Perancangan Framework Mitigasi Risiko Pengelolaan Server Menggunakan ISO 27001:2022 (Studi Kasus: Unit KJSI Politeknik Negeri Bengkalis)

Rosyidah
Keamanan Sistem Informasi, Politeknik Negeri Bengkalis, Indonesia
Email: rosyidahrsyi009@gmail.com

Abstrak

Dengan meningkatnya penggunaan teknologi informasi dan komunikasi (TIK) dalam kegiatan operasional pendidikan, risiko terhadap keamanan informasi, seperti serangan siber dan bencana alam, menjadi semakin signifikan. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan merancang langkah-langkah mitigasi risiko yang sistematis dan terstruktur, guna menjaga integritas, kerahasiaan, dan ketersediaan informasi yang dikelola oleh server. Metode yang digunakan dalam penelitian ini adalah analisis risiko dengan pendekatan FMEA (Failure Mode and Effect Analysis) dan penerapan menggunakan standar ISO 27001:2022. Proses penelitian meliputi identifikasi masalah, studi literatur, identifikasi risiko, analisis risiko, evaluasi risiko, dan perancangan framework mitigasi risiko. Penelitian ini menunjukkan bahwa terdapat beberapa risiko signifikan yang perlu ditangani, seperti kerusakan fisik pada server dan kegagalan jaringan, yang dapat mempengaruhi operasional unit KJSI. Hasil penelitian ini menghasilkan sebuah perancangan framework mitigasi risiko sebagai kerangka kerja khususnya terkait pengelolaan server pada unit KJSI dengan menggunakan standar ISO 27001:2022. Dengan demikian, penelitian ini memberikan kontribusi penting dalam upaya mitigasi risiko di lingkungan pendidikan tinggi, serta menjadi acuan bagi institusi lain dalam menerapkan standar keamanan informasi yang efektif.

Kata Kunci: Mitigasi Risiko, Penerapan ISO 27001:2022, Pengelolaan Server, Keamanan Informasi, FMEA (Failure Mode and Effect Analysis)

PENDAHULUAN

Unit Pelaksana Teknis Komputer Jaringan dan Sistem Informasi adalah unit pelaksana teknis dibidang komputer. Unit KJSI ini sendiri menjadi pusat pelayanan dan pengembangan Teknologi Informasi Politeknik Negeri Bengkalis. Dalam implementasinya penggunaan Teknologi Informasi ini meningkatkan kerentanan terhadap serangan siber yang dapat menimbulkan kerugian seperti virus, malware, Phishing, Distributed Denial of service (DDos). Perlu adanya perencanaan pengamanan dengan mengidentifikasi resiko yang meliputi risiko serangan, bencana alam, dan kerentanan lainnya untuk menentukan mitigasi tepat bagi setiap risiko keamanan yang mungkin terjadi. Dengan Menerapkan langkah-langkah keamanan informasi, unit pelaksana KJSI dapat memitigasi risiko yang terkait dengan ancaman dunia maya dan insiden keamanan lainnya. Hal ini termasuk meminimalkan risiko pelanggaran data, serangan penolakan layanan, dan aktivitas jahat lainnya. Untuk dapat mengelola, menjaga dan juga menerapkan prinsip-prinsip terkait keamanan dapat menggunakan ISO 27001. ISO 27001 merupakan sistem manajemen keamanan informasi yang berstandarkan internasional yang dapat membantu untuk kebutuhan yang berkaitan dengan keamanan informasi dari sebuah lembaga atau kebutuhan lainnya. Dengan demikian, adanya ISO 27001 ini memberikan kemudahan dan sangat membantu secara efektif.

Berdasarkan hasil survei penelitian sebelumnya dan pentingnya melakukan menganalisis, menentukan terhadap risiko yang akan terjadi maupun yang akan terjadi. Maka dalam penelitian ini akan berfokus pada sebuah Perancangan Framework menggunakan ISO 27001:2022 untuk mitigasi risiko khususnya terkait penggunaan server dan tata kelola

terhadap keamanan server pada unit KJSI. Sehingga dalam Perancangan Framework untuk mitigasi risiko khususnya pada unit KJSI Politeknik Negeri Bengkalis ini berdasarkan ISO 27001:2022 dan juga metode yang dapat menjadi acuan dalam analisis risiko salah satunya adalah menggunakan FMEA (Failure Mode and Effect Analysis). Standar kerangka pada ISO 27001 dan FMEA ini sendiri menjelaskan panduan atau langkah-langkah dalam membuat, menerapkan, melaksanakan, mengelola risiko dan juga nantinya untuk melakukan mitigasi risiko yang tepat.

Tinjauan Pustaka

ISO 27001:2022Tinjauan terakhir terhadap 27002, yang secara resmi berlaku sebagai versi standar terbaru pada bulan Februari 2022, telah menghasilkan reorganisasi yang signifikan.ISO/IEC adalah standar keamanan yang sering digunakan dan paling terkenal di dunia untuk sistem manajemen keamanan informasi (ISMS). Standar ISO/IEC 27001 memberikan panduan kepada perusahaan atau lembaga organisasi pemerintahan dari berbagai ukuran dan dari semua sektor aktivitas untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi. ISO 27001:2022 adalah standar internasional yang mengatur sistem manajemen keamanan informasi (SMKI). Salah satu elemen kunci dari ISO 27001 adalah kontrol keamanan informasi, yang tercantum dalam Annex-A dari standar tersebut. Annex-A berisi daftar kontrol keamanan informasi yang dapat diterapkan oleh organisasi untuk melindungi informasi yang sensitive dan mengurangi risiko keamanan.

Risiko

Risiko adalah sesuatu yang dapat diukur dengan melihat dari tingkat dampak dan kemungkinan risiko tersebut terjadi. Dalam mengatasi risiko keamanan membutuhkan keahlian dan pengelolaan manajemen risiko keamanan [3]. Selama penilaian risiko, risiko yang diketahui dibandingkan dengan keiteria penilaian risiko yang telah ditentukan. Dengan demikian penilaian risiko tersebut dilakukan dengan menentukan Risk Priority Number (RPN) yang diperoleh dengan rumus RPN = kejadian x keparahan x deteksi.

Mitigasi Risiko

Mitigasi Risiko adalah fase penanganan risiko, fase dimana agen risiko terpilih dari fase pertama dinilai dengan tindakan penanganan. Pengelolaan atau manajemen terhadap keamanan sistem informasi diperlukan guna mengantisipasi dan meminimalisir ancaman yang mungkin terjadi. Mitigasi ini adalah sebuah langkah terakhir untuk memberikan penanganan yang memiliki sebuah tingkat tinggi, hal ini bertujuan untuk meminimalisir terjadinya risiko dan saran yang diberikan dilakukan jika nantinya terjadi risiko.

ISO/IEC 27001:2022 Sebagai Kerangka Kerja SMKI

Untuk mendukung kegiatan operasi keamanan siber, diperlukan adanya infrastruktur berupa perangkat keras, perangkat lunak, dan infrastruktur lainnya (ruangan, infrastruktur jaringan dan lain-lain). Dalam hal operasionalnya, infrastruktur tersebut harus terpenuhi perlindungan terhadap aspek berupa kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (avaibility). Untuk memenuhi perlindungan terhadap ketiga aspek tersebut, perlu diterapkan serangkaian aksi yang dapat memastikan perlindungan terhadap ketiga aspek tersebut terpenuhi. Salah satu standar yang dapat diterapkan untuk memenuhi perlindungan kerahasiaan, keutuhan, dan ketersediaan dari infrastruktur operasi keamanan siber adalah ISO/IEC 27001:2022. Standar tersebut memiliki beberapa klausul yang mengatur mulai dari konteks organisasi hingga perbaikan.

METODE PENELITIAN

Banyak Kerangka kerja, standar, metode yang dapat menjadi acuan dalam pengukuran tingkat risiko salah satunya adalah metode FMEA. FMEA adalah Teknik rekayasa yang digunakan sebagai penetapan, identifikasi dan menghilangkan kegagalan yang telah diketahui, permasalahan, error dan jenis dari sistem, desain dan proses serta jasa sebelum mencapai konsumen. Pada FMEA ada 4 penilaian yaitu severity, occurrence, detection, dan RPN (Risk Priority Number). Severity adalah penilaian berhubungan dengan seberapa besar kemungkinan terjadi impact yang mengakibatkan terjadinya kegagalan. Occurence adalah penilaian pada seberapa sering kemungkinan terjadinya suatu risiko. Detection bertujuan mengetahui seberapa besar kemungkinan terjadinya risiko dapat dideteksi secara maksimal. Dan terakhir adalah RPN yaitu perkalian nilai dari severity, occurrence dan detection.Metode FMEA digunakan untuk mengambil data angka dan penentuan Failure Mode mana yang di prioritaskan [3]. Dalam proses analisis risiko FMEA perlu dilakukan penentuan nilai severity, occurrence, dan detection. Severity merupakan tahapan awal yang digunakan untuk menganalisis risiko-risiko dengan memberikan skala berdasarkan dampak dari risiko tersebut. Skala diberikan mulai dari satu hingga sepuluh. Tahapan occurrence merupakan pengukuran terhadap tingkat frekuensi terjadinya suatu permasalahan atau risiko yang dapat menyebabkan suatu kegagalan. Tahapan detection merupakan tahapan pengukuran terhadap kemampuan dalam mengontrol kegagalan yang nantinya akan dapat terjadi. Indeks skala detection yaitu dari satu hingga sepuluh.

HASIL PENELITIAN DAN PEMBAHASAN

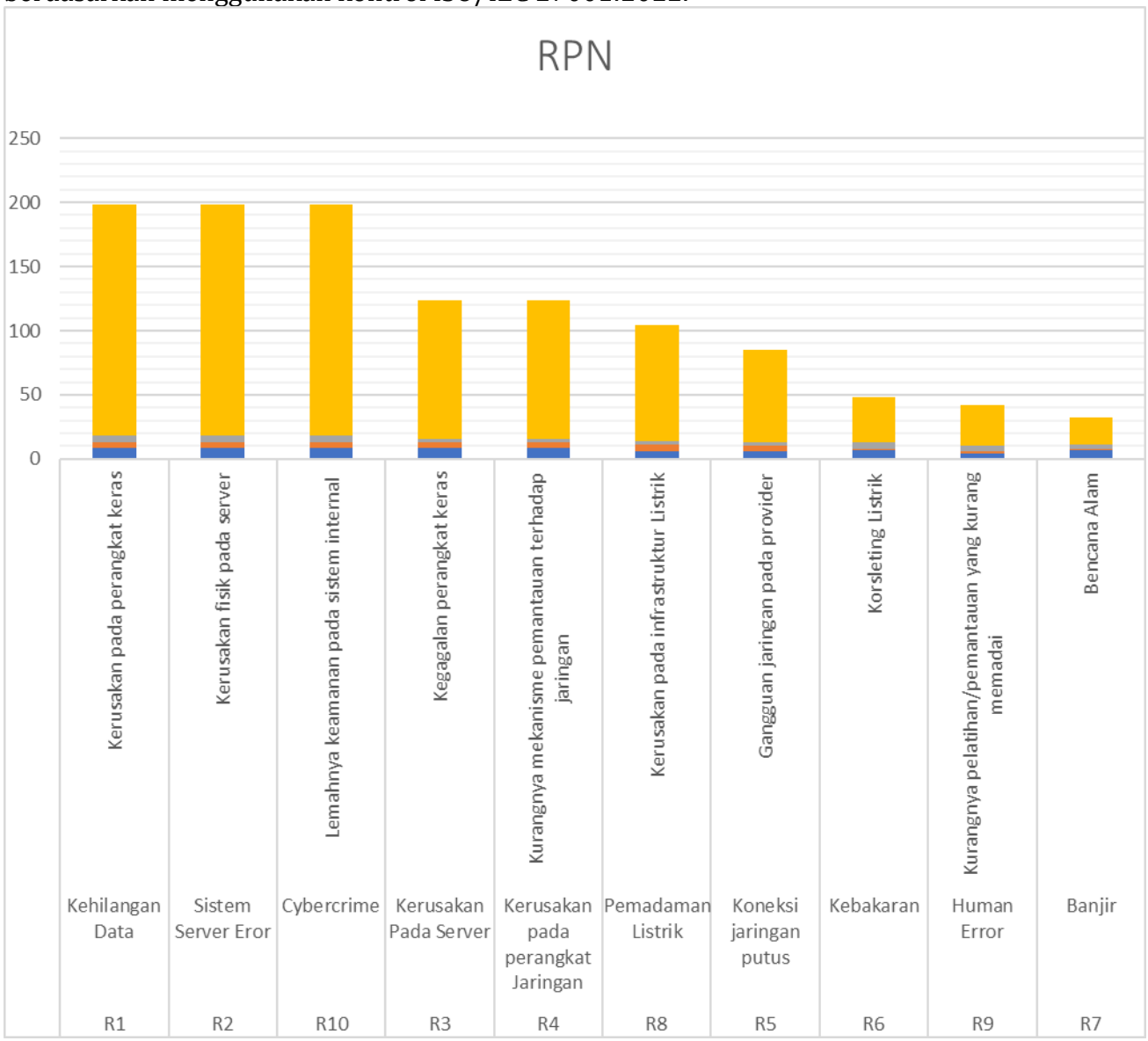
Dalam penelitian ini dilakukan untuk mengidentifikasi dan menganalisis risiko yang terkait. Dengan menerapkan langkah-langkah keamanan informasi, nantinya dapat memitigasi risiko yang terkait dengan ancaman dan risiko keamanan lainnya. Identifikasi risiko ini adalah untuk mengetahui tentang risiko yang mungkin terjadi. Setelah melakukan studi literatur, tahap ini dilakukan dengan mengumpulkan informasi guna mengetahui jenis-jenis risiko yang mungkin akan terjadi. Dalam tahap ini telah ditentukan empat konteks yang menjadi Batasan parameter internal dan eksternal untuk mempertimbangkan sumber risiko nya, yaitu alam atau lingkungan, manusia, sistem, serta infrastruktur.

Tabel 1. Rincian Penilaian Level Risiko

No.code	Risiko	Cause Failure	RPN	Penggolongan Level Risiko
R1	Kehilangan Data	Kerusakan pada perangkat keras	180	*High*
R2	Sistem Server Eror	Kerusakan fisik pada Server	180	*High*
R10	Cybercrime	Lemahnya keamanan pada sistem internal	180	*High*
R3	Kerusakan Pada Server	Kegagalan perangkat keras	108	*Medium*
R4	Kerusakan pada perangkat Jaringan	Kurangnya mekanisme pemantauan terhadap Jaringan	108	*Medium*
R8	Pemadaman Listrik	Kerusakan pada infrastruktur Listrik	90	*Medium*
R5	Koneksi jaringan putus	Gangguan jaringan pada provider	72	*Low*
R6	Kebakaran	Korsleting Listrik	35	*Low*

R9	Human Error	Kurangnya pelatihan/pemantauan yang kurang memadai	32	*Low*
R7	Banjir	Bencana Alam	21	*Low*

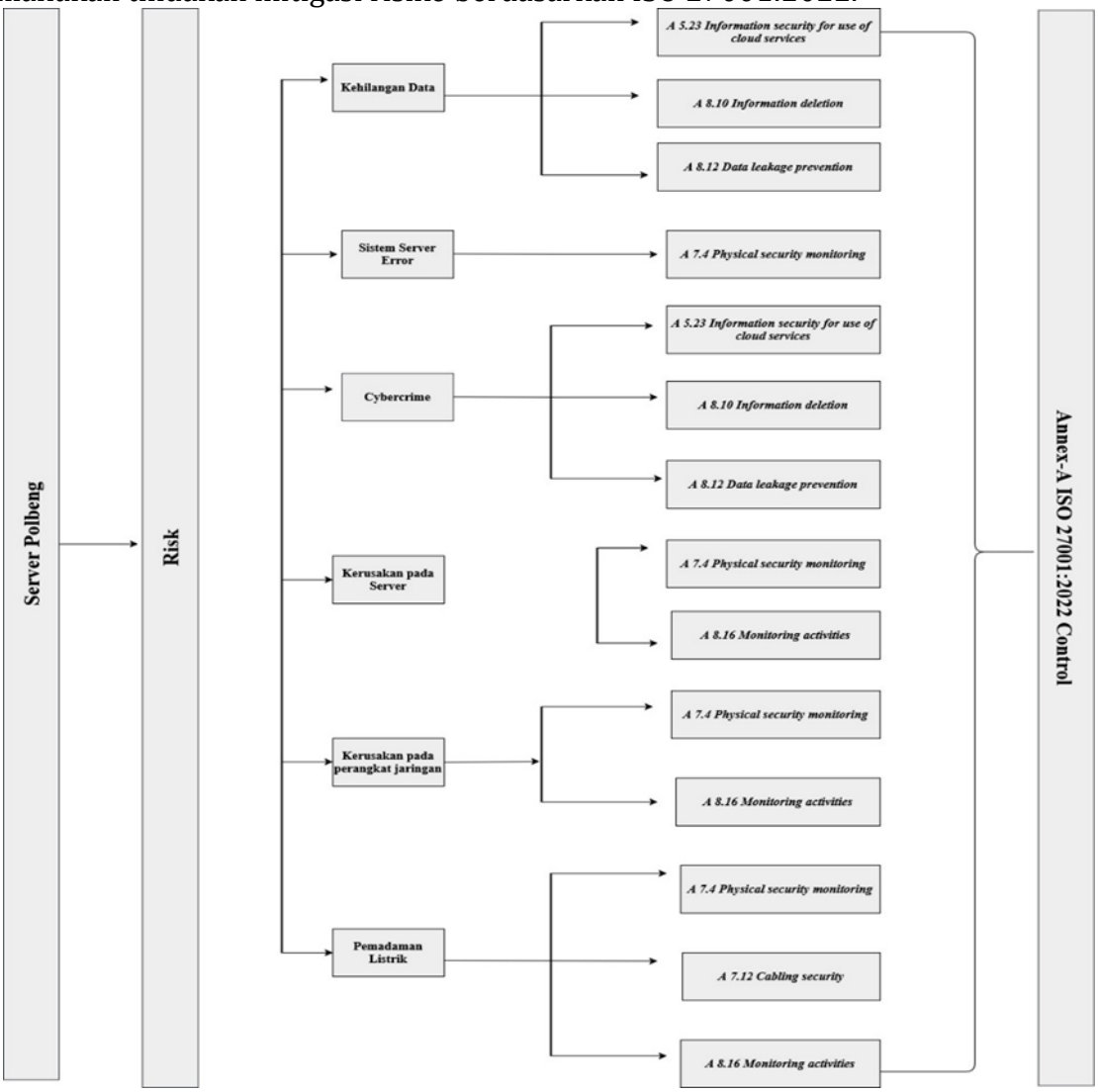
Berdasarkan hasil pemetaan pada table diatas maka cause failure yang akan dilakukan pemetaan risiko adalah risiko R1, R2, R10, R3, R4, R8 karena memiliki tingkatan yang dikategorikan perlu untuk dikontrol. Pemetaan Risiko tersebut adalah langkah untuk memberikan penanganan, hal ini bertujuan untuk meminimalisir terjadinya risiko dan saran yang diberikan dapat dilakukan jika risiko terjadi. Pada table dibawah ini dilakukan berdasarkan menggunakan kontrol ISO/IEC 27001:2022.



Gambar 1. Penilaian Risiko

Berdasarkan hasil dari penilaian level Risiko pada gambar diatas, pada pembahasan diatas dapat disimpulkan bahwa terdapat 10 Cause Failure yang menyebabkan terjadinya risiko. Oleh karena itu, peningkatan pada keamanan sistem serta pelatihan dan juga pemeliharaan yang bersifat rutin terhadap pengelolaan pada server. Guna untuk mengurangi

risiko yang lebih tinggi, sambil evaluasi terhadap risiko seperti kebakaran dan banjir selalu berada dalam rencana keberlangsungan perlu dilakukan. Pada penilaian risiko tersebut terdapat 10 cause failure yang sudah dilakukan penilaian tingkat risiko dan disorting berdasarkan mulai dari nilai risiko terbesar sampai terkecil sehingga diketahui yang mana yang akan dilakukan tindakan mitigasi risiko berdasarkan ISO 27001:2022.



Gambar 2. Risk Mitigation Framework

Berdasarkan pada gambar diatas, merupakan perancangan Framework/kerangka kerja dari mitigasi risiko pada pengelolaan server. Yang dimana framework tersebut terdiri dari risiko yang sudah di identifikasi dan di analisis sebelumnya sehingga hasil akhir nya dapat dilakukan dengan rekomendasi penanganan risiko dengan menggunakan standar ISO 27001:2022. Standar ISO 27001:2022 ini sendiri merupakan kontrol yang digunakan dalam tahap mitigasi ataupun penanganan risiko. Yang dimana pada tahap penanganan risiko tersebut menggunakan beberapa kontrol yang diterapkan sesuai dengan setiap risiko yang teridentifikasi. Terdapat kontrol pada Annex-A yang digunakan pada penanganan risiko tersebut di antaranya 5.23 Information security for use of cloud services, pada kontrol tersebut terdapat pada Annex-A yang dimana pada kontrol tersebut dijelaskan proses akuisisi, penggunaan, pengelolaan, dan keluar dari layanan cloud harus ditetapkan sesuai dengan persyaratan keamanan informasi. Pada kontrol 8.10 Information deletion, dijelaskan bahwa

informasi yang disimpan dalam sistem informasi, perangkat, atau media penyimpanan lainnya harus dihapus jika tidak diperlukan lagi. Pada kontrol 8.12 Data leakage prevention, dijelaskan bahwa tindakan pencegahan kebocoran data harus diterapkan pada sistem, jaringan, dan perangkat lain apa pun yang memproses, menyimpan, atau mengirimkan informasi sensitif. Pada kontrol 8.16 Monitoring activities, dijelaskan bahwa jaringan, sistem harus dipantau untuk melihat pelakuk anomaly dan tindakan yang tepat harus diambil untuk mengevaluasi potensi insiden keamanan informasi. Pada kontrol 7.4 Physical security monitoring, dijelaskan bahwa tempat harus dipantau untuk pemeriksaan fisik yang tidak sah mengakses. Serta pada kontrol 7.12 Cabling security, dijelaskan bahwa kabel yang membawa listrik, data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan. Pada kontrol-kontrol tersebut diterapkan untuk melindungi informasi yang sensitive dan mengurangi risiko keamanan nya khususnya terkait pada pengelolaan server.

KESIMPULAN

Dengan menggunakan Framework mitigasi risiko tersebut pihak yang terkait nantinya dapat mengetahui penilaian mengenai keamanan risiko informasi dengan diberi kategori dan peringkat level, sehingga mengetahui yang mana yang harus diperbaiki, dievaluasi dan ditingkatkan. Berdasarkan hasil pemetaan akhir untuk melihat kesesuaian nilai RPN dan Matrik didapatkan 6 cause failure yang akan dilakukan penanganan mitigasi. 6 cause failure tersebut diantaranya adalah Kehilangan data (R1), Sistem server Error (R2), Cybercrime (R10), Kerusakan pada server (R3), Kerusakan pada perangkat jaringan (R4), dan Pemadaman Listrik (R8). Yang dimana mitigasi atau penanganan 6 cause failure menggunakan standar ISO 27001:2022. Beberapa saran yang dapat digunakan antara lain, diharapkan untuk dilakukan update serta pemantauan secara rutin, melakukan identifikasi dan memberi perlindungan terhadap pada pengelolaan server untuk meminimalisir terjadinya risiko dan mengetahui tindakan yang akan dilakukan saat risiko itu terjadi.

DAFTAR PUSTAKA

A. R. Hakim and R. A. P. Wijaya, "Perancangan Perangkat Audit Internal untuk Sistem Keamanan Informasi pada Organisasi XYZ," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 3, p. 435, 2020, doi: 10.25126/jtiik.2020701940.

B. Aurabillah, L. Aprillia Putri, N. Citra Fadhlilla, and A. Wulansari, "Implementasi Framework ISO 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 454– 460, 2024, doi: 10.36040/jati.v8i1.8736.

H. G. Afiansyah and N. A. Kadarwati Febriyani, "Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan

L. Munaroh, Y. Amrozi, and R. A. Nurdian, "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013," *Technomedia J.*, vol. 5, no. 2 Februari, pp. 167–181, 2020, doi: 10.33050/tmj.v5i2.1377.

M. T. Anwar, U. Aryanti, M. Wijana, and D. Atmoko, "Mitigasi Risiko Keamanan Informasi Menggunakan SNI ISO / IEC 27001 : 2013 Berbasis Manajemen Risiko OCTAVE Allegro di Perguruan Tinggi : Studi kasus Perguruan Tinggi x," vol. 9, no. 1, pp. 73–83, 2024.

NIST CSF 2.0 dan ISO/IEC 27001:2022," Info Kripto, vol. 17, no. 3, 2023, doi: 10.56706/ik.v17i3.81.