ANALISIS KEAMANAN SISTEM INFORMASI PELAYANAN PELANGGAN MENGGUNAKAN PENDEKATAN FMEA DAN ISO/IEC 27001:2013 PADA PT PLN UP3 GRESIK

Navy Nurlyn Ajrina[1*], Putri Intan Octavia Br. Sipayung[2], Yuliani Purwitasari[3], Hellawati Ayu Rizmadita[4], Agung Brastama Putra[5], Anita Wulansari[6]

[1-6] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Indonesia

E-mail: 22082010158@student.upnjatim.ac.id[1*], 22082010159@student.upnjatim.ac.id[2], 22082010168@student.upnjatim.ac.id[3], 22082010208@student.upnjatim.ac.id[4], agungbp.si@upnjatim.ac.id[5], anita.wulansari.sisfo@upnjatim.ac.id[6]

ABSTRACT

This study aims to analyze and mitigate information security risks in the customer service information system at PT PLN UP3 Gresik using the Failure Mode and Effects Analysis (FMEA) approach combined with security controls from the ISO/IEC 27001: 2013 Annex A standard. A total of 33 potential risks were identified and evaluated based on the Risk Priority Number (RPN) value, which is calculated from severity, likelihood, and detectability. Risks categorized as Very High (RPN ≥ 200), such as hardware failure, weak password policies, and network security system weaknesses, were addressed through risk avoidance strategies, with reference to controls A.8.1.1, A.9.2.4, and A.10.1.1. Risks with High category (RPN 151-200), such as Stored XSS and SQL Injection, are handled through risk reduction or risk transfer strategies, referring to controls A.14.2.8, A.12.6.1, and A.14.2.5. Risks with Medium to Low categories are handled through risk reduction and risk acceptance strategies by considering relevant ISO controls. The results show that the integration of the FMEA method with ISO/IEC 27001:2013 can provide a systematic, standardized, and adaptive risk mitigation approach to information system conditions. This approach is expected to strengthen information security resilience and improve the reliability of digital customer services at PT PLN UP3 Gresik.

Keywords: Information Security, FMEA, ISO/IEC 27001:2013, RPN, Risk Mitigation, Customer Information System.

ABSTRAK

Penelitian ini bertujuan untuk menganalisis dan memitigasi risiko keamanan informasi pada sistem informasi layanan pelanggan di PT PLN UP3 Gresik dengan menggunakan pendekatan Failure Mode and Effects Analysis (FMEA) yang dikombinasikan dengan kontrol keamanan dari standar ISO/IEC 27001:2013 Annex A. Sebanyak 33 potensi risiko berhasil diidentifikasi dan dievaluasi berdasarkan nilai Risk Priority Number (RPN), yang dihitung dari tingkat

Article History
Received: Juni 2025
Reviewed: Juni 2025
Published: Juni 2025

Plagiarism Checker No 235
Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

keparahan, kemungkinan, dan kemampuan deteksi. Risiko-risiko dengan kategori Very High (RPN ≥ 200), seperti kegagalan perangkat keras, kebijakan kata sandi yang lemah, dan kelemahan sistem keamanan jaringan, ditangani melalui strategi risk avoidance, dengan mengacu pada kontrol A.8.1.1, A.9.2.4, dan A.10.1.1. Risiko dengan kategori High (RPN 151–200), seperti Stored XSS dan SQL Injection, ditangani melalui strategi risk reduction atau risk transfer, mengacu pada kontrol A.14.2.8, A.12.6.1, dan A.14.2.5. Risiko dengan kategori Medium hingga Low ditangani melalui strategi risk reduction dan risk acceptance dengan mempertimbangkan kontrol ISO yang relevan. Hasil penelitian menunjukkan bahwa integrasi metode FMEA dengan ISO/IEC 27001:2013 dapat memberikan pendekatan mitigasi risiko yang sistematis, terstandarisasi, dan adaptif terhadap kondisi sistem informasi. Pendekatan ini diharapkan dapat memperkuat ketahanan keamanan informasi dan meningkatkan keandalan layanan pelanggan digital di PT PLN UP3 Gresik.

Kata Kunci: Keamanan Informasi, FMEA, ISO/IEC 27001:2013, RPN, Mitigasi Risiko, Sistem Informasi Pelayanan Pelanggan.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital di berbagai sektor, termasuk layanan publik (Natika, 2024). Organisasi kini sangat bergantung pada sistem informasi untuk menunjang operasional dan pelayanan kepada masyarakat. Namun, di balik kemajuan tersebut, informasi menjadi sangat mudah diakses dan dibagikan, sehingga menjadikannya sebagai aset yang bernilai tinggi bagi individu maupun perusahaan (Nurul, Anggrainy, & Aprelyani, 2022). Pertumbuhan digital yang pesat ini turut disertai dengan peningkatan ancaman terhadap keamanan siber secara signifikan (Daeng et al., 2023). Oleh karena itu, isu keamanan informasi menjadi sangat vital dan tidak dapat diabaikan.

Keamanan informasi merupakan upaya sistematis untuk melindungi informasi dari akses, penggunaan, pengungkapan, perubahan, gangguan, pemeriksaan, pencatatan, atau perusakan yang tidak memiliki otorisasi. Informasi tersebut bisa berwujud fisik maupun digital. Tujuan utama dari keamanan informasi adalah menjaga aspek kerahasiaan, keutuhan, dan ketersediaan data, baik yang tersimpan dalam sistem elektronik maupun dalam bentuk dokumen fisik (Aurabillah, Putri, Fadhlilla, & Wulansari, 2024).

Sektor pelayanan publik menyimpan dan mengelola data dalam jumlah besar, termasuk data pelanggan yang bersifat pribadi. PT PLN (Persero) sebagai penyedia utama layanan kelistrikan di Indonesia memiliki tanggung jawab besar dalam menjaga integritas, kerahasiaan, dan ketersediaan data tersebut. Kegagalan dalam mengamankan sistem informasi dapat menyebabkan gangguan layanan, penurunan kepercayaan publik, bahkan konsekuensi hukum (Iswandari, 2021).

PT PLN (Persero) UP3 Gresik merupakan unit pelaksana yang bertugas menyediakan dan mendistribusikan listrik di wilayah Gresik dan sekitarnya. Dalam pelaksanaan tugasnya, PLN UP3 Gresik memanfaatkan teknologi digital termasuk penggunaan website sebagai media layanan

bagi pelanggan. Website ini digunakan untuk melakukan catat meter, mengirimkan tagihan kepada pelanggan, serta mencatat perpanjangan layanan. Namun demikian, sistem digital tersebut tidak terlepas dari potensi risiko, baik dari aspek teknis, aspek manusia (user error), maupun aspek prosedural (ketidaksesuaian SOP dengan kebutuhan keamanan).

Untuk memastikan bahwa sistem informasi pelayanan pelanggan aman, diperlukan kerangka kerja yang terstandarisasi dan terbukti secara internasional. Standar ISO/IEC 27002:2013 merupakan pedoman atau kode praktik untuk penerapan standar keamanan informasi di suatu organisasi serta praktik manajemen keamanan informasi (Musyarofah & Bisma, 2020).

Dalam rangka menjamin keamanan sistem informasi, diperlukan pendekatan evaluasi yang sistematis serta mengacu pada standar yang diakui. ISO/IEC 27001:2013 berperan sebagai standar internasional yang menyediakan kerangka kerja untuk merancang, mengimplementasikan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI). ISO/IEC 27001:2013 menetapkan seperangkat kontrol dan ketentuan yang harus dipenuhi dalam proses perancangan, penerapan, pengoperasian, pemantauan, peninjauan, pemeliharaan, dan peningkatan sistem manajemen keamanan informasi (Musyarofah & Bisma, 2021). Oleh karena itu, penerapan standar ini membantu organisasi dalam mengelola risiko keamanan informasi secara terencana dan efektif.

Sebagai pelengkap dari pendekatan berbasis standar tersebut, metode *Failure Mode and Effect Analysis* (FMEA) digunakan untuk menganalisis kemungkinan kegagalan dalam sistem informasi. FMEA adalah metode sistematis untuk mengidentifikasi dan mencegah masalah pada sistem, produk, dan proses sebelum masalah tersebut terjadi. Metode ini berfokus pada pencegahan masalah, peningkatan keselamatan, dan peningkatan kepuasan pelanggan (Sharma & Srivastava, 2018). Dalam penerapannya, FMEA memberikan penilaian terhadap tingkat keparahan dampak (*severity*), kemungkinan terjadinya (occurrence), dan kemampuan sistem dalam mendeteksi kegagalan (*detection*), yang kemudian menghasilkan nilai *Risk Priority Number* (RPN) (Situngkir, 2019). Nilai ini membantu organisasi dalam memprioritaskan risiko mana yang harus segera dimitigasi. Kelebihan dari pendekatan FMEA adalah kemampuannya memberikan panduan teknis dan kuantitatif dalam menilai potensi risiko yang berasal dari perangkat lunak, perangkat keras, prosedur operasional, maupun sumber daya manusia.

Meskipun isu keamanan informasi semakin krusial, penelitian yang secara spesifik menganalisis keamanan sistem informasi website pelayanan publik di lingkungan PLN, khususnya dengan pendekatan kombinatif antara FMEA dan ISO 27001, masih terbatas. Oleh karena itu, kajian ini diharapkan dapat memberikan kontribusi praktis dan akademis dalam memperkuat perlindungan informasi di sektor pelayanan publik, sekaligus mendukung peningkatan kualitas layanan digital PT PLN UP3 Gresik.

2. METODE PENELITIAN

2.1 Identifikasi Permasalahan, Tujuan & Manfaat

Pada tahap ini dilakukan proses untuk mengidentifikasi permasalahan yang terjadi dalam penggunaan website layanan pelanggan PT PLN UP3 Gresik. Tahap ini juga mencakup penentuan tujuan penelitian dan manfaat yang diharapkan, baik secara teoritis maupun praktis.

2.2 Studi Literatur

Tahap ini mencakup pencarian landasan teori yang relevan dengan mengacu pada sumber-sumber seperti buku, jurnal, dan laporan penelitian yang berkaitan dengan analisis dan manajemen risiko, keamanan informasi, teknologi informasi, metode *Failure Mode and Effects Analysis* (FMEA), serta kontrol ISO/IEC 27001:2013.

2.3 Pengumpulan Data dan Informasi

Tahap ini mencakup proses pengumpulan data dan informasi yang dilakukan melalui observasi langsung, wawancara dengan pihak terkait, serta penelaahan dokumen yang relevan. Pengambilan data menggunakan pendekatan deskriptif kuantitatif guna menjawab pertanyaan penelitian yang berkaitan dengan penggunaan *website* layanan pelanggan PT PLN UP3 Gresik terjadi. Pendekatan ini menitikberatkan pada pengumpulan informasi yang mendalam dengan tujuan untuk mengidentifikasi pola-pola tertentu yang muncul dalam penggunaan dan interaksi terhadap sistem layanan pelanggan tersebut (Kim, Sefcik, & Bradway, 2017).

2.4 Analisis Metode FMEA

Tahap 1 - Analisis Proses Bisnis Sistem

Langkah pertama yang dilakukan dalam analisis FMEA adalah membuat dan mempelajari alur proses bisnis organisasi maupun sistem menggunakan *Business Process Model and Notation* (BPMN). Analisis BPMN dilakukan terhadap sistem layanan pelanggan PT PLN UP3 Gresik.

Tahap 2 – Brainstorming Risiko Potensial

Pada tahap ini, dilakukan diskusi bersama para pemangku kepentingan untuk mengidentifikasi berbagai potensi risiko yang mungkin terjadi, seperti ancaman, kerentanan, dan dampak terhadap keamanan informasi dalam penggunaan website layanan pelanggan PT PLN UP3 Gresik.

Tahap 3 – Menentukan Nilai Risiko Berdasarkan Severity, Occurrence, Detection dan Hasil RPN

Risiko-risiko yang telah diidentifikasi kemudian dianalisis lebih lanjut dengan menilai tiga parameter utama, yaitu tingkat keparahan dampak (*Severity*), kemungkinan terjadinya risiko (*Occurrence*), dan tingkat kemampuan deteksi (*Detection*). Hasil dari ketiga nilai ini digunakan untuk menghitung Risk Priority Number (RPN), yang menjadi dasar dalam menentukan prioritas mitigasi terhadap setiap potensi kegagalan dalam sistem.

Tabel 1. Skala Severity (Tingkat Keparahan)

Dampak	Kriteria	Peringkat
Berbahaya: Tanpa Peringatan	Mengakibatkan proses organisasi dan layanan pelanggan berhenti > 1 minggu	10
Berbahaya: Dengan Peringatan	Mengakibatkan proses organisasi dan layanan pelanggan berhenti > 1 hari	9
Sangat Tinggi	Mengakibatkan proses organisasi dan layanan pelanggan berhenti dalam 1 hari	8
Tinggi	Mengakibatkan proses organisasi dan layanan pelanggan berhenti < 1 hari	7
Sedang	Menyebabkan layanan pelanggan gagal berfungsi sebagaimana mestinya	6
Rendah	Menimbulkan komplain dari pelanggan	5
Sangat Rendah	Menimbulkan gangguan yang cukup berpengaruh/menyebabkan sedikit kerugian	4

Sedikit	Menyebabkan sedikit terjadinya gangguan maupun tanpa adanya kehilangan sesuatu.	3
Sangat Sedikit	Tanpa disadari dan memberikan dampak kecil pada kinerja	2
Tidak Ada	Tanpa disadari dan tidak mempengaruhi kinerja	1

Tabel 2. Skala Occurrence (Tingkat Kejadian)

Probabilitas Resiko	Periode	Peringkat
Sangat Tinggi	Lebih dari satu kali tiap harinya	10
Tinggi: Gagal hampir pasti terjadi	Satu kali dalam 4 hari	9
Tinggi: Umumnya muncul pada proses yang historisnya sering bermasalah	Satu kali dalam seminggu	8
Proses yang sering kali gagal	Satu kali dalam sebulan	7
Moderate	Satu kali setiap 3 bulan	6
Pernah gagal, namun tidak terlalu sering	Satu kali setiap 6 bulan	5
Kegagalan yang pernah terjadi, tapi tidak dalam proporsi yang besar	Satu kali dalam setahun	4
Rendah	Satu kali dalam 1-3 tahun	3
Sangat Rendah	Satu kali dalam 3-6 tahun	2
Kegagalan tidak mungkin terjadi	Satu kali dalam 6 tahun lebih	1

Tabel 3. Skala Detectability (Tingkat Deteksi)

Dampak	Kriteria	Peringkat
Hampir Tidak Mungkin	Potensi penyebab tidak dapat diidentifikasi.	10
Sangat Sulit	Sangat sulit untuk mendeteksi risiko.	9
Sulit	Sulit terdeteksi atau sulit terkontrol.	8
Cukup Sulit	Cukup sulit untuk dideteksi	7
Normal	Bisa dideteksi dengan usaha ekstra.	6
Sedang / Moderat	Dapat dideteksi.	5
Cukup Mudah	Cukup mudah untuk dideteksi	4
Mudah	Mudah untuk dideteksi	3
Sangat Mudah	Sangat mudah untuk dideteksi.	2
Hampir Pasti	Terlihat jelas, sangat mudah pengendaliannya.	1

Tabel 4. Tabel Skala RPN

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

2.5 Mitigasi Risiko dengan Kontrol ISO 27001:2013

Tahap selanjutnya adalah melakukan mitigasi terhadap risiko-risiko yang memiliki nilai RPN tinggi dengan mengacu pada kontrol keamanan informasi yang terdapat dalam standar ISO/IEC 27001:2013. Standar ini menyediakan kontrol terstruktur yang mencakup aspek teknis, prosedural, dan kebijakan, guna memperkuat sistem keamanan informasi pada layanan pelanggan berbasis *website*.Dengan mengimplementasikan mekanisme keamanan informasi

yang tepat, organisasi mampu memitigasi risiko yang berkaitan dengan ancaman siber dan berbagai insiden keamanan lainnya (Aurabillah, Putri, Fadhlilla, & Wulansari, 2024).

2.6 Rekomendasi Mitigasi Risiko

Berdasarkan hasil analisis risiko dan referensi kontrol dari ISO 27001, disusun rekomendasi mitigasi yang sesuai dengan kondisi dan kebutuhan operasional PT PLN UP3 Gresik. Rekomendasi ini mencakup tindakan preventif, teknis, dan prosedural yang dapat diterapkan untuk menurunkan potensi ancaman dan memperkuat ketahanan sistem informasi layanan pelanggan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Bab ini menyajikan hasil dari proses analisis keamanan sistem informasi pada website layanan pelanggan PT PLN UP3 Gresik. Analisis dilakukan dengan menggunakan pendekatan Failure Mode and Effects Analysis (FMEA) untuk mengidentifikasi, mengevaluasi, dan memprioritaskan potensi risiko yang mungkin terjadi dalam sistem.

Berdasarkan hasil identifikasi dan penilaian risiko menggunakan metode FMEA, diperoleh 33 potensi risiko terhadap sistem informasi pelayanan pelanggan di PT PLN UP3 Gresik. Risiko tersebut dikelompokkan ke dalam enam kategori aset, yaitu *Hardware, Software, People, Network,* dan Data. Berikut adalah hasil analisis risiko menggunakan metode FMEA.

Tabel 5. Hasil Penilaian Risiko

Kategori	Risiko	Potential Cause	Kode	Sev	Occ	Dec	RPN	Level Risiko
Hardware	Hardware Failure	Jadwal maintenance hardware tidak teratur	H1	8	7	6	336	*Very High*
	Server down	Listrik tidak stabil	H3	6	2	3	36	*Very Low*
		Penggunaan melebihi kemampuan server	H4	6	4	5	120	*Medium*
	Server dapat diakses oleh pihak tidak berwenang	Kurangnya keamanan pada akses server	H5	7	3	5	105	*Medium*
	Tidak ada akses fisik yang terotorisasi	Lemahnya keamanan dan kurangnya penggunaan CCTV	H6	8	2	2	32	*Very Low*
Software	Terjadi kesalahan pada software	Bug atau kesalahan dalam penulisan kode program	S1	6	4	5	210	*Very High*
	Terjadi kesalahan pada software	Kesalahan Konfigurasi sistem	S2	7	5	5	175	*High*
	Sistem Layanan Pelanggan tidak bisa diakses	Serangan Dos	S3	6	2	6	72	*Low*
	Pencurian Data	Lemahnya keamanan dan perlindungan data	S4	7	2	7	98	*Low*
	Bocornya informasi kepada pihak yang tidak berwenang	SQL injection	S5	7	4	6	168	*High*
	Pengguna tidak sah dapat melihat atau memodifikasi akun pelanggan lain	Kontrol akses yang lemah (Broken Access Control)	S6	6	3	5	90	*Low*
	Pengguna tak terverifikasi dapat mengakses area terbatas atau	Penyimpanan kata sandi dalam bentuk teks biasa (Plain Text Password Storage)	S7	5	2	4	40	*Very Low*

	meningkatkan hak aksesnya							
	Peretas bisa mengakses database melalui kredensial yang mudah ditebak	Kebijakan kata sandi yang lemah (Weak Password Policy)	S8	8	4	8	256	*Very High*
	Pencurian cookie pengguna atau tampilan situs yang dirusak (defacement)	Serangan Cross-Site Scripting (Stored XSS)	S9	6	4	7	196	*High*
	Kebocoran atau pencurian data	Serangan virus atau malware	S10	8	4	4	128	*Medium*
	Sistem rentan terhadap berbagai jenis serangan	Kurangnya proteksi keamanan perangkat lunak	S11	6	2	5	60	*Low*
People	Penyalahgunaan akses yang dapat mengganggu keamanan sistem	Akun digunakan bersama (shared login)	P1	6	4	5	120	*Medium*
	Kesalahan teknis oleh staf atau teknisi	Kurangnya pelatihan terkait prosedur penggunaan sistem TI	P2	6	3	4	72	*Low*
	Hilangnya data penting atau kesalahan pencatatan data	Ketidaktelitian saat input atau penghapusan data	P3	6	4	5	120	*Medium*
	Potensi akses tidak sah oleh pihak lain saat workstation dibiarkan terbuka	Staf meninggalkan komputer tanpa logout	P4	6	3	4	72	*Low*
	Potensi modifikasi data atau pencurian isi basis data	Pengolahan data tanpa izin oleh karyawan	P5	7	4	5	140	*Medium*
	Potensi pencurian media penyimpanan atau informasi penting perusahaan	Kurangnya mekanisme pengawasan terhadap aktivitas karyawan	P6	7	4	5	140	*Medium*
Network	Rentan terhadap serangan siber seperti peretasan	Sistem keamanan jaringan internal yang lemah	N1	9	5	5	225	*Very High*
	Hilangnya koneksi internet yang mengganggu operasional layanan	Gangguan pada koneksi LAN	N2	7	4	4	112	*Medium*
	Kegagalan jaringan yang menyebabkan sistem tidak dapat beroperasi	Kerusakan fisik atau gangguan teknis pada infrastruktur jaringan	N3	8	4	4	128	*Medium*
	Ancaman tersembunyi yang tidak terdeteksi seperti pencurian data atau koneksi ilegal	Tidak adanya sistem monitoring jaringan	N4	8	5	4	160	*High*
	Konektivitas terganggu dan pengguna kesulitan mengakses sistem	Kesalahan konfigurasi pada access point	N5	6	3	4	72	*Low*
	Gangguan fisik yang menyebabkan jaringan terputus total	Kabel jaringan rusak karena digigit hewan	N6	6	3	3	54	*Low*
	Perangkat jaringan menjadi tidak dapat digunakan	Terputusnya koneksi jaringan	N7	6	3	3	54	*Low*
Data	Penyalahgunaan hak akses terhadap data	Akses data oleh pihak yang tidak berwenang	D1	8	4	5	160	*High*
	Kerusakan atau error pada data (data corrupt)	Gangguan daya listrik	D2	6	3	4	72	*Low*

	Kehilangan data penting karena kegagalan proses backup	Tidak adanya mekanisme pencadangan data	D3	7	4	4	112	*Medium*
	Kehilangan atau ketidaktepatan data dalam sistem	Kesalahan input atau penghapusan data secara tidak sengaja	D4	6	3	4	72	*Low*

Setelah proses perhitungan FMEA dan penentuan level risiko selesai dilakukan, langkah selanjutnya adalah mengurutkan risiko berdasarkan nilai Risk Priority Number (RPN). Pengurutan ini bertujuan untuk mengetahui peringkat risiko secara sistematis, sehingga dapat diidentifikasi jenis aset atau permasalahan dengan tingkat risiko High & Very High. Risiko-risiko prioritas tersebut kemudian dijadikan dasar dalam pemberian rekomendasi penanganan yang merujuk pada kontrol keamanan informasi ISO/IEC 27001:2013, mengingat urgensi penanganannya terhadap kelangsungan operasional perusahaan, khususnya pada departemen teknologi informasi.

Tabel 5. Urutan Nilai RPN dan Level Risiko

Risiko	Potential Failure	Jenis Aset	Kode	RPN	Level Risiko	Perlakuan Risiko
Hardware Failure	Jadwal maintenance hardware tidak teratur	Hardware	H1	336	*Very High*	*Risk Avoidance*
Peretas bisa mengakses database melalui kredensial yang mudah ditebak	Kebijakan kata sandi yang lemah (Weak Password Policy)	Software	S8	256	*Very High*	*Risk Avoidance*
Terjadi serangan siber seperti peretasan	Sistem keamanan jaringan internal yang lemah	Network	N1	225	*Very High*	*Risk Avoidance*
Terjadi kesalahan pada software	Bug atau kesalahan dalam penulisan kode program	Software	S1	210	*Very High*	*Risk Avoidance*
Pencurian cookie pengguna atau tampilan situs yang dirusak (defacement)	Serangan Cross-Site Scripting (Stored XSS)	Software	S9	196	*High*	*Risk Transfer*
	Kesalahan Konfigurasi sistem	Software	S2	175	*High*	*Risk Transfer*
Bocornya informasi kepada pihak yang tidak berwenang	SQL injection	Software	S5	168	*High*	*Risk Transfer*
Pencurian Data	Tidak adanya sistem monitoring jaringan	Network	N4	160	*High*	*Risk Transfer*
Penyalahgunaan hak akses terhadap data	Akses data oleh pihak yang tidak berwenang atau perubahan tidak sah	Data	D1	160	*High*	*Risk Transfer*
Potensi pencurian media penyimpanan atau informasi penting perusahaan	Kurangnya mekanisme pengawasan terhadap aktivitas karyawan	People	P6	140	*Medium*	*Risk Reduction*
Potensi modifikasi data atau pencurian isi basis data	Pengolahan data tanpa izin oleh karyawan	People	P5	140	*Medium*	*Risk Reduction*

Kebocoran atau pencurian data	Serangan virus atau malware	Software	S10	128	*Medium*	*Risk Reduction*
Kegagalan jaringan yang menyebabkan sistem tidak dapat beroperasi	Gangguan teknis/kerusakan infrastruktur jaringan	Network	N3	128	*Medium*	*Risk Reduction*
Hilangnya data penting atau kesalahan pencatatan data	Ketidaktelitian saat input atau penghapusan data	People	P3	120	*Medium*	*Risk Reduction*
Penyalahgunaan akses yang dapat mengganggu keamanan sistem	Akun digunakan bersama	People	P1	120	*Medium*	*Risk Reduction*
Server Down	Penggunaan melebihi kemampuan server	Hardware	H4	120	*Medium*	*Risk Reduction*
Kehilangan data penting karena kegagalan proses backup	Tidak adanya mekanisme pencadangan data	Data	D3	112	*Medium*	*Risk Reduction*
Hilangnya koneksi internet yang mengganggu operasional layanan	Gangguan pada koneksi LAN	Network	N2	112	*Medium*	*Risk Reduction*
Server dapat diakses oleh pihak tidak berwenang	Server dapat diakses oleh pihak tidak berwenang	Hardware	H5	105	*Medium*	*Risk Reduction*
Pencurian Data	Lemahnya perlindungan data	Software	S4	98	*Low*	*Risk Acceptance*
Pengguna tidak sah dapat melihat atau memodifikasi akun pelanggan lain	Kontrol akses lemah	Software	S6	90	*Low*	*Risk Acceptance*
Kehilangan atau ketidaktepatan data dalam sistem	Kesalahan input atau penghapusan data	Data	D4	72	*Low*	*Risk Acceptance*
Kesalahan teknis oleh staf atau teknisi	Kurangnya pelatihan teknis	People	P2	72	*Low*	*Risk Acceptance*
Potensi akses tidak sah oleh pihak lain saat workstation dibiarkan terbuka	Komputer dibiarkan terbuka	People	P4	72	*Low*	*Risk Acceptance*
Sistem Layanan Pelanggan tidak bisa diakses	Serangan DoS	Software	S3	72	*Low*	*Risk Acceptance*
Kerusakan atau error pada data (data corrupt)	Gangguan daya listrik menyebabkan kerusakan data	Data	D2	72	*Low*	*Risk Acceptance*
Konektivitas terganggu dan pengguna kesulitan mengakses sistem	Kesalahan konfigurasi pada access point	Network	N5	72	*Low*	*Risk Acceptance*
Sistem rentan terhadap berbagai jenis serangan	Kurangnya proteksi keamanan perangkat lunak	Software	S11	60	*Low*	*Risk Acceptance*

Perangkat jaringan menjadi tidak dapat digunakan	Terputusnya koneksi jaringan	Network	N7	54	*Low*	*Risk Acceptance*
Gangguan fisik yang menyebabkan jaringan terputus total	Kabel jaringan rusak karena digigit hewan	Network	N6	54	*Low*	*Risk Acceptance*
Pengguna tak terverifikasi dapat mengakses area terbatas atau meningkatkan hak aksesnya	Penyimpanan kata sandi dalam bentuk teks biasa (Plain Text Password Storage)	Software	S7	40	*Very Low*	*Risk Acceptance*
Server down	Listrik tidak stabil	Hardware	H3	36	*Very Low*	*Risk Acceptance*
Tidak ada akses fisik yang terotorisasi	Lemahnya keamanan fisik dan tidak ada CCTV	Hardware	H6	32	*Very Low*	*Risk Acceptance*

Setelah analisis FMEA dilakukan, risiko yang telah diidentifikasi dipetakan ke dalam matriks berdasarkan tingkat keparahan dan kemungkinan kejadiannya. Matriks ini mempermudah visualisasi prioritas risiko, sehingga dapat ditentukan langkah mitigasi yang tepat. Tabel 6 berikut menyajikan hasil pemetaan tersebut.

Tabel 6. Matrik Level

		Occurrence/Kemungkinan				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Saverity / Dampak	Vey High			N1		H1
	High	S5, S4, H6	S9, N4, D1, P6, P5, S10, N3, D3, N2, H5	S2	S8	
	Medium	S3, S11, S7, H3	P3, P1, H4, S6, D4, P2, P4, D2, N5, N7, N6		S1	
	Low					
	Very Low					

Berdasarkan pemetaan risiko pada Tabel 6, langkah mitigasi selanjutnya disusun dengan merujuk pada kontrol keamanan informasi ISO/IEC 27001:2013. Rekomendasi mitigasi ini difokuskan pada risiko dengan tingkat prioritas tinggi (*high*) hingga sangat tinggi (*very high*).

Tabel 7. Rekomendasi Mitigasi Risiko

Potential Failure Mode	**Rekomendasi Mitigasi berdasarkan ISO 27001:2013**	
	Kontrol ISO (Annex A)	**Rekomendasi**
Hardware failure	A.8.1.1 Tanggung Jawab terhadap Aset	A.8.1.1 (Inventaris aset): Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan diinventaris dari aset-aset ini harus dicatat dan dipelihara.

	A.11.1.4 Perlindungan terhadap Ancaman Eksternal & Lingkungan	A.11.1.4 (Melindungi terhadap ancaman eksternal dan lingkungan): Pastikan server ditempatkan di ruang aman dengan perlindungan terhadap gangguan listrik dan bencana.
Kebijakan Kata Sandi Lemah (Weak Password Policy)	A.9.4.3 Password Management System A.9.2.4 Secret Authentication Information Management	A.9.4.3 (Manajemen Password): Perusahaan/Organisasi harus memastikan penggunaan sistem manajemen kata sandi yang aman. A.9.2.4 (Informasi Autentikasi): Kebijakan harus mencakup mekanisme autentikasi yang aman seperti penggunaan multi-factor authentication (MFA).
Sistem Keamanan Jaringan Lemah	A.10.1.1 Network Controls Jaringan A.13.1.1 Protection of Information in Transit	A.10.1.1 (Keamanan jaringan): Jaringan harus dikontrol dan dilindungi dari akses tidak sah melalui firewall, IDS/IPS, dan segmentasi jaringan. A.13.1.1 (Perlindungan informasi dalam transit): Pastikan data dalam proses komunikasi jaringan aman melalui enkripsi dan kontrol akses.
Bug atau Kesalahan Kode Program	A.14.2.1 Secure Development Policy A.14.2.5 System Security Testing	A.14.2.1 (Kebijakan Pengembangan Sistem) : Diperlukan prosedur pengujian dan verifikasi kode secara berkala. A.14.2.5 (Uji keamanan sistem): Setiap pembaruan atau perubahan sistem harus melalui tahapan uji keamanan yang sistematis. Gunakan tool CI/CD dengan uji keamanan otomatis.
Serangan Cross-Site Scripting (Stored XSS)	A.14.2.8 Secure Coding Practices A.12.6.1 Technical Vulnerability Management	A.14.2.8 (Perlindungan terhadap kerentanan teknis): Pengembang harus menghindari kerentanan melalui validasi input dan penggunaan framework yang aman. Hindari penggunaan innerHTML tanpa sanitasi. A.12.6.1 (Pengelolaan kerentanan teknis): Harus ada mekanisme identifikasi, penilaian, dan mitigasi kerentanan seperti XSS. Perusahaan harus melakukan vulnerability scanning dan patching rutin.
Kesalahan Konfigurasi sistem	A.12.1.2 Restriction on Software Installation A.9.4.4 Use of Privileged Utility Programs	A.12.1.2 (Pengendalian instalasi perangkat lunak): Instalasi hanya dilakukan oleh personil yang berwenang dan sesuai kebijakan konfigurasi standar. A.9.4.4 (Pengendalian akses): Konfigurasi sistem harus dibatasi aksesnya hanya kepada admin dengan log aktivitas.
SQL injection	A.14.2.1 Secure Development Policy A.12.6.1 Technical Vulnerability Management	A.14.2.1 (Kontrol pengembangan sistem): Terapkan prosedur pengkodean aman dan gunakan ORM/prepared statements. A.12.6.1 (Pengelolaan kerentanan teknis): Lakukan audit dan scanning kode secara berkala untuk mencegah injeksi SQL.
Tidak adanya sistem monitoring jaringan	A.12.4.1 Event Logging A.12.4.3 Log Review	A.12.4.1 (Pencatatan dan pemantauan): Aktivitas jaringan harus direkam secara real-time dan disimpan untuk analisis. Aktifkan sistem log dan SIEM (Security Info & Event Management). A.12.4.3 (Review log): Log pemantauan jaringan harus direview secara rutin untuk mendeteksi potensi insiden.

Penyalahgunaan Hak Akses	A.9.2.3 Management of Privileged Access Rights A.9.2.5 Review of User Access Rights	A.9.2.3 (Pengelolaan hak akses): Hak akses harus diberikan berdasarkan kebutuhan dan dikaji secara berkala. A.9.2.5 (Review hak akses): Tinjauan berkala terhadap hak akses untuk mencegah penyalahgunaan dan memastikan prinsip least privilege diterapkan.

3.2 Pembahasan

Analisis risiko terhadap sistem informasi layanan pelanggan PT PLN UP3 Gresik dilakukan menggunakan pendekatan Failure Mode and Effects Analysis (FMEA) untuk mengidentifikasi potensi kegagalan, menilai dampaknya, serta menentukan prioritas mitigasi berdasarkan nilai Risk Priority Number (RPN) (Stamatis, 2003), (Amini & Aghaei, 2017). Selain itu, menurut Dinas Pendidikan Provinsi Sumatera Barat (2023) dan Amazon Web Services (2022), kontrol keamanan dari standar ISO/IEC 27001:2013 digunakan sebagai acuan dalam penyusunan langkah mitigasi yang sistematis dan terstandarisasi.

Berdasarkan hasil analisis risiko terhadap sistem informasi layanan pelanggan PT PLN UP3 Gresik menggunakan metode Failure Mode and Effects Analysis (FMEA), sebanyak 33 potensi risiko berhasil diidentifikasi dan dikategorikan berdasarkan nilai Risk Priority Number (RPN). Risiko-risiko dengan tingkat Very High (RPN ≥ 200), seperti *hardware failure, weak password policy, dan network security weakness,* ditangani melalui pendekatan *risk avoidance*, sejalan dengan kontrol pengamanan pada ISO/IEC 27001:2013. Sebagai contoh, untuk mencegah *hardware failure* akibat tidak adanya pemeliharaan rutin, digunakan kontrol A.8.16 tentang Monitoring kinerja sistem, dengan rekomendasi berupa implementasi prosedur pemeliharaan berkala dan dokumentasi aktivitas pemeliharaan.

Untuk risiko terkait kata sandi yang lemah, kontrol A.5.17 (Informasi Autentikasi) disarankan dengan menerapkan kebijakan kata sandi yang kuat dan penggantian berkala. Risiko kelemahan pada keamanan jaringan internal ditangani melalui kontrol A.8.20 (Keamanan Jaringan), yang merekomendasikan penggunaan firewall, IDS/IPS, dan segmentasi jaringan sebagai upaya preventif.

Risiko High (RPN 151–200), seperti XSS attacks, SQL injection, dan kesalahan konfigurasi, ditangani dengan pendekatan risk transfer maupun penguatan kontrol internal. Sebagai mitigasi, kontrol seperti A.14.2.9 (Pengujian Keamanan Sistem) mendorong pengujian aplikasi secara rutin, validasi input, dan penerapan Content Security Policy (CSP). Kontrol A.14.2.5 untuk SQL injection menekankan penggunaan prepared statements dan Web Application Firewall (WAF), sedangkan kesalahan konfigurasi dikendalikan melalui kontrol A.12.1.2 tentang Change Management.

Pada risiko Medium dan ke bawah, seperti tidak adanya monitoring jaringan atau penyalahgunaan hak akses, organisasi menerapkan risk reduction atau risk acceptance, namun tetap merujuk pada kontrol ISO seperti A.5.23 (Pemantauan Aktivitas) dan A.5.15 (Kontrol Akses), dengan rekomendasi berupa implementasi real-time monitoring, audit hak akses, dan pengelolaan akun secara terpusat.

Integrasi antara hasil FMEA dan kontrol dari ISO/IEC 27001:2013 ini menghasilkan pendekatan mitigasi yang lebih sistematis dan terstandarisasi, tidak hanya berdasarkan tingkat risiko tetapi juga selaras dengan praktik terbaik keamanan informasi internasional. Dengan

pendekatan ini, PT PLN UP3 Gresik dapat memperkuat sistem pengamanan informasi sekaligus meningkatkan keandalan layanan pelanggan berbasis digital secara menyeluruh.

KESIMPULAN

Penilaian risiko terhadap sistem informasi layanan pelanggan PT PLN UP3 Gresik menggunakan metode FMEA berhasil mengidentifikasi 33 potensi risiko yang diklasifikasikan berdasarkan tingkat keparahan, kemungkinan terjadi, dan kemampuan deteksi. Dengan menggabungkan hasil penilaian Risk Priority Number (RPN) dan referensi kontrol dari ISO/IEC 27001:2013 (Annex A), strategi mitigasi risiko dapat disusun secara lebih terarah, sistematis, dan sesuai dengan standar keamanan informasi global. Risiko dengan kategori Very High ditangani dengan pendekatan risk avoidance, didukung oleh kontrol seperti A.8.16 (Monitoring system), A.5.17 (Kebijakan Autentikasi), dan A.8.20 (Keamanan Jaringan). Risiko High dikelola melalui risk avoidance dan diperkuat oleh kontrol seperti A.14.2.9 (Pengujian Keamanan) dan A.12.1.2 (Manajemen Perubahan). Sementara itu, risiko pada tingkat Medium dan ke bawah ditangani dengan risk reduction atau risk acceptance, dengan tetap mempertimbangkan kontrol seperti A.5.23 (Pemantauan Aktivitas) dan A.5.15 (Kontrol Akses). Penerapan FMEA yang dikombinasikan dengan ISO/IEC 27001:2013 memungkinkan organisasi untuk tidak hanya mengidentifikasi risiko secara kuantitatif, tetapi juga merumuskan tindakan pengendalian yang relevan dan terukur. Dengan demikian, PT PLN UP3 Gresik dapat meningkatkan ketahanan sistem informasi terhadap berbagai potensi ancaman serta memperkuat tata kelola keamanan dalam pengelolaan layanan pelanggan digital.

DAFTAR PUSTAKA

Amazon Web Services. (2022). *ISO/IEC 27001:2022 compliance*. https://aws.amazon.com/compliance/iso-27001-faqs/

Amini, M. H., & Aghaei, A. A. (2017). Using FMEA for risk assessment in information systems. *International Journal of Information Management, 37*(6), 627–636.

Aurabillah, B., Putri, L. A., Fadhlilla, N. C., & Wulansari, A. (2024). Implementasi framework ISO 27001 sebagai proteksi keamanan informasi dalam pemerintahan (systematic literature review). JATI (Jurnal Mahasiswa Teknik Informatika), 8(1), 454-460.

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., & Virgio, V. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan siber di Indonesia. *Innovative: Journal of Social Science Research, 3*(6), 1135–1145.

Dinas Pendidikan Provinsi Sumatera Barat. (2023). *Implementasi ISO/IEC 27001:2022 Information Security Management Systems*. https://disdik.sumbarprov.go.id

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of qualitative descriptive studies: A systematic review. *Research in Nursing & Health, 40*(1), 23–42. https://doi.org/10.1002/nur.21768

Musyarofah, S. R. A., & Bisma, R. (2020). Pembuatan Standard Operating Procedure (SOP) keamanan informasi berdasarkan framework ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun. *Journal of Emerging Information System and Business Intelligence (JEISBI), 1*(1), 43–50.

Musyarofah, S. R. A., & 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.

Natika, L. (2024). Transformasi pelayanan publik di era digital: Menuju pelayanan masa depan yang lebih baik. *The World of Public Administration Journal, 6*(1), 1–11.

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, 3*(5), 564–573.

Sharma, K. D., & Srivastava, S. (2018). Failure mode and effect analysis (FMEA) implementation: A literature review. *Journal of Advance Research in Aeronautics and Space Science, 5*(1), 1–17.

Situngkir, D. I. (2019). Pengaplikasian FMEA untuk mendukung pemilihan strategi pemeliharaan pada paper machine. *FLYWHEEL: Jurnal Teknik Mesin Untirta, 1*(1), 39–43.

Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution* (2nd ed.). Milwaukee: ASQ Quality Press.