



Analisis Risiko Keamanan pada Sistem Managed Print Services (MPS) menggunakan Metode Failure Modes and Effects Analysis di PT Pertamina Patra Niaga RU III Plaju

Eqqy Adelia, Imamulhakim Syahid Putra

Sistem Informasi, Sains dan Teknologi, UIN Raden Fatah Palembang

eqqyadelia07@gmail.com, imamulhakim_uin@radenfatah.ac.id

Abstrak

Managed Print Services merupakan sistem yang digunakan untuk mendukung pengelolaan pencetakan dokumen secara terpusat melalui mekanisme Secure Print dan autentikasi pengguna. Dalam penerapannya di PT Pertamina Patra Niaga RU III Plaju, masih terdapat potensi risiko yang dapat memengaruhi keamanan dan keberlangsungan proses pencetakan. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan menentukan prioritas risiko keamanan pada sistem MPS serta memberikan rekomendasi mitigasi berdasarkan tingkat risikonya. Penelitian menggunakan pendekatan deskriptif dengan metode Failure Modes and Effects Analysis. Data diperoleh melalui observasi, wawancara, dokumentasi, dan kuesioner penilaian Severity, Occurrence, dan Detection. Penilaian Severity dan Occurrence melibatkan 50 pengguna MPS, sedangkan penilaian Detection dilakukan oleh 2 teknisi MPS. Hasil penelitian mengidentifikasi 12 failure mode dengan nilai Risk Priority Number yang berbeda. Tiga risiko dengan prioritas tertinggi adalah belum adanya autentikasi sidik jari setelah tapping ID Card dengan RPN 162,13, belum adanya monitoring penggunaan kertas harian dengan RPN 155,32, dan ID Card yang dipinjamkan kepada pegawai lain dengan RPN 148,94. Berdasarkan klasifikasi risiko, terdapat 3 risiko tinggi, 7 risiko sedang, dan 2 risiko rendah. Rekomendasi mitigasi meliputi penerapan autentikasi dua tahap menggunakan ID Card dan sidik jari, penerapan monitoring penggunaan kertas harian, penguatan pengendalian penggunaan ID Card, serta pemeliharaan berkala terhadap infrastruktur MPS. Hasil penelitian menunjukkan bahwa metode FMEA dapat digunakan untuk menentukan prioritas risiko keamanan dan menjadi dasar dalam penyusunan tindakan mitigasi pada sistem MPS.

Kata kunci : Managed Print Services, Risiko keamanan, Failure Modes and Effects Analysis, Risk Priority Number.

Abstract

Managed Print Services is a system used to support centralized document printing management through Secure Print mechanisms and user authentication. In its implementation at PT Pertamina Patra Niaga RU III Plaju, several potential risks may affect the security and continuity of the printing process. This study aims to identify, analyze, and prioritize security risks in the MPS system and provide mitigation recommendations based on their risk levels. This study employed a descriptive approach using the Failure Modes and Effects Analysis method. Data were collected through observation, interviews, documentation, and questionnaires assessing Severity, Occurrence, and Detection. Severity and Occurrence assessments involved 50 MPS users, while Detection assessments were conducted by 2 MPS technicians. The results identified 12 failure modes with different Risk Priority Number values. The three highest-priority risks were the absence of fingerprint authentication after ID Card tapping with an RPN of 162.13, the absence of daily paper usage monitoring with an RPN of 155.32, and ID Cards being lent to other employees with an RPN of 148.94. Based on the risk classification, there were 3 high-risk, 7 medium-risk, and 2 low-risk failure modes. The proposed mitigation measures include implementing two-stage authentication using an ID Card and fingerprint, implementing daily paper usage monitoring, strengthening ID Card access control, and conducting periodic maintenance of MPS infrastructure. The results indicate that FMEA can be used to prioritize security risks and provide a basis for developing mitigation measures in the MPS system.

Keywords: Managed Print Services, Security Risk, Failure Modes and Effects Analysis, Risk Priority Number.

1. Pendahuluan

Perkembangan teknologi informasi mendorong organisasi untuk mengintegrasikan teknologi digital dalam mendukung proses bisnis agar lebih efektif, efisien, dan terintegrasi. Peningkatan ketergantungan terhadap teknologi informasi juga menyebabkan organisasi menghadapi berbagai risiko yang dapat memengaruhi keberlangsungan operasional apabila tidak dikelola dengan baik (Virgiawan et al., 2025). Keamanan informasi

menjadi bagian penting dalam pengelolaan teknologi informasi karena berkaitan dengan perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi (International Organization for Standardization, 2022a). Risiko keamanan informasi dapat berasal dari faktor manusia, perangkat keras, perangkat lunak, jaringan, maupun prosedur operasional sehingga diperlukan proses identifikasi dan pengendalian risiko secara sistematis (International Organization for Standardization, 2018; International Organization for Standardization, 2022b).

Salah satu penerapan teknologi informasi yang mendukung kegiatan operasional organisasi adalah Managed Print Services. MPS merupakan layanan pengelolaan pencetakan yang mengintegrasikan perangkat printer, perangkat lunak, jaringan, dan server untuk mendukung pengelolaan proses pencetakan secara terpusat (Quocirca, 2024). Penerapan MPS dapat membantu organisasi mengendalikan penggunaan perangkat, mengelola biaya pencetakan, serta memperoleh informasi mengenai aktivitas dan penggunaan perangkat pencetakan (Quocirca, 2024). Selain aspek efisiensi, keamanan lingkungan pencetakan juga perlu diperhatikan karena dokumen yang dicetak dapat mengandung informasi penting dan berpotensi diakses oleh pihak yang tidak berwenang apabila mekanisme pengamanan tidak memadai (Quocirca, 2024). Kondisi tersebut menunjukkan bahwa pengelolaan MPS tidak hanya berkaitan dengan ketersediaan perangkat pencetakan, tetapi juga mencakup pengendalian keamanan terhadap dokumen, pengguna, dan infrastruktur yang mendukung proses pencetakan.

Perhatian terhadap keamanan pencetakan semakin meningkat seiring dengan berkembangnya ancaman terhadap infrastruktur pencetakan organisasi. Quocirca (2024) melaporkan bahwa 67% organisasi yang menjadi responden mengalami kehilangan data akibat praktik pencetakan yang tidak aman dalam satu tahun terakhir. Selain itu, hanya sebagian kecil pengambil keputusan teknologi informasi yang menyatakan sepenuhnya yakin terhadap keamanan infrastruktur pencetakan organisasinya (Quocirca, 2024). Keamanan juga menjadi salah satu prioritas utama dalam pengelolaan MPS, bersama dengan pembaruan perangkat keras dan pengembangan solusi alur kerja (Quocirca, 2024). Hal tersebut menunjukkan bahwa sistem pencetakan perlu dipandang sebagai bagian dari lingkungan teknologi informasi yang memiliki risiko keamanan dan membutuhkan pengendalian secara berkelanjutan. Perangkat printer yang terhubung ke jaringan juga dapat menjadi bagian dari permukaan risiko keamanan karena memiliki sistem operasi, aplikasi, dan antarmuka jaringan yang dapat menghadirkan potensi kerentanan apabila tidak dikelola dengan baik (Pan et al., 2024).

PT Pertamina Patra Niaga RU III Plaju telah menerapkan Sistem Managed Print Services pada Fungsi IT sebagai layanan pencetakan dokumen secara terpusat. Berdasarkan hasil observasi selama pelaksanaan kerja praktik, sistem MPS menggunakan perangkat lunak Kofax dalam pengelolaan aktivitas pencetakan, sedangkan proses pencetakan dilakukan melalui Control Print dan autentikasi menggunakan ID Card pada perangkat printer. Dokumen yang dikirim dari komputer pengguna disimpan terlebih dahulu pada print queue dan baru dapat dicetak setelah pengguna melakukan autentikasi pada printer. Sistem juga menyediakan pemantauan terhadap kondisi perangkat, seperti status printer dan kapasitas tinta. Berdasarkan data yang diperoleh dari Fungsi IT, terdapat 50 pegawai yang memiliki akses dan menggunakan Sistem MPS dalam kegiatan operasional perusahaan.

Meskipun telah memiliki mekanisme autentikasi dan monitoring, hasil observasi dan wawancara menunjukkan masih terdapat beberapa kondisi yang berpotensi menimbulkan risiko keamanan. Mekanisme autentikasi masih menggunakan ID Card sebagai media verifikasi sehingga terdapat potensi penyalahgunaan apabila kartu dipinjamkan atau digunakan oleh pihak lain. Kondisi tersebut dapat menyebabkan dokumen yang tersimpan dalam print queue dicetak oleh pengguna yang tidak berhak. Selain itu, monitoring yang tersedia lebih berfokus pada kondisi perangkat dibandingkan pemantauan penggunaan pencetakan secara harian, sehingga pengendalian terhadap penggunaan kertas dan aktivitas pencetakan masih memiliki keterbatasan. Risiko pada lingkungan pencetakan juga dapat berkaitan dengan infrastruktur jaringan, server, printer, serta proses operasional yang dapat memengaruhi keamanan maupun ketersediaan layanan (Quocirca, 2024).

Permasalahan tersebut menunjukkan bahwa identifikasi risiko perlu dilakukan secara sistematis untuk mengetahui bentuk kegagalan, penyebab, dampak, serta prioritas penanganannya. Failure Modes and Effects Analysis (FMEA) merupakan metode yang dapat digunakan untuk mengidentifikasi berbagai kemungkinan kegagalan dan menganalisis dampaknya berdasarkan parameter Severity, Occurrence, dan Detection (International Electrotechnical Commission, 2018). Ketiga parameter tersebut digunakan untuk menghitung Risk Priority Number yang dapat membantu menentukan prioritas risiko berdasarkan tingkat kepentingannya (International Electrotechnical Commission, 2018). Pendekatan berbasis FMEA juga dapat digunakan dalam pengelolaan risiko keamanan informasi untuk membantu organisasi menentukan risiko yang memerlukan perhatian dan tindakan pengendalian lebih lanjut (Harjian et al., 2025).

Penerapan FMEA dalam analisis keamanan sistem informasi telah dilakukan dalam beberapa penelitian. Ajrina et al. (2025) menggunakan FMEA yang dikombinasikan dengan ISO/IEC 27001 untuk menganalisis risiko keamanan pada sistem informasi pelayanan pelanggan dan menentukan prioritas risiko berdasarkan nilai RPN. Penelitian tersebut menunjukkan bahwa FMEA dapat digunakan untuk mengidentifikasi berbagai potensi risiko keamanan dan menentukan tindakan mitigasi yang sesuai. Penelitian Saputri et al. (2024) juga menerapkan FMEA dalam penilaian manajemen risiko keamanan sistem informasi untuk mengidentifikasi risiko dan menentukan prioritas pengendalian. Sementara itu, penelitian Harjian et al. (2025) menunjukkan bahwa FMEA dapat digunakan untuk menganalisis dan memprioritaskan risiko keamanan informasi melalui penilaian terhadap failure mode dan nilai RPN. Penelitian lain mengenai manajemen risiko aset teknologi informasi juga menunjukkan bahwa kombinasi FMEA dengan kerangka keamanan informasi dapat digunakan untuk menghasilkan prioritas pengendalian terhadap risiko yang ditemukan (Wahyuningtyas et al., 2025).

Penggunaan FMEA dalam penilaian risiko keamanan informasi juga telah diterapkan pada lingkungan organisasi untuk mengidentifikasi tingkat risiko dan memberikan rekomendasi pengamanan berdasarkan hasil penilaian risiko (Kusnandar et al., 2024). Pendekatan tersebut menunjukkan bahwa FMEA dapat digunakan sebagai instrumen sistematis untuk mengukur dan memprioritaskan risiko keamanan sebelum organisasi menentukan tindakan pengendalian.

Meskipun penelitian mengenai FMEA dan keamanan sistem informasi telah banyak dilakukan, penelitian yang secara khusus menganalisis risiko keamanan pada Managed Print Services masih relatif terbatas, khususnya pada lingkungan perusahaan yang memiliki kebutuhan pengamanan dokumen dan pengendalian aktivitas pencetakan. MPS memiliki karakteristik yang berbeda dengan sistem informasi pada umumnya karena melibatkan interaksi antara pengguna, komputer, jaringan, server, perangkat lunak pengelolaan pencetakan, mekanisme autentikasi, dan perangkat printer. Oleh karena itu, analisis terhadap risiko keamanan pada MPS perlu mempertimbangkan aspek manusia, autentikasi, infrastruktur, perangkat, serta monitoring aktivitas pencetakan.

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk mengidentifikasi dan menganalisis failure mode yang berpotensi menimbulkan risiko keamanan pada Sistem Managed Print Services di PT Pertamina Patra Niaga RU III Plaju menggunakan metode Failure Modes and Effects Analysis. Penilaian dilakukan berdasarkan parameter Severity, Occurrence, dan Detection untuk memperoleh nilai Risk Priority Number sebagai dasar dalam menentukan prioritas risiko. Hasil analisis selanjutnya digunakan untuk menyusun rekomendasi mitigasi terhadap risiko yang memiliki prioritas tinggi, khususnya yang berkaitan dengan penguatan mekanisme autentikasi, monitoring penggunaan kertas, pengendalian penggunaan ID Card, serta pemeliharaan infrastruktur MPS.

2. Metode Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif dengan pendekatan kualitatif untuk menggambarkan kondisi Sistem Managed Print Services berdasarkan fakta yang diperoleh di lapangan tanpa melakukan manipulasi terhadap objek penelitian (Sugiyono, 2019). Pendekatan tersebut digunakan untuk memperoleh pemahaman mengenai proses operasional MPS, kondisi sistem, potensi kegagalan, serta risiko keamanan yang terdapat pada implementasi MPS di PT Pertamina Patra Niaga RU III Plaju. Analisis risiko dilakukan menggunakan metode Failure Modes and Effects Analysis untuk mengidentifikasi failure mode, menganalisis penyebab dan dampaknya, serta menentukan prioritas risiko berdasarkan nilai RPN (International Electrotechnical Commission, 2018).

2.1. Lokasi dan Objek Penelitian

Penelitian dilaksanakan pada Fungsi IT PT Pertamina Patra Niaga RU III Plaju yang bertanggung jawab terhadap pengelolaan infrastruktur teknologi informasi, termasuk implementasi dan pengelolaan Sistem Managed Print Services. Objek penelitian difokuskan pada Sistem MPS yang digunakan sebagai layanan pencetakan dokumen secara terpusat di lingkungan perusahaan. Fokus penelitian mencakup proses Control Print, penyimpanan dokumen pada print server, autentikasi pengguna menggunakan ID Card, proses pencetakan dokumen, serta aktivitas monitoring dan pengelolaan sistem.

2.2. Populasi dan Sampel

Populasi penelitian merupakan seluruh pengguna Sistem MPS yang aktif menggunakan layanan pencetakan dokumen dalam kegiatan operasional perusahaan. Berdasarkan data yang diperoleh dari Fungsi IT, jumlah

pengguna MPS sebanyak 50 orang. Karena jumlah populasi relatif kecil, penelitian menggunakan teknik sampling jenuh atau total sampling, yaitu seluruh anggota populasi dijadikan sebagai sampel penelitian (Sugiyono, 2019). Dengan demikian, sebanyak 50 pengguna MPS menjadi responden dalam penilaian risiko menggunakan instrumen FMEA.

Selain responden kuesioner, penelitian melibatkan informan kunci dari Fungsi IT yang memahami implementasi dan pengelolaan Sistem MPS. Informan tersebut memberikan informasi mengenai proses operasional sistem, potensi failure mode, penyebab kegagalan, dampak kegagalan, serta mekanisme pengendalian yang telah diterapkan. Informasi dari informan kunci digunakan sebagai dasar dalam penyusunan daftar failure mode sebelum dilakukan penilaian menggunakan FMEA.

2.3. Sumber Data

Data penelitian terdiri atas data primer dan data sekunder. Data primer diperoleh secara langsung dari objek penelitian melalui observasi, wawancara, dan kuesioner penilaian FMEA. Data primer digunakan untuk memperoleh informasi mengenai mekanisme operasional MPS, kondisi sistem, potensi failure mode, penyebab dan dampak kegagalan, serta penilaian terhadap parameter Severity, Occurrence, dan Detection.

Data sekunder digunakan sebagai data pendukung yang diperoleh dari dokumen internal perusahaan, dokumentasi sistem, prosedur operasional, serta literatur yang berkaitan dengan manajemen risiko keamanan informasi, Managed Print Services, dan metode FMEA. Penggunaan data sekunder bertujuan memperkuat hasil analisis dan memberikan landasan teoritis terhadap proses identifikasi serta pengelolaan risiko (International Electrotechnical Commission, 2018; International Organization for Standardization, 2018).

2.4. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui observasi, wawancara, kuesioner, dan dokumentasi. Observasi dilakukan dengan mengamati secara langsung proses operasional Sistem MPS mulai dari pengiriman dokumen melalui komputer pengguna menggunakan Control Print, penyimpanan dokumen pada print server, proses autentikasi menggunakan ID Card, hingga proses pencetakan pada perangkat printer. Observasi juga dilakukan terhadap perangkat keras, perangkat lunak, jaringan, mekanisme autentikasi, dan prosedur operasional untuk mengidentifikasi kondisi yang berpotensi menimbulkan failure mode.

Wawancara dilakukan secara semi-terstruktur kepada informan kunci dari Fungsi IT yang bertanggung jawab terhadap pengelolaan Sistem MPS. Wawancara digunakan untuk memperoleh informasi mengenai proses operasional, mekanisme pengendalian, failure mode, penyebab kegagalan, dampak kegagalan, serta upaya mitigasi yang telah diterapkan.

Kuesioner digunakan untuk memperoleh penilaian terhadap parameter Severity (S), Occurrence (O), dan Detection (D) pada failure mode yang telah diidentifikasi melalui observasi dan wawancara. Penilaian menggunakan skala 1–10 sesuai dengan pedoman FMEA, kemudian nilai yang diperoleh diolah untuk mendapatkan nilai rata-rata setiap parameter (International Electrotechnical Commission, 2018). Kuesioner diberikan kepada 50 pengguna MPS sebagai responden penelitian.

Dokumentasi dilakukan dengan mengumpulkan dokumen dan bukti pendukung yang berkaitan dengan implementasi MPS, seperti prosedur operasional, dokumentasi sistem, foto kegiatan observasi, struktur jaringan, konfigurasi sistem, serta dokumen pendukung lainnya. Dokumentasi digunakan untuk memperkuat informasi yang diperoleh melalui observasi dan wawancara.

2.5. Instrumen Penelitian

Instrumen penelitian terdiri atas lembar observasi, pedoman wawancara, dan kuesioner penilaian FMEA. Lembar observasi digunakan untuk mencatat kondisi aktual proses pencetakan, perangkat printer, print server, jaringan, mekanisme autentikasi, dan prosedur operasional MPS. Pedoman wawancara digunakan untuk menggali informasi mengenai implementasi sistem, failure mode, penyebab dan dampak kegagalan, pengendalian yang telah diterapkan, serta rekomendasi perbaikan. Kuesioner FMEA digunakan untuk memperoleh nilai Severity, Occurrence, dan Detection pada setiap failure mode.

2.6 Tahapan Analisis FMEA

Analisis data dilakukan menggunakan metode Failure Modes and Effects Analysis untuk menentukan prioritas risiko keamanan pada Sistem MPS (International Electrotechnical Commission, 2018). Tahap pertama dilakukan dengan memahami proses dan alur kerja Sistem MPS melalui hasil observasi, wawancara, dan dokumentasi. Proses yang dianalisis meliputi Control Print, penyimpanan dokumen pada print server, autentikasi menggunakan ID Card, pencetakan dokumen, dan monitoring sistem.

Tahap berikutnya adalah mengidentifikasi failure mode yang berpotensi terjadi pada setiap proses MPS. Failure mode kemudian dianalisis berdasarkan cause of failure and effect of failure. Penyebab kegagalan dapat berasal dari faktor manusia, perangkat keras, perangkat lunak, jaringan, maupun prosedur operasional, sedangkan dampaknya dianalisis berdasarkan pengaruhnya terhadap keamanan informasi dan kelancaran layanan pencetakan.

Setiap failure mode selanjutnya dinilai berdasarkan tiga parameter FMEA, yaitu Severity (S), Occurrence (O), dan Detection (D). Severity menunjukkan tingkat keparahan dampak apabila kegagalan terjadi, sedangkan Occurrence menunjukkan tingkat kemungkinan atau frekuensi terjadinya kegagalan. Detection menunjukkan kemampuan mekanisme pengendalian dalam mendeteksi kegagalan sebelum menimbulkan dampak yang lebih besar (International Electrotechnical Commission, 2018).

Nilai Severity, Occurrence, dan Detection selanjutnya digunakan untuk menghitung Risk Priority Number. Perhitungan RPN dilakukan dengan mengalikan ketiga parameter tersebut menggunakan persamaan:

$$RPN = S \times O \times D$$

Nilai RPN digunakan untuk mengurutkan failure mode berdasarkan tingkat prioritas risiko. Semakin tinggi nilai RPN, semakin tinggi pula prioritas risiko yang perlu mendapatkan perhatian dan tindakan mitigasi (International Electrotechnical Commission, 2018).

Tahap terakhir adalah penyusunan rekomendasi mitigasi berdasarkan hasil pemeringkatan RPN. Rekomendasi disusun dengan mempertimbangkan penyebab kegagalan, dampak yang ditimbulkan, mekanisme pengendalian yang telah tersedia, serta kondisi aktual implementasi Sistem MPS di PT Pertamina Patra Niaga RU III Plaju. Rekomendasi diarahkan terutama pada failure mode yang memiliki nilai RPN tinggi sehingga dapat digunakan sebagai bahan evaluasi untuk meningkatkan keamanan dan keandalan layanan MPS.

3. Hasil dan Pembahasan

3.1 Gambaran Implementasi Sistem MPS

Berdasarkan hasil observasi dan wawancara, Sistem Managed Print Services telah diterapkan di PT Pertamina Patra Niaga RU III Plaju sejak sekitar tahun 2018 sebagai bagian dari upaya meningkatkan keamanan dokumen, efisiensi penggunaan perangkat printer, serta pengendalian biaya operasional. Sistem MPS berada di bawah pengelolaan Fungsi IT dan menggunakan perangkat lunak Kofax untuk mengelola aktivitas pencetakan, antrean dokumen, serta monitoring perangkat printer.



Gambar 1 Printer Managed Print Service

Implementasi MPS terdiri atas beberapa komponen utama, yaitu pengguna, komputer, jaringan LAN, server MPS, perangkat lunak Kofax, serta printer multifungsi yang dilengkapi dengan card reader. Dokumen yang akan dicetak dikirim melalui jaringan internal perusahaan menuju server MPS dan disimpan sementara dalam print queue sebelum dapat dicetak oleh pengguna. Mekanisme tersebut membuat dokumen tidak langsung keluar dari printer ketika perintah pencetakan diberikan melalui komputer.

Proses pencetakan dimulai ketika pengguna memilih printer MPS pada komputer dan menjalankan fitur Control Print. Dokumen kemudian dikirim ke server MPS melalui Kofax dan disimpan dalam print queue. Pengguna selanjutnya melakukan tapping ID Card perusahaan pada card reader printer untuk melakukan autentikasi. Setelah autentikasi berhasil, daftar dokumen pengguna ditampilkan pada panel printer sehingga dokumen dapat dipilih dan dicetak. Aktivitas pencetakan kemudian tercatat pada sistem sebagai bagian dari mekanisme monitoring.

Hasil observasi menunjukkan bahwa sistem telah memiliki beberapa mekanisme pengendalian, seperti autentikasi menggunakan ID Card, monitoring kondisi printer, pemantauan penggunaan perangkat secara keseluruhan, serta notifikasi ketika tinta atau kertas hampir habis. Namun, sistem belum menyediakan monitoring penggunaan kertas secara khusus berdasarkan periode harian. Selain itu, autentikasi masih menggunakan ID Card sebagai satu-satunya media verifikasi sehingga terdapat potensi penyalahgunaan apabila kartu digunakan oleh pihak lain.

3.2 Identifikasi Failure Mode

Berdasarkan hasil observasi dan wawancara dengan teknisi pengelola MPS, dan dokumentasi, ditemukan sebanyak 12 failure mode yang berpotensi memengaruhi keamanan dan operasional Sistem MPS. Failure mode tersebut berasal dari aspek manusia dan autentikasi, sistem dan server, jaringan dan infrastruktur, perangkat dan operasional, serta monitoring dan pengendalian.

Failure mode yang ditemukan meliputi ID Card dipinjamkan kepada pegawai lain, autentikasi menggunakan ID Card gagal, dokumen tertahan pada server MPS, gangguan komunikasi antara server MPS dan printer, printer tidak menerima dokumen dari server, printer kehabisan toner, printer kehabisan kertas, pengguna salah memilih dokumen pada layar printer, gangguan jaringan yang menyebabkan proses Control Print gagal, pengguna lupa mengambil dokumen setelah selesai dicetak, belum adanya autentikasi sidik jari setelah tapping kartu, serta belum adanya monitoring penggunaan kertas harian.

Dari kedua belas failure mode tersebut, beberapa kondisi memiliki keterkaitan langsung dengan keamanan dokumen. Peminjaman ID Card dapat memungkinkan dokumen dicetak oleh pihak yang tidak berwenang, sedangkan pengguna yang lupa mengambil dokumen dapat menyebabkan dokumen yang telah dicetak berpotensi dilihat oleh pihak lain. Belum adanya autentikasi sidik jari juga meningkatkan potensi penyalahgunaan akses karena proses autentikasi masih bergantung pada ID Card.

Selain risiko keamanan dokumen, terdapat failure mode yang berkaitan dengan ketersediaan layanan, seperti dokumen tertahan pada server, gangguan komunikasi server dengan printer, printer tidak menerima dokumen, kehabisan toner, kehabisan kertas, dan gangguan jaringan. Kondisi tersebut dapat menyebabkan proses pencetakan tertunda atau tidak dapat dilakukan. Sementara itu, kesalahan pengguna dalam memilih dokumen berkaitan dengan aspek integritas karena dokumen yang dicetak dapat tidak sesuai dengan dokumen yang dimaksud.

3.3 Hasil Penilaian Severity, Occurrence, dan Detection

Penilaian FMEA dilakukan menggunakan tiga parameter, yaitu Severity (S), Occurrence (O), dan Detection (D) dengan skala 1–10. Penilaian Severity dan Occurrence dilakukan oleh 50 pengguna MPS, sedangkan penilaian Detection dilakukan oleh dua teknisi yang bertanggung jawab terhadap pengelolaan Sistem MPS. Nilai dari setiap parameter kemudian dihitung berdasarkan nilai rata-rata untuk masing-masing failure mode.

Hasil penilaian Severity menunjukkan bahwa nilai rata-rata keseluruhan adalah 4,74. Nilai Severity tertinggi terdapat pada failure mode printer kehabisan toner saat proses pencetakan dengan nilai 5,22, diikuti pengguna salah memilih dokumen pada layar printer sebesar 5,20 dan belum adanya monitoring penggunaan kertas harian sebesar 5,02. Nilai Severity terendah terdapat pada gangguan jaringan yang menyebabkan proses Control Print gagal dengan nilai 4,26.

Nilai Occurrence memiliki rata-rata keseluruhan sebesar 4,63. Failure mode ID Card dipinjamkan kepada pegawai lain memperoleh nilai Occurrence tertinggi sebesar 5,42. Nilai tersebut menunjukkan bahwa berdasarkan pengalaman pengguna, kondisi tersebut memiliki kemungkinan terjadi relatif lebih tinggi dibandingkan failure mode lainnya. Nilai Occurrence berikutnya terdapat pada dokumen tertahan pada server MPS sebesar 4,84, sedangkan pengguna salah memilih dokumen dan pengguna lupa mengambil dokumen masing-masing memperoleh nilai 4,74.

Penilaian Detection menunjukkan nilai rata-rata keseluruhan sebesar 3,46. Failure mode belum adanya autentikasi sidik jari setelah tapping kartu memperoleh nilai Detection tertinggi sebesar 7,50, kemudian belum adanya monitoring penggunaan kertas harian sebesar 7,00 dan ID Card dipinjamkan kepada pegawai lain sebesar 6,00. Nilai Detection yang tinggi menunjukkan bahwa kondisi tersebut relatif lebih sulit dideteksi melalui mekanisme pengendalian yang tersedia.

3.4 Analisis Risk Priority Number

Nilai Risk Priority Number diperoleh dengan mengalikan nilai Severity, Occurrence, dan Detection menggunakan persamaan $RPN = S \times O \times D$. Berdasarkan hasil perhitungan terhadap 12 failure mode, diperoleh nilai RPN yang berbeda-beda sehingga setiap failure mode memiliki tingkat prioritas penanganan yang berbeda.

Failure mode belum adanya autentikasi sidik jari setelah tapping kartu memperoleh nilai RPN tertinggi sebesar 162,13. Nilai tersebut berasal dari Severity sebesar 4,58, Occurrence sebesar 4,72, dan Detection sebesar 7,50. Nilai Detection yang tinggi menunjukkan adanya keterbatasan mekanisme pengendalian dalam mendeteksi risiko yang berkaitan dengan autentikasi pengguna.

Failure mode dengan nilai RPN tertinggi kedua adalah belum adanya monitoring penggunaan kertas harian dengan nilai 155,32, yang terdiri atas Severity 5,02, Occurrence 4,42, dan Detection 7,00. Kondisi tersebut menunjukkan bahwa meskipun monitoring kondisi printer telah tersedia, belum adanya informasi penggunaan kertas secara harian menyebabkan pengendalian penggunaan kertas secara lebih terperinci masih terbatas.

Failure mode ID Card dipinjamkan kepada pegawai lain memperoleh nilai RPN sebesar 148,94 dengan Severity 4,58, Occurrence 5,42, dan Detection 6,00. Nilai Occurrence tersebut merupakan yang tertinggi dari seluruh failure mode sehingga peminjaman ID Card menjadi perhatian karena berkaitan langsung dengan mekanisme autentikasi dan akses terhadap dokumen yang berada pada Sistem MPS.

Sebaliknya, failure mode dengan nilai RPN terendah adalah gangguan jaringan yang menyebabkan proses Control Print gagal dengan nilai 28,50. Berdasarkan klasifikasi yang digunakan dalam penelitian, nilai RPN 1–50 termasuk risiko rendah, 51–100 termasuk risiko sedang, 101–200 termasuk risiko tinggi, dan nilai lebih dari 200 termasuk risiko sangat tinggi. Dengan klasifikasi tersebut, terdapat tiga failure mode berkategori tinggi, tujuh berkategori sedang, dan dua berkategori rendah, serta tidak terdapat failure mode yang termasuk kategori sangat tinggi.

Tabel 1 Ranking Risiko Sistem MPS Berdasarkan RPN

Ranking	Failure Mode	RPN	Klasifikasi
1	Belum adanya autentikasi sidik jari setelah tapping kartu	162,13	Tinggi
2	Belum adanya monitoring penggunaan kertas harian	155,32	Tinggi
3	ID Card dipinjamkan kepada pegawai lain	148,94	Tinggi
4	Pengguna lupa mengambil dokumen	86,08	Sedang
5	Printer kehabisan kertas	78,87	Sedang
6	Printer kehabisan toner	70,47	Sedang
7	Dokumen tertahan pada server MPS	68,53	Sedang
8	Printer tidak menerima dokumen dari server	62,9	Sedang

9	Autentikasi menggunakan ID Card gagal	54,29	Sedang
10	Gangguan komunikasi antara server MPS dan printer	50,39	Sedang
11	Pengguna salah memilih dokumen	36,97	Rendah
12	Gangguan jaringan menyebabkan Control Print gagal	28,5	Rendah

Sumber: Hasil pengolahan data penelitian.

Berdasarkan hasil tersebut, 3 failure mode dengan nilai RPN tertinggi menjadi prioritas utama dalam penyusunan mitigasi. Ketiga risiko tersebut memiliki karakteristik yang berbeda, yaitu keamanan autentikasi, pengendalian operasional, dan perilaku pengguna. Meskipun demikian, ketiganya memiliki keterkaitan dengan keterbatasan pengendalian yang tersedia pada Sistem MPS.

3.5 Analisis Risiko Berdasarkan CIA

Analisis Confidentiality, Integrity, dan Availability digunakan untuk melihat karakteristik dampak dari failure mode yang ditemukan. Pada aspek Confidentiality, risiko terutama berkaitan dengan peminjaman ID Card, pengguna yang lupa mengambil dokumen, serta belum adanya autentikasi tambahan setelah tapping kartu. Ketiga kondisi tersebut berpotensi menyebabkan dokumen diakses atau dicetak oleh pihak yang tidak berwenang.

Pada aspek Integrity, risiko ditemukan pada kondisi pengguna salah memilih dokumen pada layar printer. Kesalahan tersebut dapat menyebabkan dokumen yang dicetak tidak sesuai dengan dokumen yang seharusnya dicetak. Sementara itu, aspek Availability berkaitan dengan kegagalan autentikasi, dokumen yang tertahan pada server, gangguan komunikasi server dengan printer, printer yang tidak menerima dokumen, kehabisan toner atau kertas, serta gangguan jaringan yang dapat menyebabkan proses pencetakan tertunda atau tidak dapat dilakukan.

Hasil analisis menunjukkan bahwa tiga failure mode dengan prioritas tertinggi memiliki keterkaitan yang kuat dengan aspek Confidentiality dan pengendalian operasional. Kondisi tersebut memperlihatkan bahwa risiko keamanan pada MPS tidak hanya berkaitan dengan gangguan teknis, tetapi juga dengan mekanisme autentikasi dan pengendalian aktivitas pengguna.

3.6 Rekomendasi Mitigasi

Berdasarkan hasil FMEA, rekomendasi mitigasi utama diarahkan pada tiga failure mode yang termasuk kategori risiko tinggi. Rekomendasi pertama adalah penguatan mekanisme autentikasi dengan menerapkan autentikasi dua tahap berupa ID Card dan sidik jari. Pengguna melakukan tapping ID Card terlebih dahulu, kemudian melakukan verifikasi sidik jari sebelum dokumen dapat dicetak. Mekanisme tersebut diharapkan dapat mengurangi risiko penyalahgunaan ID Card dan memastikan bahwa pengguna yang melakukan autentikasi merupakan pihak yang berhak mengakses dokumen.

Rekomendasi kedua adalah meningkatkan monitoring penggunaan kertas dengan menyediakan pencatatan atau laporan penggunaan kertas secara harian. Monitoring tersebut dapat membantu pengelola mengetahui pola penggunaan kertas, mengidentifikasi penggunaan yang tidak wajar, serta meningkatkan pengendalian terhadap penggunaan printer dan persediaan kertas.

Rekomendasi ketiga adalah memperkuat pengendalian terhadap penggunaan ID Card melalui sosialisasi kepada pengguna agar tidak meminjamkan kartu kepada pegawai lain. Pengendalian tersebut dapat dilengkapi dengan evaluasi mekanisme autentikasi secara berkala untuk memastikan akses terhadap dokumen tetap terlindungi.

Selain tiga prioritas tersebut, pengendalian terhadap infrastruktur MPS tetap diperlukan melalui pemeriksaan server, jaringan, komunikasi antara server dan printer, kondisi printer, toner, serta kertas secara berkala. Risiko dengan kategori sedang dan rendah tetap perlu dilakukan monitoring dan evaluasi berkala sesuai dengan nilai RPN masing-masing.

Secara keseluruhan, hasil penelitian menunjukkan bahwa metode FMEA dapat digunakan untuk mengidentifikasi failure mode, menentukan prioritas risiko berdasarkan nilai RPN, dan menjadi dasar dalam penyusunan rekomendasi mitigasi pada Sistem Managed Print Services. Hasil analisis juga menunjukkan bahwa prioritas perbaikan utama berada pada aspek penguatan autentikasi dan peningkatan monitoring karena kedua aspek tersebut memiliki failure mode dengan nilai RPN tertinggi.

4. Kesimpulan

Berdasarkan hasil penelitian mengenai risiko keamanan pada Sistem Managed Print Services di PT Pertamina Patra Niaga RU III Plaju menggunakan metode Failure Modes and Effects Analysis, ditemukan 12 failure mode yang berasal dari aspek manusia dan autentikasi, sistem dan server, jaringan dan infrastruktur, perangkat dan operasional, serta monitoring dan pengendalian. Hasil penilaian FMEA menunjukkan nilai rata-rata Severity sebesar 4,74 dan Occurrence sebesar 4,63 berdasarkan penilaian 50 pengguna MPS, sedangkan penilaian Detection dilakukan oleh 2 teknisi MPS. Hasil perhitungan Risk Priority Number menunjukkan tiga failure mode dengan kategori risiko tinggi, yaitu belum adanya autentikasi sidik jari setelah tapping kartu dengan RPN 162,13, belum adanya monitoring penggunaan kertas harian dengan RPN 155,32, dan ID Card dipinjamkan kepada pegawai lain dengan RPN 148,94. Selain itu, terdapat 7 failure mode dengan kategori risiko sedang dan 2 failure mode dengan kategori risiko rendah, serta tidak terdapat failure mode dengan kategori sangat tinggi. Berdasarkan analisis CIA, risiko keamanan yang paling menonjol berkaitan dengan aspek Confidentiality, khususnya potensi penyalahgunaan akses melalui ID Card dan belum adanya autentikasi tambahan, sedangkan gangguan server, jaringan, komunikasi server-printer, printer, toner, dan kertas terutama berkaitan dengan Availability. Berdasarkan prioritas risiko tersebut, rekomendasi utama yang diberikan adalah penerapan autentikasi dua tahap menggunakan ID Card dan sidik jari, peningkatan monitoring penggunaan kertas secara harian, penguatan pengendalian terhadap penggunaan ID Card, serta pemantauan infrastruktur dan perangkat MPS secara berkala. Dengan demikian, metode FMEA dapat digunakan untuk mengidentifikasi dan menentukan prioritas risiko keamanan pada Sistem MPS serta menjadi dasar dalam penyusunan langkah mitigasi untuk meningkatkan keamanan dan pengelolaan layanan pencetakan.

Reference

1. Ajrina, N. N., Sipayung, P. I. O. B., Purwitasari, Y., Rizmadita, H. A., Putra, A. B., & Wulansari, A. (2025). Analisis keamanan sistem informasi pelayanan pelanggan menggunakan pendekatan FMEA dan ISO/IEC 27001:2013 pada PT PLN UP3 Gresik. *Kohesi: Jurnal Sains dan Teknologi*, 8(8). <https://doi.org/10.2238/pqjn1b70>
2. Harjian, A. R., Ginardi, R. V. H., & Ciptaningtyas, H. T. (2025). Analisis dan manajemen risiko keamanan informasi menggunakan metode Failure Mode and Effects Analysis (FMEA) dan kontrol ISO/IEC 27001:2022 (Studi kasus: Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ). *Jurnal Teknik ITS*, 14(1). <https://doi.org/10.12962/j23373539.v14i1.148053>
3. International Electrotechnical Commission. (2018). *IEC 60812:2018: Failure modes and effects analysis (FMEA and FMECA)*. IEC.
4. International Organization for Standardization. (2018). *ISO 31000:2018: Risk management—Guidelines*. ISO.
5. International Organization for Standardization. (2022a). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
6. International Organization for Standardization. (2022b). *ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. ISO.
7. Kusnandar, A., Rochim, A. F., & Gunawan, V. (2024). Pengukuran tingkat risiko dan keamanan informasi menggunakan metode FMEA berbasis ISO/IEC 27001 pada instansi XYZ untuk keamanan sistem informasi. *Jurnal Sistem Informasi Bisnis*, 14(4), 375–384. <https://doi.org/10.21456/vol14iss4pp375-384>
8. Pan, X., et al. (2024). Security analysis and monitoring assessment of networked printers: A report. *Electronics Letters*. <https://doi.org/10.1049/ell2.13097>
9. Quocirca. (2024). *The print security landscape, 2024*. Quocirca.
10. Saputri, S. N., Salisah, F. N., Maita, I., & Rozanda, N. E. (2024). Penggunaan metode FMEA dalam penilaian manajemen risiko keamanan sistem informasi rumah sakit. *INOVTEK Polbeng—Seri Informatika*, 9(1), 1–15. <https://doi.org/10.35314/isi.v9i1.3951>
11. Setiawan, M. S. A., Safitri, E. M., Taufiqurahman, M. A. T., & Pratama, M. A. (2023). Analisis manajemen risiko keamanan sistem informasi Rocketic.id menggunakan metode OCTAVE dan FMEA. *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, 11(3), 504–514. <https://doi.org/10.26418/JUSTIN.V11I3.66628>
12. Subektiningsih, S., Prasetyo, A. R. E., & Indrayani, R. (2022). Evaluasi aspek keamanan informasi sistem penilaian mahasiswa magang menggunakan metode Failure Mode and Effect Analysis. *Jurnal Teknik Komputer*, 8(2).
13. Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
14. Surya, M., Setiawan, A., Safitri, E. M., Asyam, M., Taufiqurahman, T., & Pratama, M. A.
15. Virgiawan, Santi, & Alfresi. (2025). [Judul artikel sesuai sumber yang digunakan dalam laporan].
16. Wahyuningtyas, A., Mandenni, N. M. I. M., & Pasirullo, M. A. (2025). Analisis dan manajemen risiko keamanan aset teknologi informasi menggunakan metode OCTAVE dan FMEA berbasis ISO 27001:2022: Studi kasus perusahaan XYZ. *Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi*, 3(2), 65–76. <https://doi.org/10.61132/neptunus.v3i2.796>