Journal of Information Technology and Computer Science (INTECOMS)
Volume 6 Nomor 2, Desember 2023
e-ISSN : 2614-1574
p-ISSN : 2621-3249

ANALISIS KEAMANAN SISTEM INFORMASI RECRUITMENT MENGGUNAKAN METODE FAILURE MODE AND EFFECT ANALYSIS (FMEA) STUDI KASUS PT ABC

ANALYSIS OF RECRUITMENT INFORMATION SYSTEM SECURITY USING FAILURE MODE AND EFFECT ANALYSIS (FMEA) METHOD CASE STUDY PT ABC

Felix Wuryo Handono[1], Syaiful Anwar[2], Fernando B Siahaan[3]
[1,2,3]Universitas Bina Sarana Informatika
felix@bsi.ac.id

ABSTRACT

As technology develops, now many activities are starting to use automated systems to make work easier. One of them is a recruitment application system that was created with the aim of facilitating work. Then the problem that arises is whether the system that has been created is safe enough so that it does not have a negative impact. Information System security analysis uses the FMEA (Failure Mode And Effect Analysis) method. From the results of the analysis it was found that the recruitment system still has a very large gap that can disrupt services to the point of data leakage which can be detrimental to the company.

Keywords: *Information Security System, FMEA Method, Security System Analysis*

ABSTRAK

Seiring berkembangnya teknologi, kini banyak kegiatan yang mulai menggunakan sistem otomatis untuk dapat mempermudah pekerjaan. Salah satunya sistem aplikasi recruitment yang dibuat dengan tujuan mempermudah pekerjaan. Kemudian masalah yang muncul adalah apakah sistem yang telah dibuat sudah cukup aman sehingga tidak memiliki dampak kerugian. Analisis keamanan Sistem Informasi menggunakan metode FMEA (Failure Mode And Effect Analysis). Dari hasil analisis didapat bahwa system recruitment masih memiliki celah yang sangat besar hingga dapat mengganggu layanan sampai pada kebocoran data yang dapat merugikan perusahan.

Kata Kunci: Sistem Keamanan Informasi, Metode FMEA, Analisa Sistem Keamanan

PENDAHULUAN

Seiring berkembangnya teknologi, kini banyak kegiatan yang mulai menggunakan sistem otomatis untuk dapat mempermudah pekerjaan. PT. ABC merupakan perusahaan yang berkembang di bidang sumber daya manusia dengan salah satu program yang mengirimkan pemagang ke Jepang. Saat ini PT. ABC telah berhasil mengirimkan program pemagangan di hampir semua bidang lebih dari 1000 setiap tahunnya (atau sekitar 100 pemagang setiap bulannya) dengan jumlah pemagang di Jepang lebih dari 2000 orang.

Untuk mempermudah proses recruitment tentu saja PT ABC membangun sebuah sistem informasi yang bisa membantu fleksibilitas pencarian pemagang yang sesuai. Tentu saja, membangun sistem ini masih membutuhkan keamanan informasi untuk melindungi dari penyalahgunaan sumber daya informasi oleh orang yang tidak berwenang.

Sistem informasi adalah alat untuk menyajikan informasi dengan cara yang berguna bagi penerimanya, Kertahadi dalam ((Sutiyono & Santi, 2020) Tujuannya adalah untuk memberikan informasi dalam perencanaan, memulai, pengorganisasian, operasional sebuah perusahaan yang melayani sinergi organisasi dalam proses mengendalikan pengambilan keputusan (Dini, 2015)

Dalam sebuah sistem informasi tentunya sangat diperlukan sebuah perlindungan yang dapat menjamin sumber daya informasi tetap aman dari

penyalahguanan pihak yang tidak berwenang. Sistem ini disebut dengan keamanan informasi.

Keamanan informasi mengacu pada proses dan metode yang dirancang dan diterapkan untuk melindungi informasi elektronik atau bentuk lain dari data rahasia, pribadi, dan sensitif dari akses, penyalahgunaan, pengungkapan, penghancuran, pengubahan, dan manipulasi yang tidak sah. (Boi, 2021)

Keamanan informasi merupakan hal yang sangat penting untuk diperhatikan. Selain itu, diperlukan penerapan manajemen TI dan analisis keamanan informasi secara berkala.

Maka setelah system informasi rekrutmen dibangun, permasalahan yang muncul adalah apakah system yang dibangun sudah cukup aman dalam memberikan layanan dari masalah yang dapat menimbulkan kebocoran data sampai dengan kerugian bagi perusahaan.

Salah satu cara untuk melakukan analisis keamanan informasi terhadap sumber daya informasi adalah dengan menggunakan metode Failure Mode and Effects Analysis (FMEA). Metodologi FMEA adalah teknik untuk mengevaluasi cacat yang terjadi pada sistem, desain, proses, maupun layanan. Menurut Ford Motor Company (Elbert et al., 2019). Memprioritaskan bentuk kesalahan memerlukan pendefinisian keparahan, kejadian, dan deteksi, dan hasil akhirnya adalah nomor prioritas risiko.

Berdasarkan informasi pada latar belakang, maka penulis tertarik membuat topik penelitian dengan judul "Analisis Keamanan Sistem Informasi Rekrutmen Menggunakan Metode Studi Kasus Failure Modes and Effects Analysis (FMEA) PT ABC". Topik penelitian ini didukung oleh penelitian dan pengambilan sumber-sumber yang mendasari topik tersebut. Penelitian sebelumnya di buku, internet, dan jurnal penelitian sebelumnya

METODE

Metode penelitian pada dasarnya adalah cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Atas dasar hal tersebut terdapat empat kata kunci yang perlu diperhatikan, cara ilmiah, data, tujuan dan kegunaan, (Sugiyono, 2017).

Metode penilaian Risiko menggunakan Metode Failure Mode And Effect Analysis(FMEA). FMEA adalah sebuah metode evaluasi kemungkinan terjadinya sebuah kegagalan dari sebuah sistem, desain, proses atau servis untuk dibuat langkah penanganannya, Yumaida dalam (Andiyanto et al., 2017). Dalam FMEA, setiap kemungkinan kegagalan yang terjadi dikuantifikasi untuk dibuat prioritas penanganan.

Dalam penelitian ini FMEA dilakukan untuk melihat risiko-risiko yang mungkin terjadi Tentang sistem keamanan informasi perekrutan operasional perusahaan. Dalam hal ini, tiga hal dapat membantu menentukan kegagalan:

- Tingkat Kejadian (Occurance)
  Dalam menentukan kejadian ini, Anda dapat menentukan seberapa parah gangguan terhadap pekerjaan pemeliharaan dan aktivitas operasional pabrik Anda.
- Jumlah Keparahan (Severity)
  Dalam perhitungan jumlah kerusakan (severity), dapat dinilai seberapa serius kerusakan akibat terjadinya cacat proses pada pemeliharaan dan pengoperasian pabrik.
- Tingkat Deteksi (Detection)
  Dalam menentukan tingkat deteksi ini, Anda dapat menentukan bagaimana kesalahan terdeteksi sebelum terjadi. Laju deteksi juga dipengaruhi oleh jumlah kontrol yang mengontrol aliran proses. Semakin banyak kontrol dan prosedur yang mengatur operasi sistem pemrosesan pemeliharaan dan aktivitas operasional, semakin tinggi cakupan atas kesalahan yang diharapkan.

Tabel 1. Klasifikasi Level Risiko

No	Level	Nilai RPN
1	Very Low	0 – 20

2	Low	21 – 80
3	Moderate	81 – 120
4	High	121 – 199
5	Very High	Lebih dari 200

Sumber : ditulis miring dan ukuran 9

Dalam metode penelitian ini juga dilakukan pengumpulan data, yang merupakan hasil penelitian dari mempelajari dan mengamati secara langsung sistem keamanan pada PT. ABC. Penulis juga mengembangkan penelitian yang berkaitan dengan analisis juga manajemen risiko, keamanan informasi teknologi informasi dan analisis manajemen menggunakan mode kegagalan dan teknik analisis dampak (FMEA).

Teknik pengumpulan data dipandang sebagai langkah strategis dalam penelitian karena tujuan utamanya adalah mengumpulkan informasi. (Sugiyono, 2017)

Teknik pengumpulan data dilakukan dengan tiga cara, yaitu:

1. Studi literatur oleh Danial dan Warsiah dalam (Yusuf Abdhul, 2023), merupakan penelitian yang dilakukan oleh peneliti dengan mengumpulkan sejumlah buku maupun majalah yang berkaitan dengan masalah serta tujuan penelitian. Dalam proses ini semua teori dikumpulkan sesuai dengan topik "Keamanan Sistem Informasi dengan Metode FMEA".
2. Pengamatan langsung merupakan cara untuk mendapatkan data secara aktual yang terjadi di lapangan, untuk mengetahui masalah yang terjadi serta faktor-faktor yang menyebabkan masalah itu terjadi sehingga peneliti akan mudah dalam memetakan langkah perbaikan yang akan dilakukan (Supriyadi & Oktaviani, 2021).
3. Wawancara, menurut Esterberg dalam (Sugiyono, 2017) wawancara adalah pertemuan dua orang yang saling bertukar informasi dan ide melalui tanggung jawab, sehingga dapat dikontruksikan makna dalam suatu topik tertentu.

Selanjutnya penulis juga melakukan proses identifikasi aset teknologi informasi yang berguna untuk proses penelitian. Identifikasi risiko merupakan suatu proses yang secara sistematis dan terus menerus dilakukan untuk mengidentifikasi kemungkinan timbulnya risiko atau kerugian terhadap kekayaan, hutang, dan personil perusahaan. Proses identifikasi risiko ini bisa menjadi proses yang terpenting, karena dari proses inilah, semua risiko yang ada atau yang mungkin terjadi pada suatu proyek, dapat diidentifikasi (Darmawi, 2008)

Proses identifikasi harus dilakukan secara cermat dan komprehensif, agar mengurangi risiko yang terlewatkan atau tidak teridentifikasi (Darmawi, 2008). Proses identifikasi ini dilakukan sebelum tahap penilaian risiko untuk mendapatkan daftar aset TI dengan risiko keamanan informasi yang lebih tinggi di PT ABC.

Menurut Ford Motor Company (1992) untuk menentukan prioritas dari kegagalan maka harus mendefinisikan apa itu Severity, Occurence, Detection, serta hasil akhirnya yang berupa Risk Priority Number (RPN). Dengan pencarian penyebab kegagalan komponen sesuai dengan level sistem, item-item khusus kritis dapat dinilai dan tindakan-tindakan perbaikan diperlukan untuk memperbaiki desain dan mereduksi probabilitas dari mode-mode kegagalan yang kritis. Dalam FMEA, dapat dilakukan perhitungan Risk Priority Number (RPN) untuk menentukan tingkat kegagalan tertinggi, Kim & Zuo dalam (Widya Wardana & Hasanah, 2019). RPN adalah produk matematis dari keseriusan effect (severity), kemungkinan terjadinya kegagalan yang berhubungan dengan effect (occurrence), dan kemampuan untuk mendeteksi kegagalan sebelum terjadi (detection) (Irianto, 2010)

HASIL DAN PEMBAHASAN

Sebelum melakukan perbaikan penulis melakukan analis risiko terlebih dahulu. Analisis risiko didefinisikan sebagai sebuah proses yang

menggabungkan ketidakpastian dalam bentuk kuantitatif, menggunakan teori probabilitas, untuk mengevaluasi dampak potensial suatu risiko (Al-Bahar & Crandall, 1990).

Penulis menganalisis risiko ancaman gangguan sistem informasi menggunakan metode FMEA. Penemuan nilai informasi ditentukan dari beberapa komponen yang mendukung operasional, antara lain SDM (Sumber Daya Manusia), perangkat keras dan lunak, jaringan juga data di perusahaan tidak terkait.

Analisa risiko menggunakan metode Failure Mode And Effect Analysis (FMEA), yaitu metode terstruktur untuk mendeteksi dan menghindari atau meminimalisir masalah yang ada dan mengevaluasi gangguan. Adapun kategori penilaian terhadap tingkat keparahan, frekuensi dan deteksi dari setiap resiko menggunakan tabel Parameter Failure Modes and Effects Analysis (FMEA). Parameter kriteria untuk Severity, Occurrence dan Detection ditunjukkan pada tabel di bawah ini.

Tabel 2. Tingkat Keparahan

No	Effect	Criteria: Severity of Effect	Ranking
1	Dangerous without warning	System failure will have dangerous effects without warning	10
2	Dangerous with warning	A system failure will have a dangerous effect with prior warning	9
3	Very High	All support systems will not function. The system can operate but not optimally	8
4	High	The system can operate but not optimally.	7
5	Moderate	The system is operational and safe but has decreased performance	6
6	Low	The system is operational and safe but has decreased performance.	5
7	Very_Low	The system experiences a gradual decline in performance.	4
8	Small	Little effect on system performance	3
9	Very small	Negligible effect on system performance	2
10	There is no effect	The effect of failure will not occur on the system.	1

Sumber : (Triana & Pangabean, 2021)

Tabel 3. Tingkat Kejadian

No	Probability of Failure	Time Period	Ranking
1	Very High: Failure is almost inevitable	More than once per day	10
		5 times in a day	9
2	Height: Failure occasionally occurs	Once every week	8
		2 times a week	7
3	Medium: Failures occur occasionally but not in large numbers	6 times in a month	6
		3 times in a month	5
		2 times in a month	4
4	Low Failures that occur are relatively small	Once a month	3
5	Very rarely: Failures that occur are relatively small and rare	Once every 3 months	2
6	Remote: Failure never occurs	Once Every 6 monhs	1

Sumber : (Triana & Pangabean, 2021)

Tabel 4. Tingkat Deteksi

No	Detection	Criteria: Likelihood the existence of a defect will be detected by process controls before next (subsequent) process, or before exposure to client	Ranking
1	Almost Impossible	There is currently no control capability that can detect failure	10
2	Very rare	Current control capabilities are very difficult to detect the cause of failure	9
3	Rare	Current control capabilities are difficult to detect the cause of failure	8
4	Very Low	The current control capability to detect the cause of failure is very low	7
5	Low	The current control ability to detect causes of failure is low	6
6	Moderate	Current control capability to detect causes of failure is moderate	5
7	Somewhat high	Current control capability to detect causes of failure is moderate to high.	4
8	High	Current control capability to detect causes of failure is high	3
9	Very High	The current control capability to detect the cause of failure is very high	2
10	Almost Certain	Current controllability can almost certainly detect causes and prevent failures	1

Sumber : (Triana & Pangabean, 2021)

Berikut tahapan identifikasi dan evaluasi keamanan (Penilaian Resiko) sistem informasi dengan menggunakan metode Failure Modes and Effects Analysis

(FMEA). Pada tahap ini yang dilakukan ialah mengidentifikasi masalah dan penilaian resiko severity, occurrence dan detection dari tiap indicator masalah:

Tabel 5. Penilaian Resiko

No	Process Step/Input	Potential Failure Mode	Potential Failure Effects	Potential Causes	Current Controls	S	O	D	RPN
1	Login Aplikasi	Salah input username & password	Muncul bug/error report pada program yang dapat dimanfaatkan oleh hacker	Input field dengan karakter tertentu atau injeksi	Pengecekkan dokumentasi source code pada form login	7	10	10	700
2	Login Aplikasi	Salah input username & password	Muncul bug/error report pada program yang dapat dimanfaatkan oleh hacker	Input field dengan karakter tertentu atau injeksi	Pengecekkan dokumentasi source code pada form login	7	10	10	700
3	Login Aplikasi	Salah input username & password	Mendapatkan data pribadi maupun internal perusahaan	Input field dengan karakter tertentu atau injeksi	Pengecekkan tabel user pada database	10	5	8	400
4	Login Aplikasi	Salah input username & password	Menghapus database perusahaan	Input field dengan karakter tertentu atau injeksi	Pengecekkan tabel user pada database	10	5	8	400
5	Login Aplikasi	Menggunakan password yang sama dalam kurun waktu yang panjang	Password akan mudah dikenali	Tidak mengganti password secara berkala	Pengecekan log login user	10	5	7	350
6	Login Aplikasi	Melakukan login berulang tanpa pembatasan jumlah gagal	Melakukan login berulang secara robot	Tidak membatasi jumlah kegagalan login	Pengecekan log login user	10	8	7	560
7	Input Text pada Modul Input	Menggunakan karakter khusus	Muncul bug/error report pada program yang membuat aplikasi tidak dapat digunakan dan celah tersebut dapat dimanfaatkan oleh hacker	Input field dengan karakter tertentu atau injeksi	Pengecekan dokumentasi source code pada form Modul input	8	6	8	384
8	Input Dokumen (Pdf, Jpeg, Png)	Input file yang tidak sesuai ketentuan	Aplikasi tidak bisa diakses / Error	Input Dokumen dengan file format tertentu	Pengecekkan dokumentasi source code pada Modul input dokumen	8	6	8	384
9	Import Dokumen (Excel)	Import Dokumen Excel mengandung Macro	Aplikasi Terinfeksi Virus dan tidak dapat digunakan	Import Dokumen Excel Tanpa Scanning	Pengecekkan dokumentasi source code pada Modul Import Dokumen	8	6	8	384
10	Database Slow Process	Waktu proses query > 3 detik	Akses Aplikasi menjadi Lambat	Query untuk mengakses database tidak teroptimalisasi dengan baik	Pengecekan slow queries	3	10	7	210
11	Database Slow Process	Waktu proses query > 3 detik	Akses Aplikasi menjadi Lambat	Query untuk mengakses database tidak teroptimalisasi dengan baik	Standar dalam pembuatan Query ke Database yang teroptimalisasi	3	10	7	210
12	Database Failure	Database Corrupt	Aplikasi tidak bisa diakses / Error	Virus	Antivirus	8	6	6	288
13	Database Failure	Database Corrupt	Aplikasi tidak bisa diakses / Error	Injection Query	Access List	8	6	6	288
14	Database Failure	Database Corrupt	Aplikasi tidak bisa diakses / Error	Injection Query	Web Application Firewall	8	6	6	288
15	Database Failure	Database Corrupt	Aplikasi tidak bisa diakses / Error	Injection Query	Replikasi database	8	6	6	288

Sumber : Hasil Penelitian

Dari hasil pengurutan RPN didapatkan proses Login Aplikasi mempunyai urutan RPN (Risk Priority Number) tertinggi yaitu 3300, dapat disimpulkan bahwa tahap login merupakan proses yang paling penting dan memiliki tingkat kegagalan tinggi dalam penginputan informasi recruitment. Sedangkan proses database failure mempunyai urutan tertinggi kedua yaitu 1152, yang bisa terbilang cukup parah, karena pada proses ini semua data akan tersimpan dan akan fatal jika masih terdapat eror di dalam sistem.

Dampak ditimbulkan oleh kedua proses ini sangat berpengaruh besar terhadap sistem informasi recruitment, yang menandakan bahwa keamanan sistem informasi di PT. ABC terdapat mode kegagalan yang harus dilakukan perbaikan. Berdasarkan analisis RPN sebelumnya, proses Login Aplikasi mempunyai urutan RPN tertinggi yaitu 3300, dan RPN terendah ada pada proses database slow process dengan nilai 210. Dapat disimpulkan bahwa angka tersebut masih ternilai tinggi dan memerlukan perbaikan

SIMPULAN

Berdasar hasil pengolahan data dan analisa menggunakan metode FMEA, penulis mendapat kesimpulan bahwa sistem recruitment yang digunakan oleh PT ABC masih memiliki sistem keamanan yang sangat rendah dan rentan terjadi error yang akan berdampak pada proses recruitment. Terbukti dari hasil nilai RPN yang relatif sangat tinggi, hal itu terjadi dari awal proses input username & password hingga database untuk penyimpanan data para pelamar yang sangat membahayakan bagi pelamar, maupun perusahaan.

Perlu segera dilakukan perbaikan pada sistem informasi recruitment berdasarkan hasil penelitian manajemen resiko dengan melakukan skala prioritas pada nilai RPN tertinggi hingga terendah

DAFTAR PUSTAKA

Al-Bahar, J. F., & Crandall, K. C. (1990). Systematic risk management approach for construction projects. *Journal of Management and Engineering ASCE* , *3*, 533–546.

Andiyanto, S., Sutrisno, A., & Punuhsingon, C. (2017). Penerapan

Metode Fmea (Failure Mode And Effect Analysis) Untuk Kuantifikasi Dan Pencegahan Resiko Akibat Terjadinya Lean Waste. 45–57. https://ejournal.unsrat.ac.id/index.php/poros/article/view/14864

Boi, A. (2021, March 23). *Cyber-Security:* Apa yang perlu diketahui untuk memastikan keamanan sistem komputer dan mencegah serangan. Florence. https://liberalforum-eu.translate.goog/2021/03/digitising-europe-cyber-security-what-to-know-to-ensure-the-security-of-computer-systems-and-prevent-attacks/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

Darmawi, H. (2008). *Manajemen Risiko*. Bumi Aksara.

Dini. (2015, November 7). *14 Pengertian Sistem Informasi Menurut Para Ahli*. Dosenit.Com. https://dosenit.com/kuliah-it/sistem-informasi/pengertian-sistem-informasi-menurut-para-ahli

Elbert, J., Setyawan, A. B., & Widjaja S, S. B. (2019). Pengendalian Kualitas Menggunakan Metode Fmea (Failure Mode And Effect Analysis) Di Pt. Asia Mandiri Lines Surabaya. *Jurnal Ilmiah Mahasiswa Universitas Surabaya*, *7*, 2570–2583.

Irianto, D. (2010). Failure Mode & Effect Analysis. *Manufacturing Systems Research Group ITB.*

Sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Alfabeta, CV.

Supriyadi, E., & Oktaviani, H. (2021). *Analysis Of Rtrto60k16 Pkx Yarn Production Process With Objective Matrix (Omax) Method*. 59–67.

Sutiyono, & Santi. (2020). MEMBANGUN Sistem Informasi Pendaftaran Siswa Baruberbasis Webdengan Metode Mdd (Model Driven Development) Di Raudhatul Athfal Nahjussalam. *Jurnal Sistem Informasi, J-SIKA*, *2*, 50–56. https://ejournal.unibba.ac.id/index.php/j-sika/article/view/284/244

Triana, Y. S., & Pangabean, R. A. M. (2021). Risk Analysis in the Application of Financore Information Systems Using FMEA Method. *Journal of Physics: Conference Series*, *1751*(1). https://doi.org/10.1088/1742-6596/1751/1/012032

Widya Wardana, M., & Hasanah, S. (2019). Penerapan Metode Failure Mode And Effect Analysis (Fmea) Dalam Mengidentifikasi Masalah Kerusakan Produk Pakan Ayam Pada Pt. Japfa Comfeed Indonesia, Tbk Unit Lampung.

Yusuf Abdhul. (2023). *7 Tahapan Penelitian yang Wajib Kamu Ketahui*. Https://Deepublishstore.Com/Blog/Tahapan-Penelitian/.