Jurnal Teknik Komputer AMIK BSI
Volume 8, No.2, Juli 2022
P-ISSN 2442-2436, E-ISSN: 2550-0120
Akreditasi Ristekdikti, No: 36/E/KPT/2019 (Sinta 4)
DOI: 10.31294/jtk.v4i2

Evaluasi Aspek Keamanan Informasi Sistem Penilaian Mahasiswa Magang Menggunakan Metode *Failure Mode and Effect Analysis*

Subektiningsih[1], Aan Romadhon Eko Prasetyo[2], Rini Indrayani[3]

[1,2,3]Universitas Amikom Yogyakarta
[1]e-mail: subektiningsih@amikom.ac.id
[2]e-mail: aandinatha@gmail.com
[3]e-mail: rini.i@amikom.ac.id

Diterima	Direvisi	Disetujui
18-07-2022	20-07-2022	26-07-2022

Abstrak - Perusahaan Rintisan XY menggunakan Sistem Pendukung Keputusan Penilaian Mahasiswa Magang untuk menilai mahasiswa dan mendapatkan perangkingan. Dalam sistem yang berbasis website tersebut tersimpan data-data yang bersifat *sensitive* dan perlu memberikan batasan akses kepada pengguna untuk menjaga kredibilitas data. Saat data hilang atau diubah oleh pengguna yang tidak bertanggung jawab dapat mengakibatkan kesalahan dalam pemberian nilai mahasiswa magang. Oleh sebab itu, perlu dilakukan evaluasi terhadap aspek keamanan menggunakan Metode *Failure Mode and Effect Analysis* (FMEA) untuk memetakkan prioritas resiko yang dapat terjadi pada sistem dalam dimensi CIA *(Confidentiality, Integrity, Availability).* Hasil evaluasi menyatakan bahwa resiko paling tinggi dapat terjadi pada aspek *confidentiality* yang mengakibatkan kehilangan akses sistem karena kehilangan data user yang harus digunakan untuk login ke dalam sistem. Prioritas resiko kedua ada di aspek *integrity* yang berkaitan dengan data tidak valid yang disebabkan oleh kesalahan input data atau data tidak sengaja terhapus oleh user yang sedang mengelola data sistem. Prioritas resiko ketiga berada pada aspek *availability* dengan resiko data tidak dapat ditampilkan dikarenakan kesalahan sambungan dengan database dan atau koneksi sistem dengan web server yang tidak aktif. Ketiga prioritas resiko tersebut bersatus *very high*. Resiko paling rendah dengan level *very low* berupa resiko gagal memperbaharui *data user.* Penggunaan metode FMEA memberikan hasil dengan level dan kriteria yang jelas dengan batasan tingkat resiko. Sehingga, Perusahaan XY dapat memfokuskan untuk mengantisipasi resiko yang paling berpotensi dengan cara yang lebih tepat.

Kata Kunci: confidentiality integrity availability, FMEA method, information security

Abstract *- Startup XY uses the Student Apprentice Assessment Decision Support System to assess students and obtain rankings. In the website-based system, sensitive data is stored and it is necessary to provide access restrictions to users to maintain the credibility of the data. When data is lost or changed by irresponsible users, it can result in errors in grading interns. Therefore, it is necessary to evaluate the security aspect using the Failure Mode and Effects Analysis (FMEA) method to map out the priority risks that can occur in the system in the CIA dimension (Confidentiality, Integrity, Availability). The results of the evaluation state that the highest risk can happen in the confidentiality aspect, which results in loss of system access due to loss of user data that must be used to log into the system. The second risk priority is the integrity aspect related to invalid data caused by input errors or data accidentally deleted by users managing system data. The third risk priority is on the availability aspect with the risk that data cannot be displayed due to an error in connection with the database and or system connection with an inactive web server. The three risk priorities are very high together. The lowest risk with a shallow level is the risk of failing to update user data. The FMEA method provides results with precise levels and criteria with limits on the level of risk. Thus, Company XY can focus on anticipating the most potential risks more appropriately.*

Keywords: confidentiality integrity availability, FMEA method, information security

PENDAHULUAN

Informasi menjadi aset yang penting karena berpengaruh terhadap proses bisnis organisasi, instansi, bahkan dapat menjadi ancaman (Saputra et al., 2020). Disebutkan oleh (Tiorentap & Hosizah, 2020) dalam ISO 27001 menyebutkan bahwa informasi yang dapat dipertanggungjawabkan kebenaran dan jaminan kesesuainnya harus mencakup tiga aspek, yaitu: *confidentiality, integrity, availability.* Aspek kemanan informasi yang dikenal dengan istilah CIA Triad tersebut menjadi model dasar keamanan data dan informasi (Yampolskiy et al., 2021). Oleh sebab itu, menjadi penting untuk menjaga keamanan informasi. Saat melakukan upaya untuk menjaga keamanan informasi, maka reputasi perusahaan juga dapat terjaga (Kelrey & Muzaki, 2019). Sehingga, perusahaan perlu mengkaji bagaimana penerapan aspek keamanan informasi tersebut dalam dalam sistem yang digunakan oleh perusahaan. Hal ini dikarenakan sebuah sistem perusahaan menyimpan banyak data dan informasi yang sangat bernilai. Informasi tersebut harus dikelola dengan tepat supaya tidak menimbulkan resiko maupun kerusakan (Ramadhani, 2018). Aspek keamanan informasi *Confidentiality* atau kerahasiaan mempunyai ruang lingkup untuk memastikan bahwa informasi hanya diakses oleh pihak yang berhak (Nurul et al., 2022). Bahkan, pembatasan pengguna juga dapat diterapkan untuk akses perangkat (Subektiningsih et al., 2022). Aspek *Integrity* atau integritas berkaitan dengan tindakan mengubah data hanya dapat dilakukan oleh pihak yang berwenang, sehingga informasi terjaga keutuhan, keakuratan, dan metode pemrosesannya (Saputra et al., 2020). Aspek *Availability* atau ketersediaan menyatakan bahwa informasi harus dapat diakses saat dibutuhkan (Wowor et al., 2018). Aspek ketersediaan juga menjamin bahwa hanya pengguna yang berhak, yang dapat memanfaatkan informasi tersebut (Kelrey & Muzaki, 2019). Informasi harus dapat diakses kapanpun saat dibutuhkan (Triandi, 2019). Ketika aspek ketersediaan dalam keamanan informasi dijadikan target serangan, maka dapat menimbulkan dampak hilangnya akses terhadap informasi tersebut (Jumardi, 2018).

Aspek keamanan informasi dalam sistem rekam medis eletronik diuraikan dalam (Tiorentap & Hosizah, 2020). Penelitian tersebut menghasilkan persentase pencapaian keamanan informasi yang diterapkan berdasarkan aspek *privacy, integrity, authentication, availability, access control, non-repudiation*. Berdasarkan ke semua aspek keamanan informasi tersebut terdapat *gap* atau temuan dikarenakan belum menerapkan audit ISO 27001 tentang Sistem Manajemen Keamanan Informasi. Dalam menelitian memberikan saran untuk segera melakukan audit internal dan eksternal terhadap sistem rekam medis elektronik yang diterapkan di klink Medical Check-Up MP.

Dalam (Triandi, 2019) melakukan kajian tentang bentuk ancaman terhadap keamanan informasi yang terkait dengan aksiologi. Memaparkan pentingnya keamanan informasi berdasarkan teori aksiologi sebagai cara untuk berfikir. Dalam (Saputra et al., 2020) menguraikan tentang manajemen sistem keamanan informasi berdasarkan ISO 17799. Kebijakan yang diterapkan di dalam organisasi antara lain: kontrol dan proteksi; pemantauan dan audit; serta ancaman yang dapat terjadi dalam memanajemen sistem keamanan informasi. Analisis pengaruh sistem keamanan informasi dari nasabah yang memanfaatkan *internet banking* diuraikan dalam (Ava Dianta & Zusrony, 2019). Keamanan sistem informasi perbankan dalam melakukan transaksi layanan menjadi penting untuk mewujudkan layanan yang akuntabel. Dalam penelitian ini juga meninjau dari aspek *confidentiality, integrity, availability* dengan melakukan *Forum Group Discussion* terhadap karyawan di PT. XYZ, Salatiga. Hasil dari penelitian menyatakan bahwa indikator *access speed* dari dimensi *availability* yang paling berpengaruh terhadap keamanan sistem untuk fitur *internet banking,* yang selanjutnya dapat dijadikan rekomendasi untuk peningkatan keamanan data fitur *internet banking* tersebut.

Dalam (Kelrey & Muzaki, 2019) menguraikan pentingnya melindungi asset digital perusahaan karena dapat mempengaruhi kinerja dari sebuah bisnis. Konsep keamanan informasi yang dijabarkan berdasarkan aspek *confidentiality, integrity, availability.* Selain itu, juga menjelaskan tentang konsep keamanan informasi yang berkaitan dengan orang yang memanfaatkan informasinya, yaitu: *authentication, authorization, non-repudation.* Menyajikan pengaruh dari *ethical hacking* untuk menjamin sistem informasi perusahaan tetap handal. Penelitian tentang *confidentiality, integrity, availability* dalam sumber daya informasi untuk mewujudkan keamanan sistem informasi diuraikan dalam (Nurul et al., 2022). Kemanan informasi ditujukan untuk melindungi komputer, non-peralatan komputer, data, informasi, dan fasilitas dari penyalahgunaan orang yang tidak mempunyai izin akses. Hasil dari penelitian tersebut adalah keamanan sistem informasi dipengaruhi oleh keamanan informasi, teknologi informasi, dan *network* atau jaringan. Dalam (Jumardi, 2018) menyatakan bahwa semakin berharga informasi dibutuhkan standar keamanan untuk tetap menjaga informasi. Standar keamanan informasi ini juga berkaitan dengan perlindungan privasi terhadap informasi karyawan di sebuah perusahaan. Perlindungan privasi karyawan di perusahaan menjadi faktor yang harus diperhatikan dalam menerapkan keamanan sistem informasi. Dalam hal ini penerapan kebijakan keamanan sistem informasi antara lain: memelihara sistem, menangani resiko, mengatur hak akses dan sumber daya manusia,

keamanan dan mengendalikan aset informasi, serta kebijakan keamanan server. Penerapan kebijakan tersebut akan menjadi wujud perlindungan terhadap informasi perusahaan dan menjaga kerahasiaan privasi karyawan Perusahaan XYZ. Dimensi penelitian aspek keamanan informasi disajikan dalam Tabel 1.

Tabel 1. Dimensi Penelitian Aspek Keamanan Informasi

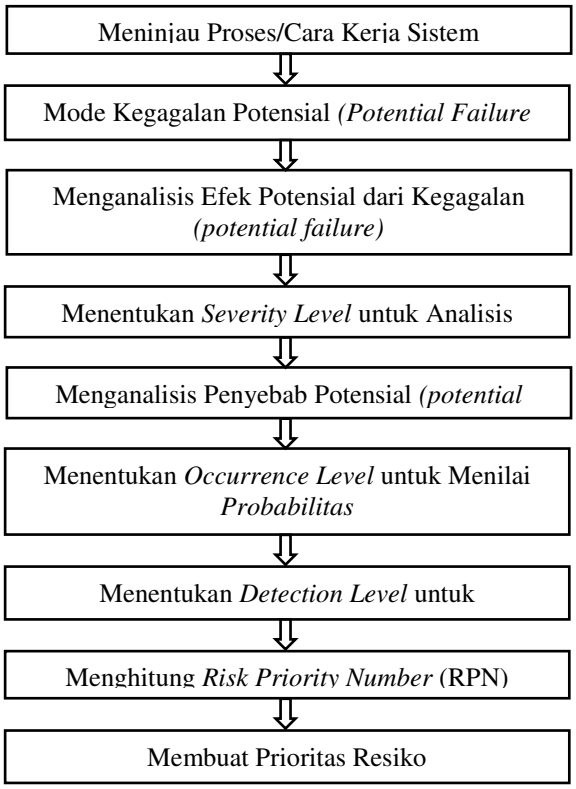
Tahun	Nama Peneliti	Aspek Keamanan Informasi yang Diteliti
2022	Nurul, S., Anggrainy, S., & Aprelyani, S.	Menerapkan aspek confidentiality, integrity, availability dalam sumber daya informasi untuk mewujudkan keamanan sistem informasi dalam melindungi komputer, non-peralatan komputer, data, informasi, dan fasilitas dari penyalahgunaan orang yang tidak mempunyai izin akses.
2020	Tiorentap, D. R. A., & Hosizah, H.	Aspek keamanan informasi dalam sistem rekam medis eletronik berdasarkan aspek privacy, integrity, authentication, availability, access control, non-repudiation.
2020	Saputra, H. M. J., Sinambela, B. S., Awal, R. J., & Fiqar, T. P.	Penerapan standar manajemen sistem keamanan informasi adalah ISO:17799 untuk kontrol dan proteksi, proses pemantauan dan audit, dan mengetahui ancaman dalam sistem keamanan informasi.
2019	Kelrey, A. R., & Muzaki, A	Konsep keamanan informasi yang dijabarkan berdasarkan aspek confidentiality, integrity, availability. Konsep keamanan informasi yang berkaitan dengan orang yang memanfaatkan informasinya, yaitu: authentication, authorization, non-repudation.
2019	Ava Dianta, I., & Zusrony, E.	Manajemen sistem keamanan informasi berdasarkan ISO 17799 dengan menganalisis pengaruh sistem keamanan informasi dari nasabah yang memanfaatkan internet banking diuraikan dalam tinjauan aspek confidentiality, integrity, availability dengan melakukan Forum Group Discussion terhadap karyawan di PT. XYZ.
2018	Jumardi, R.	Penerapan kebijakan keamanan sistem informasi berdasarkan pada standar ISO 17799: 27002 dan juga standar yang dikeluarkan oleh ID SIRTII meliputi: EISP, ISSP dan SSP. Mempertimbangkan prinsip utama keamanan sistem informasi, yaitu confidentiality, integrity, availability, privacy, access control, authority, authentication, non-repudiation untuk mengkaji kebijakan keamanan sistem informasi di Perusahaan XYZ yang berkaitan dengan perlindungan kerahasiaan data karyawan.

Setiap informasi pasti mempunyai nilai (Sudjiman & Sudjiman, 2018). Keamanan informasi berkaitan dengan beberapa aspek ancaman, yaitu: *interruption, interception, modification, fabrication* (Kelrey & Muzaki, 2019). Ancaman ini dapat berasal dari sisi internal maupun eksternal dengan cara yang disengaja atau bahkan tidak disengaja (Ramadhani, 2018). Kondisi kasus atau ancaman yang terjadi dapat dipengaruhi oleh spesifikasi kasus (Subektiningsih et al., 2018) maupun tujuan dari penyerang. Sehingga, perlu untuk memperhatikan ketiga aspek keamanan informasi yang berupa *confidentiality, integrity, availability.* Berlaku juga bagi Perusahaan Rintisan XY di Yogyakarta yang perlu menjaga keamanan infromasi yang dimilikinya. Dalam Perusahaan Rintisan XY terdapat kegiatan magang mahasiswa yang ditahap akhir terdapat proses penilaian. Supaya penilaian dapat dilakukan secara objektif dan transparan, maka Perusahaan Rintisan XY menggunakan Sistem Pendukung Keputusan Penilaian Mahasiswa Magang Tujuan dari perangkingan ini adalah untuk menentukan mahasiswa magang terbaik. Sistem tersebut menggunakan metode eletre untuk proses penentuan keputusan penilaian mahasiswa. Penggunaan sistem memang dapat diandalkan oleh pengambil keputusan dengan pertimbangan manfaat yang diperoleh (Komalasari, 2020).

Dalam sistem yang berbasis website tersebut tersimpan berbagai data, yaitu: data login sistem, profil admin, alternatif, kriteria, nilai, perhitungan nilai akhir, mahasiswa, penguna sistem, *role access.* Data-data tersebut bersifat *sensitive* dan perlu memberikan batasan akses kepada pengguna untuk menjaga kredibilitas data. Saat data hilang atau diubah oleh pengguna yang tidak bertanggung jawab dapat mengakibatkan kesalahan dalam pemberian nilai mahasiswa magang. Oleh sebab itu, perlu dilakukan evaluasi terhadap aspek keamanan dari berbagai jenis informasi yang tersimpan di dalam sistem perusahaan. Evaluasi dilakukan menggunakan Metode *Failure Mode and Effect Analysis* (FMEA) yang menyajikan prosedur terstruktur untuk mengidentifikasi sebanyak mungkin penyebab kegagalan (Suryana et al., 2017). Identifikasi mode kegagalan bertujuan untuk mengetahui apakah sistem hanya dapat diakses oleh orang yang berwenang? Apakah sistem dapat menjamin bahwa data utuh, akurat, dan tidak berubah tanpa izin dari pihak yang berhak? Serta memastikan apakah data akan selalu tersedia saat diperlukan? Metode *Failure Mode and Effect Analysis* diterapkan untuk mengidentifikasi kegagalan sistem yang berfokus pada data, fitur, cara kerja sistem untuk penilaian mahasiswa dan penerapan mekanisme keamanan informasi pada sistem, sehingga dapat dipetakkan prioritas resiko yang dapat terjadi pada sistem dalam dimensi CIA *(Confidentiality, Integrity, Availability).*

METODOLOGI PENELITIAN

Pengumpulan data dilakukan dengan melakukan wawancara terhadap pegawai di Perusahaan Rintisan XY untuk mengetahui kriteria, alternatif, dan pembobotan dalam penilaian mahasiswa magang. Selain itu, wawancara juga dilakukan untuk mendapatkan berbagai fitur dan cara kerja dari Sistem Pendukung Keputusan Penilaian Mahasiswa Magang tersebut. Pengumpulan data juga dilakukan dengan cara studi Pustaka, yaitu mengkaji berbagai referensi untuk mengumpulkan informasi yang relevan dengan topik yang difokuskan. Sumber referensi yang dikaji antara lain: jurnal ilmiah dan *e-book*. Metode yang digunakan adalah FMEA (Failure Mode and Effect Analysis) dengan langkah-lagkah yang ditunjukkan dalam Gambar 1 (Suryana et al., 2017) dipadukan dalam (Gambino et al., 2018).



Gambar 1. Tahap Penelitian dengan Metode *Failure Mode and Effect Analysis* (FMEA)

Dalam penelitian harus dapat melihat dan memahami fokus masalah dalam konteks lebih luas di jejaring realitas yang bertaut secara berkelanjutan (Helaluddin & Wijaya, 2019). Data yang diperlukan diperoleh melalui wawancara, buku, website yang terus menerus dikumpulkan sampai data jenuh (Zakariah et al., n.d.).

Tahap yang dilakukan dalam Gambar 1 adalah sebagai berikut:

1. Meninjau Proses/Cara Kerja Sistem

Tahap yang pertama dalam metode *Failure Mode and Effect Analysis* adalah mendeskripsikan berbagai fitur yang ada di dalam sistem dan berbagai proses yang terjadi di dalam sistem. Bagian ini menjinjau tentang berbagai data dan informasi yang dikelola oleh sistem. Meninjau bagaimana mekanisme aspke keamanan diterapkan di dalam bagian-bagian tersebut. Sehingga, diketahui keterkaitan antara mekanisme keamanan yang diterapkan dalam sistem dengan data, informasi, fitur, dan proses yang terjadi dalam sistem.

2.* Mode Kegagalan Potensial *(Potential Failure Mode)

Dalam tahap ini membuat daftar kegagalan sistem yang berpotensi dapat dialami oleh sistem. Saat mekanisme dalam aspek keamanan tidak diterapkan dalam sistem dimungkinkan menyebabkan kegagalan dalam fitur sistem beroperasi.

3. Menganalisis Efek Potensial dari Kegagalan *(potential failure)*

Tahap ini melakukan analisis kemungkinan efek potensial yang dapat terjadi karena terjadinya kegagalan sistem.

4. Menentukan *Severity Level* untuk Analisis Resiko

Tahap ini menentukan nilai *severity.* Dalam hal ini *Severity level* adalah penilaian untuk mengetahui tingkat keparahan dari dampak *(effect)* yang terjadi akibat kegagalan sistem *(failure mode)*. Mengetahui tingkat keparahan dari dampak kegagalan yang dapat mempengaruhi *output* dan cara sistem bekerja atau proses sistem.

5.* Menganalisis Penyebab Potensial *(potential cause)

Dalam tahap ini melakukan analisis terhadap penyebab potensial yang menyebabkan berbagai dampak, kegagalan, dan resiko sistem. Mengetahui bagiamana pemenuhan aspek keamanan diterapkan.

6. Menentukan *Occurrence Level* untuk Menilai Probabilitas

Tahap ini melakukan penilaian tentang peluang atau frekuensi kegagalan yang dapat terjadi, sehingga menimbulkan *failure mode* selama menggunakan sistem penilaian mahasiswa. Kriteria *Ocurrence* ditunjukkan dalam Tabel 2 (Gambino et al., 2018).

Tabel 2. *Occurrence*

Rating	Klasifikasi	Keterangan
10 dan 9	Sangat Tinggi	Kegagalan yang tak terganti
8 dan 7	Tinggi	Kegagalan berulang
6 dan 5	Sedang	Kegagalan sesekali
4, 3 dan 2	Rendah	Sedikit kegagalan

7. Menentukan *Detection Level* untuk Pengendalian

Tahap ini menganalisis kemampuan pengendalian kegagalan yang dapat terjadi karena aspek keamanan informasi tidak terpenuhi.

8. Menghitung *Risk Priority Number* (RPN)

Tahap ini mendapatkan nilai dari *Risk Priority Number.* Nilai ini diperoleh dari hasil perkalian antara nilai *Severity (S), Occurrence (O), Detection (D)*. Rumus dari RPN = S x O x D (Gambino et al., 2018). Nilai RPN digunakan sebagai acuan untuk mengetahui tingkat keparahan berdasarkan hasil yang paling tinggi, yang berarti memerlukan penanganan serius.

9. Membuat Prioritas Resiko

Dalam tahap ini membuat daftar resiko yang diprioritaskan untuk ditindaklanjuti. Daftar ini diperoleh berdasarkan dari Nilai RPN yang paling tinggi hingga paling rendah.

HASIL DAN PEMBAHASAN

Penerapan Metode *Failure Mode and Effect Analysis* (FMEA) untuk mengevaluasi aspek keamanan informasi pada Sistem Penilaian Mahasiswa Magang di Perusahaan Rintisan XY diuraikan sebagai berikut:

1. Meninjau Proses/Cara Kerja Sistem

Sistem Penilaian Mahasiswa Magang Mahasiswa di Perusahaan Rintisan XY berbasis website yang dibangun menggunakan framework CodeIgniter. Sistem ini bisa diakses oleh perusahaan secara *local network* dengan xampp sebagai web server. Dalam tahap ini dilakukan analisis kebutuhan fungsional dan non-fungsional untuk mengetahui kebutuhan sistem supaya dapat beroperasi. Kebutuhan fungsional sistem berisi proses-proses yang dilakukan oleh sistem, sehingga mempunyai fungsi-fungsi yang dapat dijalankan, antara lain:

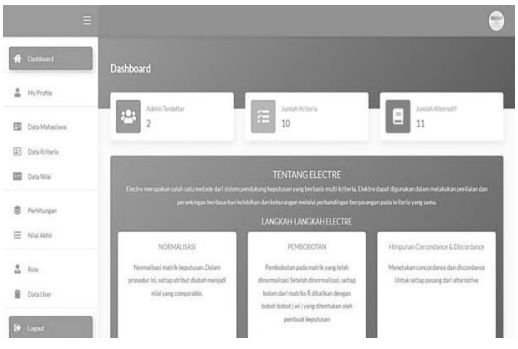
a. Sistem dapat menyimpan data alternatif, kriteria, serta nilai juga dapat menampilkan data tersebut;
b. Sistem mampu mengolah data alternatif dan juga kriteria;
c. Sistem yang dibuat berdasarkan data dan perhitungan dari kriteria yang telah ditentukan dapat memberikan hasil yang lebih akurat dalam penilaian mahasiswa magang;
d. Sistem mampu membedakan hak akses setiap pengguna *(user)* dengan *username* dan *password* yang tersimpan pada database;
e. Sistem mampu memberikan hasil akhir perangkingan secara objektif dengan penghitungan menggunakan metode electre.

Pada kebutuhan non fungsional perangkat keras dan perangkat lunak yang digunakan untuk menjalankan sistem. Dalam menjalankan sistem penilaian mahasiswa magang ini dapat menggunakan laptop atau *personal computer* dengan spesifikasi minimal RAM 4 GB, processor Intel (R) Celeron, media penyimpanan berupa Hard Disk 500 GB, VGA Intel(R) HD Graphics. Sedangkan, untuk perangkat lunak dalam menjalankan sistem membutuhkan minimal spesifikasinya dengan Sistem Operasi Windows 7, xampp sebagai web server, chrome atau firefox sebagai web browser. Sistem penilaian mahasiswa ini berbasis website yang beroperasi di jaringan lokal. Data yang ada di dalam sistem berupa:

a. Data login sistem terdiri dari *username* yang berupa email dan *password*.
b. Data Alternatif mempunyai id alternatif dan nama alternatif.
c. Data Kriteria mempunyai id kriteria, nama kriteria, dan bobot.
d. Data Nilai antara lain: id alternatif, nama alternatif, nilai berdasarkan dari data kriteria.
e. Data Perhitungan nilai akhir akan membentuk perbandingan berbdasarkan alternatif dan kriteria.
f. Data mahasiswa antara lain: id mahasiswa, nama, email, nim, jurusan, kampus, divisi, judul, no, dan alamat.
g. Data Nilai Akhir akan menampilkan data nama mahasiswa, total nilai akhir dan ranking dari mahasiswa.
h. Data Penguna sistem *(user)* mempunyai data berupa id user, nama, email, image, password, role_id, dan tanggal.
i. Data R*ole access* mempunyai data id dan *role.*

Sistem penilaian mahasiswa mempunyai berbagai fitur, antara lain:

a. Halaman login yang digunakan untuk dapat mengakses sistem. Pengguna harus mempunyai *username* yang berupa alamat email dan *password* supaya bisa melakukan login dan menggunakan sistem. Sistem akan mengecek kesesuaian *username* dan *password* setelah pengguna yang telah menginputkan *username* dan *password* tersebut. Saat *username* dan *password* benar, maka akan masuk ke dalam halaman *dashboard* yang ditunjukkan dalam Gambar 2. Namun, jika *username* dan *password* tidak sesuai ketika sistem melakukan pengecekan, maka sistem akan menampilkan pesan error bahwa *username* dan *password* tidak sesuai.



Gambar 2. Tampilan Dashboard Sistem Penilaian Mahasiswa Magang

Dalam halaman login terdapat fitur "*forgot password"* yang digunakan oleh pengguna untuk mendapatkan akses kembali ketika kehilangan atau lupa dengan *password* atau kata sandi yang dimiliki. Fitur yang lainnya adalah dapat digunakan untuk membuat akun pengguna baru. Tampilan login ditunjukkan dalam Gambar 3.

Gambar 3. Fitur Login

b. Halaman My Profile yang berfungsi untuk menampilkan data pengguna *(user data)* yang login ke dalam sistem. Pada halaman ini Admin Sistem dapat mengubah data pengguna dan mengubah *password.* Sistem akan melakukan pengecekan atas kesesuaian data yang diubah. Sistem akan memastikan bahwa semua *form* telah diisi. Sistem juga akan melakukan pengecekan terhadap *password* yang diganti. Apabila password lama salah dan *password* baru yang diinputkan tidak sesuai dengan *repeat password,* maka sistem akan menampilkan pesan kesalahan atau *error*. Apabila *password* yang diisikan telah sesuai, maka *password* berhasil diubah dan tersimpan.
c. Halaman Data Mahasiswa digunakan untuk mengelola data mahasiswa. Fitur digunakan untuk menambah data mahasiswa. Sistem akan memastikan bahwa semua *form* yang diminta telah terisi. Saat terdapat *form* belum terisi, maka akan menampilkan pesan error. Namun, ketika semua *form* telah diisi, maka data mahasiswa dapat disimpan. Fitur ini dapat digunakan untuk mengedit dan menghapus data mahasiswa.
d. Halaman Data Alternatif yang menampilkan berbagai data alternatif yang telah diinputkan oleh Admin Sistem. Pada halaman ini Admin Sistem juga dapat menambahkan data, mengedit data, dan menghapus data dalam sistem.
e. Halaman Data Kriteria yang digunakan untuk menampilkan data kriteria yang telah diinputkan oleh Admin Sistem. Perlakuan yang sama juga dapat dilakukan dalam halaman ini, yaitu; Admin Sistem dapat menambahkan data, mengedit data, dan menghapus data.
f. Halaman data nilai menampilkan data nilai yang telah diinputkan oleh admin, pada halaman ini admin dapat mengubah data nilai.
g. Halaman Perhitungan yang menggunakan metode electre menampilkan penilaian mulai dengan:
   - Membentuk Perbandingan Berpasangan (X);
   - Perbandingan Berpasangan Ternormalisasi (R);
   - Menentukan Bobot tiap-tiap Kriteria (W);
   - Membentuk Matrik Preferensi (V);
   - Menentukan Concordance Index (Ckl);
   - Menentukan Discordance Index (Dkl);
   - Membentuk Matriks Concordance (C);
   - Membentuk Matriks Discordance (D);
   - Membentuk Matrik Concordance Dominan(F);
   - Membentuk Matrik Discordance Dominan(G);
   - Membentuk Matrik Agregasi Dominan(E).

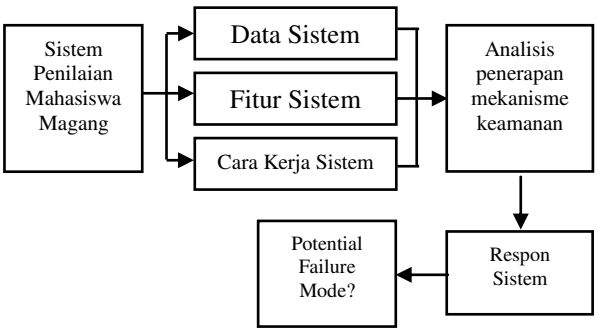
Hasil yang akan ditampilkan adalah nilai akhir dan rangking dari alternatif yang telah dihitung.

h. Halaman Data Nilai Akhir menampilkan data alternatif nilai akhir dan rangking dari alternatif yang telah dihitung.
i. Halaman Data User menampilkan data user yang telah diinputkan oleh admin, pada halaman ini admin dapat menambahkan data, detail data, mengedit data, dan menghapus data.
j. Halaman role user digunakan untuk mengatur *role user,* hak akses pengguna terhadap sistem.

Bagian fitur untuk *delete data* dibagian halaman data mahasiswa, halaman data alternatif, halaman data kriteria, halaman data nilai akan muncul pesan peringatan. Tindakan penghapusan data akan memunculkan peringatan untuk memastikan pengguna akan menghapus data tersebut. Pesan yang ditampilkan sistem adalah "YAKIN DATA INI AKAN DIHAPUS?". Data yang dihapus akan hilang dari *database.*

2. Mode Kegagalan Potensial *(Potential Failure Mode)*

Tahap ini menguraiakan kemungkinan kegagalan potensial yang dapat dialami oleh sistem atas diterapkan atau tidaknya aspek keamanan informasi dalam fitur-fitur sistem. Tahap menguraikan dilakukan terhadap aspek keamanan informasi yang berupa *confidentiality* (kerahasiaan)*, integrity* (integritas)*,* dan *availability* (ketersediaan) dari berbagai jenis informasi yang tersimpan di dalam sistem perusahaan dan respon sistem yang terjadi. Proses ini diilustrasikan dalam Gambar 4 dan daftar kegagalan potensial ada di dalam Tabel 3.



Gambar 4. Proses Menguraikan Kegagalan Potensial Sistem Atas Aspek Keamanan

Tabel 3. Kegagalan Potensial

CIA	Proses Sistem	Data Sistem	Fitur Sistem	Mekanisme Keamanan	Kegagalan potensial
Confidentiality (C)		Data login (email dan password)	Halaman login	Username, password, enkripsi,	-Lupa password -Lupa username
		Data penggun a sistem	Halaman data user	Daftar kontrol akses	-Data user terhapus
	Sistem mampu membedaka n hak akses	Data role access	Halaman role access	Daftar kontrol akses	Kesalahan pemilihan user
			Halaman My Profile	Daftar kontrol akses	-Lupa password lama Menginput kan Password baru tidak sesuai (repeat) Kesalahan input format email
Integrity (I)		Data alternatif	Halaman data alternatif	-Enkripsi data -kontrol akses	-Data terhapus
		Data kriteria	Halaman data kriteria	-Enkripsi data -kontrol akses	-Data terhapus -Kesalahan pilih kriteria
		Data mahasis wa	Halaman data mahasis wa	-Enkripsi data -kontrol akses	-Data terhapus - Kesalahan input format email
		Data nilai	Halaman data nilai	-Enkripsi data -kontrol akses	-Data terhapus -User error dalam melakukan input nilai
		Data perhitun gan dan perangki ngan	Halaman perhitun gan dan perangki ngan	-Enkripsi data -kontrol akses	
		Data nilai akhir	Halaman data nilai akhir	-Enkripsi data -kontrol akses	
Availability (A)	Sistem mampu menyimpan data			Dapat diakses pengguna terdaftar	-Kesalahan sambungan dengan database
	Sistem mampu mengolah data			Dapat diakses pengguna terdaftar	-Kesalahan sambungan dengan database
	Sistem mampu melakukan penghitung an nilai			Dapat diakses pengguna terdaftar	
	Sistem menampilk an nilai akhir dan perangking an			Dapat diakses pengguna terdaftar	

3. Menganalisis Efek Potensial dari Kegagalan *(potential failure)*

Berdasarkan tabel kegagalan potensial dari keterkaitan dengan aspek keamanan tersebut mempunyai damapak atau efek potensial yang ditunjukkan dalam Tabel 4.

Tabel 4. Dampak Potensial

Aspek Keamanan	Kegagalan Potensial	Dampak Potensial
Confidentiality	- Lupa password - Lupa username - Data user terhapus - Kesalahan pemilihan user - Lupa password lama - Menginputkan Password baru tidak sesuai *(repeat)* - Kesalahan input format email	- Gagal akses dashboard sistem - Gagal akses dashboard sistem - Kehilangan akses sistem - Kesalahan pemberian akses user - Gagal memperbaharui data user - Tidak dapat login dan atau mengirimkan informasi
Integrity	- Data terhapus - Kesalahan input data - Kesalahan input format email	- Data tidak valid - Data tidak valid - Tidak dapat mengirimkan informasi
Availability	- Kesalahan sambungan dengan database dan/atau web server	- Data tidak dapat ditampilkan

4. Menentukan *Severity Level* untuk Analisis Resiko

Penilaian *severity* ini menggunakan indeks 1 hingga 10, semakin besar indeks menunjukkan dampak yang ditimbulkan semakin beresiko. Nilai ini diperoleh dengan melakukan wawancara terhadap pengguna sistem penilaian mahasiswa. Nilai *Severity* ditunjukkan dalam Tabel 5.

Tabel 5. Nilai Severity

Aspek Keamanan	Dampak Potensial	Nilai Severity
Confidentiality	- Gagal akses dashboard sistem lupa password/username	8
	- Kehilangan akses sistem	10
	- Kesalahan pemberian akses user	7 4
	- Gagal memperbaharui data user - Tidak dapat login dan atau mengirimkan informasi	9
Integrity	- Data tidak valid	10
	- Tidak dapat mengirimkan informasi	7
Availability	- Data tidak dapat ditampilkan	10

5. Menganalisis Penyebab Potensial *(potential cause)*

Berdasarkan nilai *severity* pada Tabel 5 menunjukkan bahwa dampak potensial yang paling parah atau berbahaya saat terjadi kegagalan sistem mencakup di semua aspek keamanan. Pada aspek *confidientility* dampak yang paling berbahaya adalah kehilangan akses sistem dikarenakan user terhapus.

Dampak yang masih berbahaya berikutnya adalah tidak dapat login dan atau mengirimkan informasi dikarenakan *email* yang diinputkan saat membuat user tidak sesuai format standar email. Gagal akses *dashboard* sistem menajdi dampak berbahaya ketiga yang disebabkan oleh lupa *username* dan *password*. Namun, saat hal ini terjadi sistem masih mengakomodir fitur untuk memulihkan akses kembali dengan fitur *"forgot password"*.

Bagian *Integrity* mempunyai dampak paling berbahaya berupa data tidak valid yang disebabkan oleh kesalahan saat input data maupun karena data tidak sengaja terhapus. Walaupun terdapat peringatan saat akan menghapus data, namun terkadang pengguna mengabaikan peringatan tersebut dan menekan tombol enter. Aspek *Availability* terdapat dampak yang paling berbahaya adalah data tidak dapat ditampilkan yang disebabkan karena sistem tidak dapat tersambung ke database. Hal ini dapat terjadi karena web server lokal belum diaktifkan atau kondisi paling buruk adalah databse terhapus.

6. Menentukan *Occurrence Level* untuk Menilai Probabilitas

Pemberian nilai *Occurrence* berdasarkan pada Tabel 2. Hasil dari *Occurrence Level* disajikan dalam Tabel 6.

Tabel 6. *Occurrence Level*

Dampak Potensial	Indeks	Klasifikasi	Keterangan
Kehilangan akses sistem	10	Sangat Tinggi	Kegagalan yang tak terganti
Tidak dapat login dan atau mengirimkan informasi	9		
Data tidak valid	10		
Data tidak dapat ditampilkan	10		
Gagal akses dashboard sistem lupa password/username	6	Sedang	Kegagalan sesekali
Kesalahan pemberian akses user	6		
Tidak dapat mengirimkan informasi	6		
Gagal memperbaharui data user	4	Rendah	Sedikit kegagalan

7. Menentukan *Detection Level* untuk Pengendalian

Tahap pengendalian ini juga dinilai menggunakan indeks 1 – 10, Semakin sulit penyebab kegagalan dideteksi semakin tinggi nilai indeks. Pemberian nilai ini berdasarkan (Gambino et al., 2018). Hasil *Detection Level* ada di Tabel 7.

Tabel 7. *Detection Level*

Dampak Potensial	Penyebab	Indeks
Kehilangan akses sistem	Data user terhapus	10
Data tidak valid	Kesalahan input data, data terhapus	10
Data tidak dapat ditampilkan	Kesalahan sambungan dengan database dan atau web server	5
Tidak dapat login dan atau mengirimkan informasi	Kesalahan input format email	2
Gagal akses dashboard sistem lupa password/username	Tidak mengingat username atau password	2
Kesalahan pemberian akses user	Kesalahan pemilihan user	4
Tidak dapat mengirimkan informasi	Kesalahan input format email	2
Gagal memperbaharui data user	Password baru yang diinputkan tidak sesuai *(repeat)* dan atau lupa password lama	1

8. Menghitung *Risk Priority Number* (RPN)

Formula untuk menghitung nilai RPN = Severity (S) x Occurrence (O) x Detection (D). Tabel RPN ditunjukkan oleh Tabel 8. Berdasarkan kriteria yang disebutkan dalam (Suryana et al., 2017) pada Tabel 9.

Tabel 8. Hasil *Risk Priority Number*

Dampak Potensial	Severity (S)	Occurrence (O)	Detection (D)	RPN
Kehilangan akses sistem	10	10	10	1000
Data tidak valid	10	9	10	900
Data tidak dapat ditampilkan	10	10	5	200
Tidak dapat login dan atau mengirimkan informasi	7	10	2	140
Gagal akses dashboard sistem lupa password atau username	8	6	2	96
Kesalahan pemberian akses user	7	6	4	168
Tidak dapat mengirimkan informasi	7	6	2	84
Gagal memper-baharui data user	4	4	1	16

Tabel 9. Tabel Kriteria RPN

RPN	Calculation Level
0 - 19	Very Low
20 - 79	Low
80 - 119	Medium
120 - 199	High
=/>200	Very High

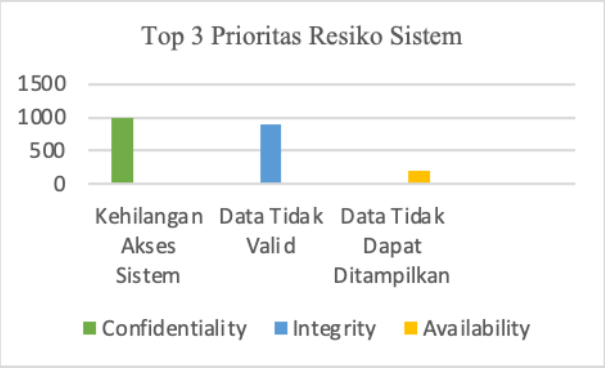
2.9 Membuat Prioritas Resiko

Daftar prioritas resiko dan keterkaitannya dengan aspek keamanan informasi yang ditunjukkan pada Tabel 10 disajikan berdasarkan hasil dari penghitungan nilai RPN *(Risk Priority Number).*

Tabel 10. Prioritas resiko

Resiko Prioritas	RPN	Calculation Level	Aspek Keamanan
Kehilangan akses sistem	1000	Very High	*Confidentiality*
Data tidak valid	900	Very High	*Integrity*
Data tidak dapat ditampilkan	200	Very High	*Availability*
Kesalahan pemberian akses user	168	High	*Confidentiality*
Tidak dapat login dan atau mengirimkan informasi	140	High	*Confidentiality*
Gagal akses dashboard sistem lupa password/username	96	Medium	*Confidentiality*
Tidak dapat mengirimkan informasi	84	Medium	*Integrity*
Gagal memperbaharui data user	16	Very Low	*Confidentiality*

Berdasarkan evaluasi aspek keamanan dari sistem penilaian mahasiswa magang menggunakan metode *Failure Mode and Effect Analysis (FMEA)* diperoleh bahwa dalam sistem tersebut diperoleh 3 prioritas resiko tertinggi mencakup ketiga aspek keamanan informasi. Grafik top 3 dari prioritas resiko tertinggi ditampilkan dalam Gambar 5.



Gambar 5. Grafik Prioritas Resiko

Prioritas resiko paling tinggi terkait dengan aspek *Confidentiality* yang dapat mengakibatkan kehilangan akses sistem karena kehilangan data user yang harus digunakan untuk login ke dalam sistem. Kehilangan data user ini artinya data user telah hilang dari database sistem dan tidak dapat dipulihkan, oleh sebab itu level resikonya berada di rentang *very high.*

Prioritas resiko kedua ada di aspek *integrity* yang berkaitan dengan data tidak valid yang disebabkan oleh kesalahan input data atau data tidak sengaja terhapus oleh user yang sedang mengelola data sistem. Level RPN berada pada tingkat very high. Prioritas resiko ketiga berada dalam dimensi aspek *availability* dengan level RPN *very high* dengan resiko data tidak dapat ditampilkan dikarenakan kesalahan sambungan dengan database dan atau koneksi sistem dengan web server yang tidak aktif.

Tingkat resiko paling rendah berada pada aspek *confidentiality* berupa gagal memperbaharui data user yang disebabkan karena ketidaksesuaian saat menginputkan password baru. Hal ini dikarenakan dalam memperbaharui data user harus memasukkan password baru sebanyak dua kali. Penyebab lain adalah user tidak mengingat password lama. Karena saat akan mengubah data user juga membutuhkan password sebelumnya. Namun, hal ini berada pada level *very low* dikarenakan resiko tersebut bukan permasalahan yang krusial. Saat terjadai kesalahan input password baru, maka dapat memilih alternatif password lain yang mudah diingat. Bahkan, saat tidak mengingat password lama, maka bisa melakukan *logout* sistem dan memanfaatkan fitur *"forgot password"*.

Dalam sistem penilaian mahasiswa magang ini sudah memenuhi aspek keamanan informasi dengan memberikan pembatasan hak akses user, namun keberadaan pembatasan akses sistem ini juga bisa menjadi resiko yang paling prioritas. Oleh sebab itu, disarankan kepada Perusahan Rintasan XY untuk membuat prosedur penggunaan sistem dan mengelola akun untuk akses sistem.

KESIMPULAN

Confidentiality mencakup dimensi kontrol akses dan tindakan yang bertujuan untuk melindungi informasi supaya tidak dimanfaatkan oleh pengguna yang tidak berwenang. Memastikan bahwa data dan informasi di Perusahaan Rintisan XY hanya dapat diakses oleh pengguna yang mempunyai *role access* dan mempunyai *username* serta *password* untuk mengakses sistem penilaian mahasiswa. Sehingga, data mahasiswa, nilai, alternatif dan kriteria tidak dapat dimanipulasi oleh pengguna yang tidak mempunyai *role access*, bagian ini perwujudan dari *availability.* Sehingga, *integrity* data dan informasi Perusahaan XY terjamin dan tidak dapat dimanipulasi oleh pengguna atau user yang tidak mempunyai hak akses. Namun, walaupun Perusahaan XY telah menerapkan mekanisme keamanan tetap dapat mengalami resiko terkait penggunaan sistem penilaian mahasiswa.

Berdasarkan evaluasi menggunakan metode *Failure Mode and Effect Analysis* diperoleh hasil bahwa resiko paling tinggi dengan status *very high* dapat terjadi pada aspek *confidentiality* yang dapat mengakibatkan kehilangan akses sistem karena kehilangan data user yang harus digunakan untuk login ke dalam sistem. Kehilangan data user ini artinya data user telah hilang dari database sistem dan tidak dapat dipulihkan. Prioritas resiko kedua ada di aspek *integrity* yang berkaitan dengan data tidak valid yang disebabkan oleh kesalahan input data atau data tidak sengaja terhapus oleh user yang sedang mengelola data sistem. Prioritas resiko ketiga

berada pada aspek *availability* dengan resiko data tidak dapat ditampilkan dikarenakan kesalahan sambungan dengan database dan atau koneksi sistem dengan web server yang tidak aktif. Prioritas kedua dan ketiga juga bersatus *very high*. Sedangkan, untuk resiko *medium* berupa kemungkinan gagal akses dashboard sistem lupa password atau username. Resiko paling rendah dengan level *very low* berupa resiko gagal memperbaharui data user dengan nilai RPN (*Risk Priority Number)* 16. Penggunaan metode FMEA memberikan hasil dengan level dan kriteria yang jelas karena terdapat batasan-batasan tingkat resiko. Sehingga, Perusahaan XY dapat memfokuskan untuk mengantisipasi resiko yang paling berpotensi dengan cara yang lebih tepat.

REFERENSI

Ava Dianta, I., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking. *Intensif*, *3*(1), 2549–6824.

Gambino, M. A., Ikbal, M., Santoso, M. W., & Sarjono, H. (2018). *Penerapan Failure Mode and Effect Analysis (FMEA) dan Diagram Fishbone Pada Percetakan PT. Pandji Media Gemilang*. Under Graduate Program Management-Binus University Business School. https://bbs.binus.ac.id/management/2018/12/penerapan-failure-mode-and-effect-analysis-fmea-dan-diagram-fishbone-pada-percetakan-pt-pandji-media-gemilang/

Helaluddin, & Wijaya, H. (2019). *Analisis Data Kualitatif: Sebuah Tinjauan Teori & Praktik*. Sekolah Tinggi Theologia Jaffray.

Jumardi, R. (2018). Kajian Kebijakan Keamanan Sistem Informasi Sebagai Bentuk Perlindungan Kerahasiaan Pribadi Karyawan Perusahaan XYZ. *JSAI (Journal Scientific and Applied Informatics)*, *1*(1), 13–17. https://doi.org/10.36085/jsai.v1i1.8

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81.https://doi.org/10.14421/csecurity.2019.2.2.1625

Komalasari, N. (2020). Sistem Pendukung Keputusan Kelaikan Terbang (SPK2T). *Jurnal Industri Elektro Dan Penerbangan 4 (1)*, *4*(1), 1–11. https://scholar.google.com/scholar?oi=bibs&cluster=5738099113658044 04&btnI=1&hl=id&authuser=1

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.

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Saputra, H. M. J., Sinambela, B. S., Awal, R. J., & Fiqar, T. P. (2020). Kebijakan-Kebijakan Iso 17799 Pada Organisasi Sebagai Manajemen Sistem Keamanan Informasi. *DoubleClick: Journal of Computer and Information Technology*, *3*(2), 67–74.

Subektiningsih, Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, *7*(3), 294–304. https://doi.org/10.17781/p002463

Subektiningsih, Renaldi, & Ferdiansyah, P. (2022). Analisis Perbandingan Parameter QoS Standar TIPHON Pada Jaringan Nirkabel Dalam Penerapan Metode PCQ. *Explore*, *12*(1), 57–63.

Sudjiman, P. E., & Sudjiman, L. S. (2018). Analisis sistem Informasi Manajemen Berbasis Komputer Dalam Proses Pengambilan Keputusan. *Jurnal Teknologi Informasi Dan Komunikasi (TelKa)*, *8*(2), 55–67.

Suryana, D. Y., Vinolia, & Ibrahim, A. (2017). Evaluasi Celah Keamanan Sistem Webserver Dengan Metode Failure Mode And Effects Analysis. *Prosiding Annual Research Seminar*, *3*(1), 1–4.

Tiorentap, D. R. A., & Hosizah, H. (2020). Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP. *Prosiding 4 SENWODIPA*, *November*, 53–66.https://prosiding.esaunggul.ac.id/index.php/FHIR/article/view/71

Triandi, B. (2019). Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0. *JURIKOM (Jurnal Riset Komputer)*, *6*(5),477483.http://ejurnal.stmikbudidarma.ac.id/index.php/jurikom/article/view/1556

Wowor, N. E., Sentinuwo, S. R., & Karouw, S. D. S. (2018). Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks Kami. *Jurnal Teknik Informatika*, *13*(3), 1–10.

Yampolskiy, M., Gatlin, J., & Yung, M. (2021). Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. *AMSec 2021 - Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, Co-Located with CCS 2021*, 3–9. https://doi.org/10.1145/3462223.3485618

Zakariah, A. M., Afriani, V., & Zakariah, M. K. (n.d.). *Metodologi Penelitian Kuantitatif, Kualitatif, Action Research, Research and Development (R and D)*. Yayasan Pondok Pesantren Al-Mawaddah Warrahmah.