Analisis Pengendalian Kualitas Produk Kain Grey PS 946 dalam Upaya Mengurangi Tingkat Kecacatan Produk Menggunakan Metode Failure Mode and Effect Analysis (FMEA) dan Pendekatan Kaizen (Studi Kasus Pt. Primissima). *Industrial Engineering Online Journal*, 12(3).

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

Calache, L.D.D.R., Zanon, L.G., Arantes, R.F.M, Osiro, L., Carpinetti, L.C.R., 2021. Risk Prioritization Based on the Combination of Fmea and Dual Hesitant Fuzzy Sets Method. *Production*, 31, 1–16. https://doi.org/10.1590/0103-6513.20200081

Carvalho, C., Marques, E., 2019. Adapting Iso 27001 To A Public Institution. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*. 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

Desy, I., Hidayanto, B.C., Astuti, H.M., 2014. Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effects

Analysis di Divisi TI Pt . Bank XYZ Surabaya. *Seminar Nasional Sistem Informasi Indonesia (Sesindo)*, 2014, 467-472.

Fathurohman, A., Witjaksono, R.W., 2020. Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using Annex Control (Case Study: District of Government of Bandung City). *Computer Science and Electrical Engineering*, 1(1), 1-11. https://doi.org/10.25008/bcsee.v1i1.2

Filz, M.A., Langner, J.E.B., Herrmann, C., Thiede, S., 2021. Data-Driven Failure Mode and Effect Analysis (FMEA) to Enhance Maintenance Planning. *Computers In Industry*, 129. 103451. https://doi.org/10.1016/j.compind.2021.103451

Handayani, N.U., Wibowo, M.A., Sari, D.P., Satria, Y., Gifari, A.R., 2018. Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect and Analysis Berbasis Framework Iso 27001. *Teknik*, 39(2), 78-85. https://doi.org/10.14710/teknik.v39i2.15918

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

Kang, D., Shao, Y., Yin, X., Xiao, J., Rao, T., Shen, B., Chen, H., Zhu, Z., Wang, G., Liang, Y., 2017. Bioanalytical Assay Development and Validation for Simultaneous Quantification of Five Schisandra Lignans in Rat Primary Hepatocytes Based on Lc-Ms/Ms: Application to a Real-Time Uptake Study for Schisandra Lignan Extract. *Biomedical Chromatography*, 31(2). https://doi.org/10.1002/bmc.3797

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: Jurnal Ilmiah Sistem Informasi* 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), 171–90. https://doi.org/10.4186/ej.2019.23.1.171

Nugraha, B.A., Perdanakusuma, A.R., Rachmadi, A., 2020. Analisa Manajemen Risiko Pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. *JPTIIK*, 4(1):223-231.

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

Nurul, S., Anggrainy, S., Aprelyani, S., 2022. Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi (JEMSI)*, 3(5), 564-573. https://doi.org/10.38035/jemsi.v3i5.992

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

Sulistyowati, I., Ginardi, R.V.H., 2019. Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University). *Iptek Journal of Proceedings Series*, 1. http://dx.doi.org/10.12962/j23546026.y2019i1.5103

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

Syreyshchikova, N.V., Pimenov, D.Y., Mikolajczyk, T., Moldovan, L., 2019. Information Safety Process Development According To ISO 27001 for an Industrial Enterprise. *Procedia Manufacturing*, 32, 278-285. https://doi.org/10.1016/j.promfg.2019.02.215

Yaqin, R.I., Zamri, Siahaan, J.P., Priharanto, Y.E., Alirejo, M.S., Umar, M.L., 2020. Pendekatan FMEA dalam Analisa Risiko Perawatan Sistem Bahan Bakar Mesin Induk: Studi Kasus di KM. Sidomulyo. *Jurnal Rekayasa Sistem Industri*, 9(3), 189-200. https://doi.org/10.26593/jrsi.v9i3.4075.189-200

Yoseviano, H.F., Retnowardhani, A., 2018. The Use Of ISO/IEC 27001: 2009 To Analyze The Risk And Security Of Information System Assets: Case Study In XYZ, Ltd. *2018 International Conference on Information Management and Technology (ICIMTech)*, 21-26. https://doi.org/10.1109/ICIMTech.2018.8528096

Yusnanto, T., Mustofa, K., Mahmudi, M.A., Wahyudiono, S., 2021. Fenomena Keamanan Informasi Pasca Era Revolusi Industri 5.0. *Jurnal Transformasi*, 17(2), 24-35.