JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 1 Juni 2025
ISSN 3025-0919 (media online)
Hal 10-14

Analisis Manajemen Risiko Keamanan Informasi Menggunakan Metode *Failure Mode and Effect Analysis* (FMEA) (Studi Kasus: BPS Kota Pangkal Pinang)

Syafira Nur Iftizam[1], Dimas Firmansyah[2]

[*1,2]Fakultas Sains dan Teknik, Program Studi Teknologi Informasi, Universitas Bangka Belitung, Bangka, Indonesia

Email: *[1]syafiranur364@gmail.com, [2]dimasfirmansyah657@gmail.com

Abstrak− Keamanan informasi menjadi aspek penting dalam pengelolaan data di instansi pemerintahan, terutama bagi Badan Pusat Statistik (BPS) yang menangani data strategis nasional. Penelitian ini bertujuan untuk menganalisis potensi risiko keamanan informasi yang terdapat pada sistem BPS Kota Pangkalpinang menggunakan metode *Failure Mode and Effect Analysis* (FMEA). Metode ini digunakan untuk mengidentifikasi bentuk kegagalan, mengevaluasi tingkat keparahan, kemungkinan terjadinya, serta kemampuan sistem dalam mendeteksi kegagalan melalui perhitungan *Risk Priority Number* (RPN). Pengumpulan data dilakukan melalui observasi dan wawancara langsung dengan pihak internal BPS. Hasil analisis menunjukkan bahwa serangan *ransomware*, dan kebocoran data merupakan risiko dengan nilai RPN tertinggi dan menjadi prioritas utama untuk mitigasi. Berdasarkan temuan tersebut, penelitian ini memberikan beberapa rekomendasi peningkatan sistem keamanan informasi, seperti penguatan infrastruktur jaringan, penerapan sistem backup yang terintegrasi, serta peningkatan kesadaran keamanan siber di lingkungan kerja. Penelitian ini diharapkan dapat menjadi acuan dalam pengelolaan risiko keamanan informasi di instansi pemerintah.

Kata Kunci: BPS; FMEA; Keamanan Informasi; Risiko; Sistem Informasi;

Abstract−Information security is an important aspect in data management within government institutions, especially for the Central Bureau of Statistics (BPS), which handles national strategic data. This study aims to analyze the potential risks of information security found in the BPS Kota Pangkalpinang system using the Failure Mode and Effect Analysis (FMEA) method. This method is used to identify failure modes, evaluate severity levels, likelihood of occurrence, and the system's ability to detect failures through the calculation of the Risk Priority Number (RPN). Data collection was carried out through direct observation and interviews with internal BPS parties. The analysis results show that ransomware attacks and data breaches are the risks with the highest RPN values and become the main priorities for mitigation. Based on these findings, this research provides several recommendations for improving the information security system, such as strengthening network infrastructure, implementing integrated backup systems, and increasing cybersecurity awareness in the workplace environment. This research is expected to become a reference in managing information security risks in government institutions.

Keywords: BPS; FMEA; Information Security; Risk; Information System

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat membawa dampak besar dalam pengelolaan data dan informasi, baik di sektor swasta maupun pemerintahan. Teknologi informasi kini menjadi tulang punggung dalam berbagai aktivitas organisasi, termasuk dalam perencanaan, pelaporan, dan pengambilan keputusan strategis. Namun, di balik kemudahan dan efisiensi yang ditawarkan, ancaman terhadap keamanan informasi juga terus meningkat. Kebocoran data, akses ilegal, dan serangan siber kini menjadi tantangan nyata yang harus dihadapi oleh setiap organisasi, termasuk instansi pemerintah.

Salah satu instansi pemerintahan yang sangat bergantung pada keamanan informasi adalah Badan Pusat Statistik (BPS)(Kasus et al., n.d.). Sebagai lembaga yang mengelola data strategis nasional, BPS memiliki tanggung jawab besar dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi(Sarihastuti, 2024). Data yang dikelola oleh BPS mencakup informasi penting tentang kependudukan seperti, sosial ekonomi, ketenagakerjaan, dan indikator pembangunan yang menjadi dasar perumusan kebijakan nasional. Maka dari itu, keberlangsungan sistem informasi di lingkungan BPS harus dijaga dengan baik agar meningkatnya kepercayaan masyarakat kepada instansi pemerintah dalam menjaga kerahasiaan data mereka.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 1 Juni 2025
ISSN 3025-0919 (media online)
Hal 10-14

(Naufal & Rokhman, 2024)(Septiyanto Wibowo & Anggai, n.d.) BPS Kota Pangkalpinang sebagai bagian dari jaringan BPS nasional juga memiliki peran penting dalam mengelola data-data sensitif yang berkaitan dengan kependudukan, sosial ekonomi, hingga hasil survei statistik lainnya. Oleh karena itu, keberadaan sistem manajemen keamanan informasi (SMKI) yang handal menjadi hal yang sangat krusial. Risiko-risiko seperti kebocoran data, akses tidak sah, serta serangan siber dapat mengancam integritas data dan merusak kepercayaan publik, jika terjadi serangan seperti ini dapat mengganggu atau mengancam operasi pada BPS, terjadinya pencurian data sensitif, atau bahkan merusak infrastruktur penting yang ada di BPS. Tingginya tingkat kerentanan ini mengharuskan BPS untuk terus meningkatkan kemampuan mereka dalam mengidentifikasi, mencegah, dan merespons serangan-serangan yang dapat merugikan BPS

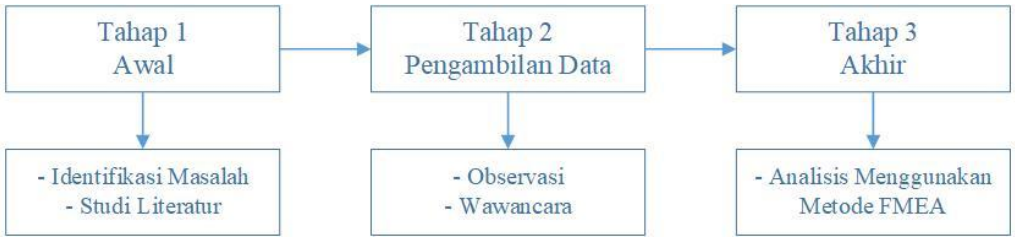
Hasil observasi dan wawancara yang dilakukan oleh penulis mengungkapkan bahwa pada tahun 2023 seluruh website BPS di Indonesia pernah mengalami serangan *ransomware*, termasuk yang dikelola oleh BPS Kota Pangkalpinang. Insiden ini menyebabkan gangguan operasional secara luas dan menjadi bukti nyata bahwa sistem keamanan informasi yang ada belum sepenuhnya mampu menghadapi serangan siber. Hal ini menunjukkan perlunya evaluasi menyeluruh terhadap manajemen risiko keamanan informasi yang diterapkan pada BPS Kota Pangkal Pinang maupun BPS pusat.

(Dewi & Yuamita, 2022) Untuk mendukung proses evaluasi tersebut, diperlukan metode yang mampu mengidentifikasi risiko secara sistematis dan menyusun prioritas penanganan berdasarkan tingkat keparahan dampak. Salah satu metode yang digunakan secara luas dalam manajemen risiko adalah *Failure Mode and Effect Analysis* (FMEA). FMEA adalah metode penilaian risiko yang kuat, yang dimana menilai risiko–risiko yang mungkin terjadi, mengidentifikasi potensi kegagalan pada sistem, dan mengevaluasi dampak yang akan terjadi serta penyelesaian nya

Penelitian ini bertujuan untuk menganalisis potensi risiko keamanan informasi yang terdapat pada sistem BPS Kota Pangkalpinang menggunakan metode *Failure Mode and Effect Analysis* (FMEA). Penelitian ini diharapkan dapat memberikan gambaran terhadap tingkat kesiapan dan kesesuaian manajemen risiko yang dilakukan oleh BPS Kota Pangkalpinang dengan metode FMEA serta memberikan rekomendasi perbaikan guna meningkatkan keamanan informasi di lingkungan kerja.

2. METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus yang difokuskan pada penerapan analisis manajemen risiko keamanan informasi dengan menggunakan metode *Failure Mode and Effect Analysis* (FMEA) sebagai alat bantu identifikasi, pengambilan keputusan berdasarkan prioritas, dan evaluasi risiko (Ramayani, 2022). Metodologi penelitian dapat dilihat pada Gambar 1. Diagram Alir Penelitian



Gambar 1. Diagram Alir Penelitian

2.1 Identifikasi Masalah

Identifikasi masalah merupakan tahap awal dari penelitian. Proses ini bertujuan untuk memahami kondisi awal keamanan informasi yang ada di Badan Pusat Statistik (BPS) Kota Pangkalpinang, mengidentifikasi adanya potensi kerentanan atau kelemahan yang mungkin belum disadari, serta mementukan arah fokus pengumpulan data lebih lanjut untuk hasil data yang lebih relevan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 1 Juni 2025
ISSN 3025-0919 (media online)
Hal 10-14

2.2 Studi Literatur

Pada penelitian ini, studi literatur digunakan sebagai sumber pendukung penelitian untuk memperoleh landasan teori yang kuat dalam memahami konsep manajemen keamanan informasi, dan metode *Failure Mode Effect and Analysis* (FMEA).

2.3 Observasi dan Wawancara

Kegiatan observasi meliputi pengamatan langsung di Badan Pusat Statistik Kota Pangkalpinang, dengan tujuan untuk memperkuat data dan memahami kondisi aktual sistem keamanan informasi yang digunakan. Fokus observasi mencakup proses kerja sistem dan kendala oprasional.

Sementara itu, wawancara dilakukan kepada staff IT. Wawancara ini bertujuan untuk menggali informasi mendalam mengenai penerapan kebijakan keamanan, presepsi potensi risiko, serta upaya mitigasi risiko yang telah dilakukan. Informasi yang diperoleh dari wawancara dan observasi akan dikombinasikan untuk analisis risiko menggunakan metode FMEA.

2.4 Analisis Metode FMEA

Tahap akhir dalam penelitian ini adalah melakukan analisis menggunakan metode *Failure Mode and Effect Analysis* (FMEA). Metode ini bertujuan untuk mengidentifikasi potensi kegagalan (*failure mode*) dalam sistem keamanan informasi, menganalisis penyebab dan dampaknya, serta menentukan prioritas risiko berdasarkan nilai *Risk Priority Number* (RPN). Langkah awal dalam tahap ini dimulai dengan mengidentifikasi proses-proses utama dalam pengelolaan informasi di BPS Kota Pangkalpinang. Selanjutnya, setiap proses dianalisis untuk menentukan kemungkinan kegagalan yang dapat terjadi. Masing-masing potensi risiko dinilai berdasarkan tiga aspek utama, yaitu tingkat keparahan (*Severity*/S), kemungkinan terjadinya (*Occurrence*/O), dan kemampuan sistem untuk mendeteksi kegagalan (*Detection*/D) [6]. Nilai dari ketiga aspek tersebut dikalikan untuk memperoleh nilai RPN. Risiko dengan nilai RPN tertinggi kemudian diprioritaskan untuk dilakukan tindakan mitigasi. Hasil analisis ini menjadi dasar rekomendasi peningkatan sistem keamanan informasi secara terstruktur dan efektif di BPS Kota Pangkalpinang.

$$\mathbf{RPN = Severity \times Occurrence \times Detection}$$

Gambar 2. Rumus RPN

3. ANALISA DAN PEMBAHASAN

(Eze & Eneh, 2022)Untuk menganalisis keamanan informasi pada sistem di Badan Pusat Statistik Kota Pangkalpinang perlu dilakukan analisa potensi kegagalan serta akibat dari kegagalan menggunakan variabel dependen yaitu *Risk Priority Number* (RPN) dengan besaran variabel dari skala 1 sampai 10 [7].

3.1 Identifikasi *Potential Failure Mode*

Identifikasi *potential failure mode* merupakan tahap awal dalam analisis FMEA yang bertujuan untuk mengenali bentuk-bentuk kegagalan yang berpotensi terjadi dalam proses keamanan informasi di BPS Kota Pangkalpinang. Proses ini dilakukan melalui observasi dan wawancara, hasil identifikasi ini menjadi dasar dalam menentukan penyebab, dampak, serta prioritas risiko pada tahapan analisis selanjutnya.

Tabel 1. Identifikasi Risiko

No. *Code*	Risiko
RK1	*Ransomware*
RK2	*Malware*
RK3	*Phishing*
RK4	Kebocoran Data
RK5	Ancaman dari Dalam

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 1 Juni 2025
ISSN 3025-0919 (media online)
Hal 10-14

Tabel 2. Dampak dari Kegagalan

No. *Code*	*Potential Failure Mode*
RK1	*System down* yang sangat lama
RK2	Sistem terinfeksi dan rusak
RK3	Risiko hilangnya data hingga akun
RK4	Terjadi akses tidak sah terhadap data sensitif
RK5	Pegawai dengan sengaja menyebarkan data privasi

3.2 *Ranking Risk Priority* (RPN)

Setelah mengidentifikasi risiko dan dampak dari kegagalan, dilakukan analisis *Risk Priority Number* (RPN) pada setiap risiko yang terjadi. Untuk menentukan nilai RPN digunakan tiga komponen utama yaitu *Severity* (tingkat keparahan), *Occurance* (kemungkinan terjadi), dan *Detection* (deteksi). Berikut adalah hasil analisis pada Tabel 3. *Risk Priority Number* (RPN)

Tabel 3. ***Risk Priority Number*** **(RPN)**

No. *Code*	Identifikasi Masalah	Penyebab Masalah	Dampak Masalah	S	O	D	RPN
RK1	*Ransomware*	Serangan *ransomware* atau overload pada sistem	*System down* yang sangat lama	9	6	5	270
RK2	*Malware*	Infeksi *malware* akibat perangkat tidak terlindungi antivirus	Sistem terinfeksi dan rusak	8	7	4	224
RK3	*Phishing*	Serangan *phishing* atau pengguna mengklik tautan tidak aman	Risiko hilangnya data hingga akun	8	6	5	240
RK4	Kebocoran Data	Kebocoran data akibat lemahnya pengamanan akses (misal, *password* lemah)	Terjadi akses tidak sah terhadap data sensitif	9	5	6	270
RK5	Ancaman dari Dalam	Ancaman dari internal (*insider threat*)	Pegawai dengan sengaja menyebarkan data privasi	7	4	6	128

3.3 *Prioritize* RPN

Prioritize RPN (*Risk Priority Number*) merupakan langkah penting dalam metode FMEA (*Failure Mode and Effects Analysis*) yang bertujuan untuk menentukan urutan prioritas penanganan terhadap potensi risiko berdasarkan tingkat keparahan, kemungkinan terjadinya (Tjahjaningsih, 2016). Dari hasil analisis perhitungan pada Tabel 3. *Risk Priority Number* (RPN), langkah selanjutnya adalah menentukan urutan nilai RPN berdasarkan indeks tertinggi ke rendah.

Tabel 4. Prioritas RPN

No. Code	*Potential Failure Mode*	RPN	Usulan Perbaikan
RK1	*System down* yang sangat lama	270	Implementasi sistem *backup* dan *failover,* serta pemeliharaan secara berkala.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 1 Juni 2025
ISSN 3025-0919 (media online)
Hal 10-14

RK4	Terjadi akses tidak sah terhadap data sensitif	270	Menerapkan kontrok akses.
RK3	Risiko hilangnya data hingga akun	240	Menerapkan kebijakan *backup* otomatis dan menggunakan *cloud storage* terenkripsi.
RK2	Sistem terinfeksi dan rusak	224	Melakukan *update patch* secara rutin, serta menggunakan *anti-malware* serta *firewall* yang andal.
RK5	Pegawai dengan sengaja menyebarkan data privasi	168	Menerapkan aturan dan sanksi tegas, serta evaluasi pegawai secara berkala.

4. KESIMPULAN

Contain Pada penelitian ini membuktikan bahwa metode *Failure Mode and Effect Analysis* (FMEA) mampu digunakan secara efektif dalam menganalisis dan memetakan risiko keamanan informasi pada BPS Kota Pangkalpinang. Dengan mengidentifikasi berbagai potensi kegagalan seperti serangan *ransomware*, *phishing*, dan kebocoran data, metode ini membantu menentukan prioritas penanganan berdasarkan nilai *Risk Priority Number* (RPN).

Hasil analisis menunjukkan bahwa ancaman dengan nilai RPN tertinggi, seperti *ransomware*, merupakan risiko yang paling kritis dan perlu ditangani segera. Berdasarkan temuan tersebut, penelitian ini juga memberikan usulan mitigasi yang dapat dijadikan acuan dalam memperkuat sistem keamanan informasi, seperti penguatan infrastruktur jaringan, peningkatan kesadaran keamanan siber pegawai, serta penerapan kebijakan backup dan enkripsi.

Saran pengembangan penelitian ke depan adalah dengan melakukan perluasan objek penelitian ke instansi pemerintah lain untuk memperoleh hasil komparatif, serta menggunakan metode FMEA dengan standar keamanan seperti ISO/IEC 27001 atau kerangka kerja NIST, agar hasil analisis lebih menyeluruh. Selain itu, penelitian selanjutnya juga disarankan untuk mengembangkan sistem penilaian risiko secara otomatis menggunakan bantuan perangkat lunak atau *tools* berbasis web.

REFERENCES

Eze, M. N., & Eneh, I. I. (2022). Using Failure Occurrence, Severity, Detection, and Risk Priority Number in Developing FMEA Worksheet in a Brewery for Failure Mitigation. In *Risk Priority Number International Journal of Engineering and Environmental Sciences | IJEES* (Vol. 5, Issue 3). https://airjournal.org/ijees

Kasus, S., Web, A., Bps, J., Pandudinata, M., & Ridho, F. (n.d.). *Analisis Keamanan Aplikasi Berbasis Web di Lingkungan BPS RI Study : Jafung BPS Web Application)*. https://www.jafung.bps.go.id

Ramayani, Y. (2022). Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA). *INOVTEK Polbeng - Seri Informatika*, *7*(2), 289. https://doi.org/10.35314/isi.v7i2.2631

Sarihastuti, D. (2024). *Optimalisasi Penyelenggaraan Statistik Sektoral Sebagai Upaya Pemenuhan Data Statistik Berkualitas di Indonesia* (Vol. 5, Issue 10).

Septiyanto Wibowo, R., & Anggai, S. (n.d.). *Analisis Dan Implementasi Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 (Studi Kasus Pada PT.XYZ)* (Vol. 2, Issue 2). Desember.

Tjahjaningsih, Y. S. (2016). Penentuan Prioritas Perbaikan Kegagalan Proses Dalam Pengendalian Kualitas Dengan Mengintegrasikan FMEA Dan Grey Theory. *Edisi Nopember*, *6*(2).