

Analisis Risiko Website BMKG Maritim Tanjung Perak dengan ISO 31000:2018

Hikmah Fajriana Anggun Pitaloka^{1*}, Anang Kunaefi², Mohammad Khusnu Milad³, Andhy Permadi⁴

^{1,2,3}Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sunan Ampel Surabaya

E-mail: fajrianapita@gmail.com^{1*}, akunaefi@uinsby.ac.id², m.milad@uinsa.ac.id³, andhy@uinsby.ac.id⁴

ARTICLE INFO

Riwayat Artikel

Received: 21/01/2026

Revised: 23/02/2026

Accepted: 02/03/2026

Keywords: Risk Management; ISO 31000; Maritime Website; BMKG; Information System

Kata Kunci: Manajemen Risiko; ISO 31000; Website Maritim; BMKG; Sistem Informasi

ABSTRACT

The BMKG Maritim Tanjung Perak website plays an important role in disseminating maritime weather information that supports navigation safety in East Java. This study aims to identify, analyze, and develop risk treatment strategies for the website's information system using the ISO 31000:2018 framework. The research employed a descriptive qualitative approach through a case study, with the research object focusing on the website's operational processes, including weather data updates, server management, and information distribution. Data were collected through direct observation of the workflow for updating information and the technical conditions of the infrastructure, as well as semi-structured interviews with two key informants: a forecaster and a network technician responsible for system operations. The instruments used included observation guidelines, interview question lists, and internal documentation related to operational procedures. Risk analysis was conducted through the stages of identifying assets, risks, and impacts; assessing likelihood and impact; and evaluating risks using a risk matrix. The findings indicate that 18 risks were identified, with five categorized as high risks related to human resource capability and network stability. The risk treatment strategy focuses on risk reduction through improving personnel competence, enhancing network infrastructure, and strengthening information system governance. These findings provide a foundation for implementing structured risk management in maritime weather information services.

ABSTRAK

Website BMKG Maritim Tanjung Perak berperan penting dalam penyebaran informasi cuaca maritim yang mendukung keselamatan pelayaran di Jawa Timur. Penelitian ini bertujuan mengidentifikasi, menganalisis, dan menyusun strategi perlakuan risiko pada sistem informasi website menggunakan kerangka ISO 31000:2018. Penelitian dilakukan dengan pendekatan kualitatif deskriptif melalui studi kasus, dengan objek penelitian berupa proses operasional website yang meliputi pembaruan data cuaca, pengelolaan server, dan distribusi informasi. Data dikumpulkan melalui observasi langsung terhadap alur kerja pembaruan

informasi dan kondisi teknis infrastruktur, serta wawancara semi-terstruktur kepada dua informan kunci yaitu forecaster dan teknisi jaringan sebagai pihak yang bertanggung jawab terhadap operasional sistem. Instrumen yang digunakan berupa pedoman observasi, daftar pertanyaan wawancara, serta dokumentasi internal terkait prosedur operasional. Analisis risiko dilakukan melalui tahapan identifikasi aset, risiko, dan dampak; penilaian likelihood dan impact; serta evaluasi menggunakan matriks risiko. Hasil penelitian menunjukkan terdapat 18 risiko teridentifikasi, dengan lima risiko berkategori tinggi terkait kemampuan SDM dan kestabilan jaringan. Strategi perlakuan risiko difokuskan pada pendekatan pengurangan risiko melalui peningkatan kompetensi personel, perbaikan infrastruktur jaringan, dan penguatan tata kelola sistem informasi. Temuan ini memberikan dasar dalam penerapan manajemen risiko yang terstruktur pada layanan informasi cuaca maritim.

PENDAHULUAN

Informasi cuaca maritim merupakan salah satu komponen penting dalam mendukung keselamatan pelayaran dan aktivitas masyarakat pesisir. Di wilayah Jawa Timur, kebutuhan akan informasi tersebut semakin tinggi seiring dengan meningkatnya lalu lintas pelayaran dan aktivitas kelautan. BMKG Maritim Tanjung Perak menyediakan layanan ini melalui website resmi yang memuat prakiraan tinggi gelombang, pasang surut, arah angin, serta peringatan dini yang dapat diakses oleh publik. Sementara itu, penelitian Usmany & Legowo (Euggelion Kevin Usmany, 2025) menegaskan bahwa penerapan ISO 31000:2018 memungkinkan organisasi untuk memilih strategi perlakuan risiko yang tepat (hindari, kurangi, alihkan, atau terima), serta menekankan pentingnya pelatihan keamanan berkelanjutan dan dokumentasi insiden sebagai bagian dari mitigasi risiko yang efektif (Bayu et al., 2024).

Di balik manfaatnya yang besar, sistem informasi daring seperti website BMKG juga membawa tantangan tersendiri, terutama dalam hal keandalan dan kesinambungan layanan. Dalam kondisi darurat cuaca, misalnya, keterlambatan pembaruan atau gangguan teknis dapat berdampak langsung pada keselamatan pengguna (Badan Meteorologi Klimatologi dan Geofisika, 2023). Hal ini menegaskan bahwa sistem informasi publik bukan sekadar alat bantu, melainkan bagian dari sistem pengambilan keputusan yang berdampak nyata di lapangan. Digitalisasi layanan publik yang semakin masif turut meningkatkan kerentanan terhadap risiko-risiko baru. Gangguan tidak hanya berasal dari sisi teknis seperti perangkat keras, tetapi juga dari aspek non-teknis seperti kesalahan operasional dan lemahnya kebijakan pengelolaan risiko (Pratama Dinatha & Rangga, 2024). Sebuah sistem yang kompleks seperti website layanan maritim memerlukan pendekatan pengelolaan risiko yang

tidak hanya bersifat responsif, tetapi juga strategis dan terukur (Putri & Rudianto, 2025).

ISO 31000:2018 menawarkan solusi dalam bentuk kerangka kerja yang komprehensif untuk manajemen risiko organisasi. Kerangka ini terdiri dari proses sistematis mulai dari penetapan konteks hingga strategi perlakuan risiko (Marhaditha & Pangeran, 2022). Namun, keberhasilan penerapannya bergantung pada sejauh mana pendekatan tersebut dapat disesuaikan dengan karakteristik organisasi publik seperti BMKG yang bersifat hierarkis dan berbasis regulasi (Lathifah Agustina Wicahyani & Salman, 2023). Studi-studi sebelumnya memang menunjukkan bahwa ISO 31000 mampu meningkatkan keamanan dan keandalan sistem informasi di instansi pemerintah (Junior et al., 2025). Namun, perlu dicermati bahwa konteks implementasi di masing-masing lembaga bisa sangat bervariasi. Risiko pada layanan maritim, misalnya, memiliki dinamika yang berbeda dibandingkan layanan administrasi atau dokumen (Anggreani et al., 2025).

Lebih jauh, beberapa literatur menggarisbawahi pentingnya pendekatan manajemen risiko yang tidak hanya fokus pada aspek teknis, tetapi juga pada tata kelola, peran SDM, dan kapasitas institusi (Mesin et al., 2025). Di sisi lain, pendekatan berbasis angka dan pemetaan risiko berdasarkan kemungkinan dan dampak tetap menjadi fondasi penting dalam proses evaluasi risiko (Herlambang et al., 2024). Keterlibatan manajemen puncak dalam integrasi manajemen risiko juga tidak bisa diabaikan. Komitmen ini berperan sebagai penentu apakah sistem manajemen risiko berjalan sebagai prosedur administratif belaka, atau benar-benar menjadi bagian dari budaya organisasi (Aziz & Muharam, 2024). Selain itu, penguatan ekosistem risiko melalui pelatihan dan pembentukan peran khusus juga disarankan dalam berbagai studi (Maynard et al., 2024).

Sektor ini memiliki karakteristik risiko yang sangat kritis karena berhubungan langsung dengan keselamatan di laut. Website BMKG Maritim Tanjung Perak menjadi contoh kasus yang menarik untuk dikaji karena berperan strategis namun belum memiliki kerangka manajemen risiko terdokumentasi secara formal. Analisis risiko pada sistem informasi ini dilakukan dengan mengacu pada kerangka kerja ISO 31000:2018. Diharapkan hasil dari penelitian ini tidak hanya menggambarkan risiko yang dihadapi, tetapi juga memberikan solusi yang aplikatif dan sesuai dengan konteks operasional BMKG.

Berdasarkan uraian tersebut, tujuan penelitian ini adalah untuk mengidentifikasi, menganalisis, dan mengevaluasi potensi risiko pada sistem informasi website BMKG Maritim Tanjung Perak dengan menggunakan kerangka kerja ISO 31000:2018, serta menyusun strategi perlakuan risiko yang relevan dengan kondisi operasional instansi. Penelitian ini memberikan kontribusi ilmiah berupa penerapan pendekatan manajemen risiko berbasis ISO 31000 pada sektor maritim yang belum banyak diteliti sebelumnya, serta menghasilkan rekomendasi strategi perlakuan risiko yang dapat menjadi acuan dalam penguatan tata kelola sistem informasi publik. Keterbatasan penelitian ini terletak pada lingkup analisis yang difokuskan pada aspek operasional website tanpa mengevaluasi efektivitas implementasi perlakuan risiko dalam jangka panjang.

TINJAUAN PUSTAKA

Manajemen Risiko Sistem Informasi

Manajemen risiko merupakan proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan menangani risiko yang dapat mempengaruhi pencapaian tujuan organisasi. Dalam konteks sistem informasi, manajemen risiko menjadi semakin penting seiring dengan meningkatnya ketergantungan organisasi terhadap teknologi informasi (Pratama Dinatha & Ranga, 2024).

Penelitian (Anggreani et al., 2025) menunjukkan bahwa implementasi manajemen risiko pada sistem informasi dapat meningkatkan keamanan dan keandalan layanan. Pendekatan berbasis ISO 31000 terbukti efektif dalam mengidentifikasi dan memitigasi risiko pada berbagai jenis sistem informasi di instansi pemerintah.

ISO 31000:2018

ISO 31000:2018 merupakan standar internasional yang memberikan panduan komprehensif tentang manajemen risiko. Standar ini menekankan pada pendekatan sistematis yang mencakup penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko (Herlambang et al., 2024).

Kelebihan ISO 31000:2018 adalah fleksibilitasnya yang memungkinkan organisasi untuk

menyesuaikan kerangka kerja sesuai dengan karakteristik dan kebutuhan spesifik mereka. Penelitian (Euggelion Kevin Usmany, 2025) menunjukkan bahwa penerapan ISO 31000:2018 pada e-commerce dapat meningkatkan keamanan informasi dan mengurangi risiko operasional secara signifikan.

Sistem Informasi Maritim

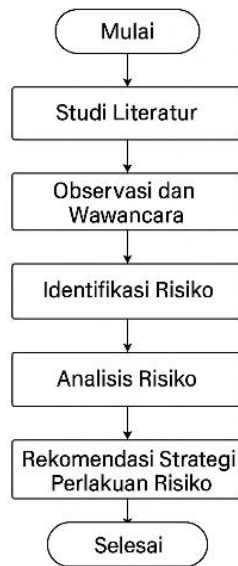
Website informasi cuaca maritim memiliki peran kritis dalam mendukung keselamatan pelayaran. Informasi yang akurat dan tepat waktu sangat diperlukan oleh pelaut, nelayan, dan operator pelabuhan dalam mengambil keputusan operasional (Bistolen et al., 2024).

Karakteristik unik dari sistem informasi maritim adalah tingkat kritikalitasnya yang tinggi, dimana kesalahan atau keterlambatan informasi dapat berdampak langsung pada keselamatan jiwa manusia. Oleh karena itu, pengelolaan risiko pada sistem ini memerlukan perhatian khusus dan pendekatan yang komprehensif.

METODOLOGI PENELITIAN

Pendekatan penelitian yang digunakan adalah kualitatif deskriptif dengan metode studi kasus pada sistem informasi website BMKG Maritim Tanjung Perak. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam terkait kondisi operasional, potensi risiko, dan strategi perlakuan risiko yang relevan dengan konteks lembaga. Partisipan penelitian terdiri dari dua informan utama, yaitu Forecaster yang sekaligus bertanggung jawab pada pengelolaan website serta Senior Teknisi yang menangani jaringan, infrastruktur, dan troubleshooting teknis. Pemilihan informan dilakukan secara purposif karena keduanya terlibat langsung dalam operasional sistem dan penanganan risiko.

Pengumpulan data dilakukan melalui observasi langsung terhadap proses pembaruan informasi cuaca serta wawancara semi-terstruktur untuk menggali informasi mengenai aset sistem, potensi gangguan, pengalaman teknis, dan mekanisme penanganan risiko. proses troubleshooting yang dilakukan langsung saat masalah muncul tidak ada pencatatan. Untuk menggambarkan langkah penelitian secara sistematis, digunakan alur penelitian seperti ditunjukkan pada Gambar 1.



Gambar 1 Alur Penelitian
Sumber : Hasil Olah Data

Untuk memberikan gambaran menyeluruh mengenai proses penelitian, alur penelitian ditunjukkan pada Gambar 1. Tahapan penelitian diawali dengan studi literatur untuk memahami konsep dasar manajemen risiko, standar ISO 31000:2018, serta referensi terkait pengelolaan sistem informasi di lembaga meteorologi. Pemahaman awal ini menjadi fondasi dalam merancang langkah analisis yang sistematis sesuai kerangka kerja ISO. Setelah itu, dilakukan observasi langsung terhadap aktivitas operasional website dan wawancara semi-terstruktur dengan informan kunci untuk memperoleh data kontekstual mengenai alur pembaruan informasi, potensi gangguan, serta kondisi teknis infrastruktur yang menunjang layanan.

Data yang terkumpul selanjutnya digunakan untuk mengidentifikasi aset kritis dan potensi risiko yang relevan dengan operasional website. Risiko yang teridentifikasi kemudian dianalisis berdasarkan tingkat kemungkinan dan dampaknya menggunakan skala kualitatif untuk memperoleh gambaran tingkat kerentanan sistem. Hasil analisis tersebut dievaluasi lebih lanjut melalui pemetaan ke dalam matriks risiko guna menentukan prioritas perlakuan risiko. Tahap akhir penelitian adalah menyusun rekomendasi strategi perlakuan risiko yang realistis dan sesuai dengan kondisi operasional BMKG Maritim Tanjung Perak. Seluruh tahapan pada alur tersebut dibahas secara rinci pada bagian hasil dan pembahasan (Masita, 2022).

HASIL DAN PEMBAHASAN

Penetapan Konteks

Penetapan konteks dilakukan untuk memahami lingkungan operasional website BMKG Maritim

Tanjung Perak yang menyediakan informasi cuaca maritim secara real-time, seperti tinggi gelombang, arah angin, pasang surut, dan peringatan dini. Layanan ini sangat bergantung pada perangkat keras, perangkat lunak, jaringan internet, dan ketepatan data yang diproses oleh forecaster. Berdasarkan observasi dan wawancara, pengelolaan website dilakukan oleh dua orang utama, yaitu forecaster dan teknisi, sehingga kapasitas SDM memegang peran penting. Konteks ini menjadi dasar dalam menentukan ruang lingkup dan jenis risiko yang relevan.

Sebelum melakukan identifikasi risiko, aset-aset yang terlibat dalam operasional website terlebih dahulu dipetakan seperti pada Tabel 1. Aset yang diidentifikasi mencakup lima kategori, yaitu hardware, software, jaringan, data, dan SDM.

Tabel 1. Identifikasi Aset

Kode Aset	Kategori	Nama Aset	Deskripsi
A01	Hardware	Komputer	Perangkat komputer untuk mengolah dan mengupdate informasi
A02	Hardware	Genset	Sumber listrik cadangan saat terjadi pemadaman
A03	Hardware	Server Database	Server yang menyimpan database website
A04	Jaringan	Jaringan Internet	Konektivitas internet untuk akses website
A05	Jaringan	Jaringan listrik	jaringan listrik utama untuk operasional sistem
A06	Software	Web Server	Software yang menjalankan layanan web
A07	Software	Database	Software pengelola database website
A08	Software	Python Scripts	Script Python untuk mengupload dan update informasi cuaca
A9	Data	Data Cuaca dan Maritim	Data hasil pengamatan dan prakiraan cuaca maritim
A10	SDM	Senior Teknisi	Personel yang mengelola website dan bertanggung jawab atas pemantauan risiko
A11	SDM	Forecaster	Personel yang menyiapkan dan memperbarui konten cuaca

Tabel 1 menunjukkan daftar aset yang digunakan dalam operasional website BMKG Maritim Tanjung Perak, yang terdiri dari lima kategori utama: hardware, software, jaringan, data, dan SDM. Aset-aset ini diidentifikasi berdasarkan hasil observasi dan wawancara, di mana pengelola menyatakan bahwa

setiap komponen memiliki peran langsung dalam proses pengolahan dan publikasi informasi cuaca maritim. Keberadaan aset tersebut menjadi dasar dalam menentukan potensi kerentanan dan titik-titik risiko yang dapat mengganggu operasional sistem. Dengan demikian, identifikasi aset ini menjadi langkah awal yang penting sebelum melakukan analisis risiko pada tahap selanjutnya

Identifikasi Risiko

Setelah identifikasi aset dilakukan, tahapan selanjutnya adalah mengidentifikasi potensi risiko yang dapat mengganggu operasional sistem. Berdasarkan observasi dan wawancara, diketahui bahwa proses identifikasi risiko di BMKG Maritim Tanjung Perak selama ini bersifat reaktif, yaitu "melihat error terlebih dahulu kemudian debugging secara manual." Dari proses ini diperoleh 18 risiko yang dikelompokkan ke dalam kategori SDM, sistem dan infrastruktur, serta bencana alam sebagaimana ditampilkan dalam Tabel 2. Risiko-risiko tersebut menggambarkan potensi ancaman yang dapat memengaruhi ketersediaan layanan, akurasi informasi, dan kelancaran penyampaian data maritim.

Tabel 2. Identifikasi Risiko

Kode Risiko	Kategori Risiko	Kemungkinan Risiko	Aset Terkait
R001	SDM	Penyalahgunaan hak akses	A06, A07, A10, A11
R002	SDM	Kesalahan dalam menginputkan data	A08, A09, A11
R003	SDM	Human error dalam pengelolaan data	A09, A10, A11
R004	SDM	Kurangnya pelatihan	A10, A11, A12
R005	Sistem dan infrastruktur	Kerusakan perangkat keras	A01, A02, A03
R006	Sistem dan infrastruktur	Koneksi Internet tidak stabil	A04
R007	Sistem dan infrastruktur	Koneksi Jaringan terputus	A04
R008	Sistem dan infrastruktur	Pemadaman Listrik	A01, A02, A03, A05
R009	Sistem dan infrastruktur	Data corrupt	A07, A09
R010	Sistem dan infrastruktur	Database server down	A03, A07
R011	Sistem dan infrastruktur	Overload server	A03, A06
R012	Sistem dan infrastruktur	Bug atau error pada website	A06, A08
R013	Sistem dan infrastruktur	Server down/tidak dapat diakses	A03, A06
R014	Sistem dan infrastruktur	Kegagalan backup data	A03, A07, A09
R015	SDM	Ketidakkakuratan data	A08, A09, A11
R016	SDM	Keterlambatan	A04,

Kode Risiko	Kategori Risiko	Kemungkinan Risiko	Aset Terkait
		penyampaian informasi	A06, A09
R017	SDM	Serangan cyber (hacking)	A03, A04, A06, A07
R018	Bencana Alam	Bencana alam	A01, A02, A03, A04, A05

Berdasarkan hasil wawancara dan kondisi operasional website BMKG Maritim Tanjung Perak, teridentifikasi 18 kemungkinan risiko yang dikategorikan ke dalam tiga kelompok utama yang dijabarkan pada Tabel 2. Risiko sumber daya manusia (SDM) berjumlah 6 (R001-R004, R015-R016). Risiko sistem dan infrastruktur mendominasi dengan 11 risiko (R005-R014, R017) Risiko bencana alam hanya 1 (R018) namun memiliki dampak signifikan terhadap seluruh sistem.

Setelah risiko diidentifikasi dilanjutkan pada proses identifikasi dampak risiko. Dampak risiko mencakup konsekuensi yang dapat memengaruhi akurasi data, ketersediaan layanan, keamanan sistem, serta keselamatan pengguna informasi cuaca maritim. Berdasarkan hasil wawancara dan observasi, sejumlah risiko dinilai memiliki dampak kritis, terutama yang berkaitan dengan ketidakkakuratan data, keterlambatan penyampaian informasi, serta gangguan jaringan dan server. Pemahaman terhadap dampak ini menjadi langkah penting sebelum melakukan analisis risiko, karena tingkat keparahan konsekuensi menjadi dasar dalam menentukan prioritas penanganan pada tahap selanjutnya. Hasil identifikasi dampak risiko ditunjukkan pada tabel 3.

Tabel 3. Identifikasi Dampak Risiko

Kode Risiko	Dampak
R01	Manipulasi data website, kebocoran informasi sensitif, dan penurunan kepercayaan pengguna.
R02	Informasi cuaca dan maritim tidak akurat yang menyebabkan keputusan salah oleh pengguna dengan potensi membahayakan keselamatan.
R03	Kesalahan pengolahan data menghasilkan informasi yang tidak konsisten dan laporan cuaca yang tidak akurat.
R04	Ketidakmampuan menangani masalah teknis, pengelolaan sistem tidak optimal, dan lambatnya respons terhadap insiden.
R05	Gangguan operasional sistem, ketidakmampuan mengakses data, dan terhentinya layanan website.
R06	Gangguan akses website, keterlambatan update informasi, dan pengalaman pengguna yang buruk.
R07	Website tidak dapat diakses sehingga informasi cuaca dan maritim tidak tersedia dan terjadi

Kode Risiko	Dampak
	gangguan dalam penyampaian informasi penting.
R08	Gangguan operasional server, website down, dan kehilangan data yang belum tersimpan.
R09	Kehilangan integritas data menyebabkan informasi tidak
R10	Website tidak dapat mengakses data, gangguan layanan informasi, dan informasi yang tidak update.
R11	Lambatnya respons website, potensi server crash, dan ketidakmampuan mengakses website.
R12	Fungsi website terganggu, tampilan tidak sesuai, dan kesulitan pengguna dalam mengakses informasi.
R13	Website tidak dapat diakses sehingga informasi cuaca dan maritim tidak tersedia dan terjadi penurunan kepercayaan pengguna.
R14	Kehilangan data historis, kesulitan pemulihan saat terjadi kerusakan sistem, dan tidak tersedianya data untuk analisis tren.
R15	Informasi cuaca dan maritim tidak akurat sehingga menyebabkan keputusan yang salah oleh pengguna dengan potensi membahayakan keselamatan.
R16	Informasi tidak tersedia tepat waktu menyebabkan keputusan yang terlambat oleh pengguna dengan potensi dampak pada keselamatan maritim.
R17	Kerusakan sistem, manipulasi atau pencurian data, serta gangguan layanan dan masalah reputasi.
R18	Kerusakan fisik pada perangkat keras, kehilangan data, dan gangguan layanan jangka panjang.

Pada Tabel 3, analisis dampak menunjukkan bahwa sebagian besar risiko berpotensi menimbulkan konsekuensi serius terhadap keselamatan maritim dan kualitas layanan. Risiko dengan dampak paling kritis adalah yang berkaitan dengan ketidakakuratan data dan keterlambatan informasi (R002, R015, R016), karena dapat menyebabkan pengambilan keputusan yang salah oleh pengguna dan berpotensi membahayakan keselamatan pelayaran. Risiko teknis seperti server down dan gangguan jaringan (R006, R007, R010, R013) berdampak pada ketidaktersediaan layanan informasi yang vital bagi komunitas maritim. Risiko keamanan seperti serangan siber (R017) tidak hanya mengancam integritas data tetapi juga reputasi institusi. Dampak ini menekankan pentingnya pengelolaan risiko yang komprehensif.

Analisis Risiko

Selanjutnya masuk ke tahapan analisis risiko, Informasi dampak risiko kemudian menjadi dasar dalam menentukan nilai risiko pada tahap berikutnya. Setelah risiko dan dampaknya dipetakan, langkah selanjutnya adalah melakukan analisis risiko dengan

menilai tingkat kemungkinan (likelihood) dan dampak (impact) menggunakan skala kualitatif sebagaimana ditunjukkan pada Tabel 4 dan Tabel 5.

Tabel 4. Kriteria Likelihood

Level	Deskripsi	Frekuensi
1	Rare	Hampir tidak mungkin terjadi (lebih dari 2 tahun)
2	Unlikely	Kemungkinan kecil terjadi (1 – 2 tahun)
3	Possible	Mungkin terjadi (7 - 11 bulan)
4	Likely	Kemungkinan besar terjadi (4 - 6 bulan)
5	Certain	Hampir pasti terjadi (1-3 bulan)

Tabel 4 dan Tabel 5 mendefinisikan skala penilaian likelihood dan impact secara kualitatif sebagai dasar penilaian risiko. Penilaian ini penting untuk mengidentifikasi seberapa sering sistem rentan terhadap gangguan yang sama di masa mendatang (Bistolen et al., 2024).

Tabel 5. Kriteria Impact

Level	Deskripsi	Frekuensi
1	Insignificant	Tidak mengganggu layanan website, dampak minimal
2	Minor	Gangguan kecil pada website, masih dapat diakses
3	Moderate	Gangguan sedang, beberapa fitur website tidak berfungsi
4	Mayor	Gangguan signifikan, website sulit diakses atau tidak akurat
5	Catastrophic	Website tidak berfungsi sama sekali, berdampak pada keselamatan maritim

Penilaian dampak semacam ini diperlukan agar organisasi dapat mengantisipasi risiko yang memiliki konsekuensi fatal (Yusuf et al., 2024). Kedua kriteria ini kemudian dikombinasikan untuk menghitung skor risiko tiap risiko yang telah diidentifikasi. Penilaian risiko ini disajikan pada Tabel 6 untuk penilaian risiko berdasarkan kriteria likelihood dan impact dari masing-masing risiko yang ada.

Tabel 6. Penilaian Risiko

Kode Risiko	Deskripsi Risiko	Likelihood	Impact
R01	Penyalahgunaan hak akses	1	5
R02	Kesalahan dalam menginputkan data	2	4
R03	Human error dalam pengelolaan data	2	3
R04	Kurangnya pelatihan	5	3
R05	Kerusakan perangkat keras	2	4
R06	Koneksi Internet tidak	3	5

Kode Risiko	Deskripsi Risiko	Likelihood	Impact
	stabil		
R07	Koneksi Jaringan terputus	3	5
R08	Pemadaman Listrik	1	4
R09	Data corrupt	1	5
R10	Database server down	1	5
R11	Overload server	1	5
R12	Bug atau error pada website	1	5
R13	Server down/tidak dapat diakses	1	5
R14	Kegagalan backup data	1	4
R15	Ketidakakuratan data	2	5
R16	Keterlambatan penyampaian informasi	2	5
R17	Serangan cyber (hacking)	1	5
R18	Bencana alam	1	5

Berdasarkan hasil penilaian kombinasi likelihood dan impact yang di tunjukkan pada Tabel 6, terdapat tiga risiko dengan tingkat risiko tinggi, yaitu R04, R06, dan R07. Risiko-risiko ini menjadi prioritas perlakuan karena dapat menghambat distribusi informasi cuaca secara akurat dan real-time. Selain itu, terdapat lima risiko berkategori sedang, yaitu R02, R03, R05, R15, dan R16. Risiko ini memiliki tingkat kemungkinan menengah dengan dampak signifikan jika tidak diantisipasi secara berkala. Sebanyak 10 risiko lainnya tergolong rendah, seperti R01, R08, R09, R10, R11, R12, R13, R14, R17, dan R18. Meski memiliki potensi dampak besar, nilai likelihood-nya rendah, sehingga penanganannya bisa bersifat monitoring berkala. Proses evaluasi risiko dilakukan guna menetapkan prioritas penanganan sesuai dengan tingkat risiko yang telah diidentifikasi. (Arif et al., 2024). Hasil penilaian pada Gambar 2, diperlihatkan posisi tiap risiko dalam matriks evaluasi menurut kemungkinan (likelihood) dan dampak (impact).

Likelihood	Certain	5			R04		
	Likely	4					
	Possible	3					R06, R07
	Unlikely	2			R03	R02, R05	R15, R16
	Rare	1				R08, R14	R01, R09, R10, R11, R12, R13, R17, R18
	Kriteria		1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Catastrophic
	Impact						

Gambar 2. Matriks Evaluasi Risiko

Hasil analisis likelihood dan impact kemudian dipetakan pada matriks evaluasi risiko pada gambar 2, guna menetapkan tingkat risiko secara keseluruhan

(Rendah, Sedang, dan Tinggi). Proses evaluasi ini berfungsi untuk mengidentifikasi risiko yang perlu ditangani segera serta risiko yang bisa dimonitor secara berkala. Kombinasi antara frekuensi kejadian dan besarnya dampak menjadi dasar utama dalam klasifikasi ini. Evaluasi ini juga memperlihatkan risiko mana yang paling mendesak untuk diberi perlakuan, terutama risiko dengan tingkat high seperti R004, R006 dan R007 serta R015 dan R016 yang lebih jelasnya bisa dilihat pada Tabel 7.

Tabel 7. Evaluasi Risiko

Kode Risiko	Deskripsi Risiko	Likelihood	Impact	Level Risiko
R01	Penyalahgunaan hak akses	1	5	Sedang
R02	Kesalahan dalam menginputkan data	2	4	Sedang
R03	Human error dalam pengelolaan data	2	3	Sedang
R04	Kurangnya pelatihan	5	3	Tinggi
R05	Kerusakan perangkat keras	2	4	Sedang
R06	Koneksi Internet tidak stabil	3	5	Tinggi
R07	Koneksi Jaringan terputus	3	5	Tinggi
R08	Pemadaman Listrik	1	4	Sedang
R09	Data corrupt	1	5	Sedang
R10	Database server down	1	5	Sedang
R11	Overload server	1	5	Sedang
R12	Bug atau error pada website	1	5	Sedang
R13	Server down/tidak dapat diakses	1	5	Sedang
R14	Kegagalan backup data	1	4	Sedang
R15	Ketidakakuratan data	2	5	Tinggi
R16	Keterlambatan penyampaian	2	5	Tinggi

Kode Risiko	Deskripsi Risiko	Likelihood	Impact	Level Risiko
	informasi			
R17	Serangan cyber (hacking)	1	5	Sedang
R18	Bencana alam	1	5	Sedang

Seperti pada Tabel 7, Hasil evaluasi risiko menunjukkan bahwa risiko dengan tingkat High (R04, R06, R07, R15, R16) perlu segera diprioritaskan. Berdasarkan wawancara, pengelola mengakui bahwa faktor SDM (pelatihan, human error) serta masalah jaringan merupakan tantangan utama saat ini. Selain itu, risiko ketidakakuratan dan keterlambatan informasi sangat dikhawatirkan karena bisa mengakibatkan kesalahan dalam pengambilan keputusan oleh pengguna, terutama nelayan dan pelaut.

Rekomendasi Strategi Perlakuan Risiko

Berdasarkan hasil evaluasi risiko, strategi perlakuan risiko dirumuskan dengan mengacu pada empat pendekatan utama: hindari, kurangi, alihkan, dan terima. Sebagian besar risiko direkomendasikan menggunakan strategi kurangi, karena risiko-risiko tersebut dapat ditindaklanjuti melalui peningkatan kompetensi SDM, pemeliharaan sistem, dan perbaikan infrastruktur jaringan. Pendekatan ini diterapkan pada risiko-risiko tinggi seperti kurangnya pelatihan, koneksi internet tidak stabil, dan gangguan jaringan.

Strategi alihkan digunakan untuk risiko bencana alam (R18), yang tidak dapat dikendalikan secara langsung oleh pengelola website. Alternatifnya adalah penyusunan Disaster Recovery Plan (DRP) dan perlindungan aset melalui asuransi. Sementara itu, strategi terima diterapkan pada risiko risiko tertentu seperti pemadaman listrik (R08), dengan mempertimbangkan bahwa dampaknya sudah diminimalkan melalui penggunaan UPS dan genset. Seluruh rekomendasi perlakuan risiko dijelaskan pada Tabel 8 dan disesuaikan dengan kondisi sumber daya dan infrastruktur BMKG Maritim Tanjung Perak.

Tabel 8. Pendekatan Strategi Perlakuan Risiko

No	Strategi	Penjelasan
1	Hindari	Menghindari aktivitas atau kondisi yang dapat memicu timbulnya risiko.
2	Kurangi	Mengurangi kemungkinan terjadinya risiko atau dampaknya melalui tindakan preventif atau protektif.
3	Alihkan	Mentransfer risiko kepada pihak lain, misalnya melalui kerja sama teknis atau asuransi.
4	Terima	Menerima risiko sebagaimana adanya jika dianggap tidak signifikan atau biaya

penanganannya terlalu tinggi.

Dari strategi yang ada pada Tabel 8, Strategi yang dipilih bertujuan agar pengelolaan risiko lebih terintegrasi dengan proses bisnis yang ada, sekaligus mempertimbangkan efisiensi penggunaan sumber daya. berikut adalah rekomendasi perlakuan risiko untuk website BMKG Maritim Tanjung Perak yang di tunjukkan pada Tabel 9.

Tabel 9. Rekomendasi Strategi Perlakuan Risiko

Kode Risiko	Deskripsi Risiko	Strategi	Tindakan Mitigasi
R01	Penyalahgunaan hak akses	Kurangi	Menerapkan sistem autentikasi berlapis dan audit log aktivitas pengguna.
R02	Kesalahan dalam menginputkan data	Kurangi	Memberikan pelatihan input data dan validasi otomatis pada form isian.
R03	Human error dalam pengelolaan data	Kurangi	Menyediakan SOP yang jelas dan pelatihan berkala bagi petugas.
R04	Kurangnya pelatihan	Kurangi	Melakukan pelatihan rutin dan evaluasi kompetensi pengguna sistem.
R05	Kerusakan perangkat keras	Kurangi	Pemeliharaan perangkat keras secara berkala dan memiliki perangkat cadangan.
R06	Koneksi Internet tidak stabil	Kurangi	Berlangganan ke penyedia internet yang andal dan menyediakan koneksi cadangan.
R07	Koneksi Jaringan terputus	Kurangi	Meningkatkan infrastruktur jaringan internal dan menyiapkan backup koneksi.
R08	Pemadaman Listrik	Terima	Menggunakan UPS dan genset serta kerja sama dengan penyedia listrik.
R09	Data corrupt	Kurangi	Melakukan backup berkala dan pengecekan integritas data.
R10	Database server down	Kurangi	Menyediakan sistem monitoring server dan jadwal pemeliharaan rutin.
R11	Overload server	Kurangi	Melakukan optimasi sistem dan kapasitas server, serta load balancing.
R12	Bug atau error pada website	Kurangi	Menerapkan proses pengujian (testing) sebelum deployment

Kode Risiko	Deskripsi Risiko	Strategi	Tindakan Mitigasi
R13	Server down/tidak dapat diakses	Kurangi	dan perbaikan rutin. Pemantauan server 24/7, implementasi sistem notifikasi kegagalan
R14	Kegagalan backup data	Kurangi	Otomatisasi proses backup dan penyimpanan backup di lokasi yang berbeda.
R15	Ketidakakuratan data	Kurangi	Implementasi proses validasi data multi-tahap, dan audit data secara berkala.
R16	Keterlambatan penyampaian informasi	Kurangi	Otomatisasi proses penyampaian informasi dan prioritasasi informasi berdasarkan urgensi.
R17	Serangan cyber (hacking)	Kurangi	Implementasi firewall dan sistem deteksi intrusi, audit keamanan secara berkala.
R18	Bencana alam	Alihkan	Pengembangan Disaster Recovery Plan (DRP), asuransi untuk peralatan dan infrastruktur.

Pada Tabel 10, Setelah dilakukan pemetaan terhadap risiko yang telah dievaluasi strategi perlakuan risiko difokuskan pada pendekatan kurangi (pengurangan risiko) karena sebagian besar risiko yang dihadapi memiliki dampak signifikan terhadap layanan informasi cuaca dan maritim. Pendekatan ini mencakup tindakan-tindakan preventif seperti peningkatan infrastruktur, pelatihan personel, optimasi sistem, serta penguatan prosedur pengelolaan data. Strategi ini diambil dengan mempertimbangkan keterbatasan sumber daya dan karakteristik organisasi. Selain strategi kurangi, beberapa risiko juga ditangani melalui pendekatan Terima, Kurangi dan Alihkan.

Dengan strategi-strategi tersebut, diharapkan organisasi dapat mengurangi tingkat risiko yang ada ke level yang dapat diterima, sekaligus meningkatkan kesiapan dalam menghadapi potensi gangguan di masa depan. Perencanaan perlakuan risiko ini juga bisa menjadi dasar dalam penyusunan kebijakan manajemen risiko yang berkelanjutan di lingkungan BMKG Maritim Tanjung Perak.

Hasil penelitian menunjukkan bahwa risiko yang paling dominan berasal dari faktor SDM dan jaringan, sesuai dengan pernyataan pengelola bahwa keterbatasan teknis dan kapasitas personel sering menjadi penghambat dalam penyampaian informasi. Hal ini sejalan dengan beberapa studi sebelumnya yang menegaskan pentingnya penguatan SDM dan

tata kelola sistem dalam konteks manajemen risiko teknologi informasi. Temuan ini juga menunjukkan bahwa pendekatan ISO 31000 dapat diterapkan secara adaptif pada instansi pemerintah dengan menyesuaikan tahapan analisis terhadap kondisi operasional.

Penerapan strategi perlakuan risiko yang berfokus pada tindakan preventif dinilai relevan mengingat website berperan sebagai sumber informasi kritis bagi keselamatan pelayaran. Penguatan prosedur, pelatihan, dan perbaikan infrastruktur menjadi aspek yang sangat dibutuhkan. Dengan demikian, penelitian ini memberikan gambaran komprehensif mengenai risiko operasional website maritim dan dapat menjadi dasar bagi pengembangan kebijakan manajemen risiko yang lebih terstruktur di BMKG.

Seperti dalam penelitian (Veronika Trinovianti, 2023) menyatakan bahwa strategi berbasis konteks sangat efektif diterapkan di institusi publik berskala menengah. Namun demikian, keberhasilan implementasi sangat ditentukan oleh komitmen struktural. Pentingnya dukungan manajemen agar strategi tidak berhenti pada dokumen, tetapi diimplementasikan sebagai bagian dari budaya organisasi. Selain itu, komunikasi risiko juga menjadi aspek krusial. Dalam jurnal (Astuti et al., 2025) menunjukkan bahwa komunikasi rutin antara teknisi dan manajemen dapat menurunkan frekuensi kesalahan dan meningkatkan kesiapan organisasi. Dalam konteks BMKG, komunikasi risiko dapat dilakukan melalui pelatihan berkala dan review internal prosedur operasional. Sementara itu, penelitian (Euggelion Kevin Usmany, 2025) menegaskan bahwa penerapan ISO 31000:2018 memungkinkan organisasi untuk memilih strategi perlakuan risiko yang tepat hindari, kurangi, alihkan, atau terima serta menekankan pentingnya pelatihan keamanan berkelanjutan dan dokumentasi insiden sebagai bagian dari mitigasi risiko yang efektif

KESIMPULAN DAN SARAN

Berdasarkan hasil analisis menggunakan kerangka kerja ISO 31000:2018, diperoleh 18 potensi risiko teridentifikasi yang dapat mengganggu operasional sistem informasi pada website BMKG Maritim Tanjung Perak. Risiko tersebut dikelompokkan ke dalam tiga kategori utama, yaitu sumber daya manusia (SDM), sistem dan infrastruktur, serta bencana alam. Hasil evaluasi menunjukkan bahwa lima risiko termasuk dalam kategori tinggi, seperti kurangnya pelatihan SDM dan gangguan koneksi jaringan yang berdampak pada keterlambatan penyampaian informasi. Sebagai tindak lanjut, disusun strategi perlakuan risiko yang bersifat preventif dan kontekstual melalui pendekatan

pengurangan risiko (risk reduction), dengan fokus pada peningkatan kompetensi SDM dan optimalisasi infrastruktur jaringan. Temuan ini menegaskan perlunya penerapan manajemen risiko yang terstruktur untuk menjaga keandalan dan keberlanjutan layanan informasi cuaca maritim di lingkungan BMKG. Untuk pengembangan lebih lanjut, disarankan adanya evaluasi terhadap efektivitas penerapan strategi risiko secara berkelanjutan serta pengembangan sistem mitigasi berbasis otomatisasi guna meningkatkan ketahanan sistem informasi publik di sektor maritim.

UCAPAN TERIMA KASIH

Penulis berterima kasih kepada BMKG Maritim Tanjung Perak, khususnya tim teknis dan pengelola sistem informasi, atas bantuan dalam proses pengumpulan data. Ucapan terima kasih juga disampaikan kepada dosen pembimbing atas bimbingan dan dukungan selama proses penelitian.

DAFTAR PUSTAKA

- Anggreani, M., Maria, P., Informasi, T., Informasi, S., Kristen, U., & Wacana, S. (2025). *Analisis Manajemen Risiko Pada Sistem Informasi Kurikulum Saraswati Menggunakan ISO*. 10, 89–101.
- Arif, G. S., Erliani, Y., & Ratnasari, A. (2024). Analysis of Risk Management Using E-Office Application with ISO 31000:2018 in National Public Procurement Agency (NPPA/LKPP). *Airlangga Journal of Innovation Management*, 5(2), 260–277. <https://doi.org/10.20473/ajim.v5i2.56656>
- Astuti, B., Zidan, & Vista, U. F. (2025). Analisis Manajemen Risiko Teknologi Informasi Pada Aplikasi LMS Sevima Edlink Menggunakan Framework ISO 31000 (Studi Kasus: Prodi Teknologi Informasi). *Jurnal Manajemen Risiko*, 06(01), 53–68.
- Aziz, H., & Muharam, Q. (2024). *Information System Risk Assessment on Website Jogja Smart Service using ISO 31000*. 186(43), 15–20.
- Badan Meteorologi Klimatologi dan Geofisika. (2023). *Informasi Maritim Tanjung Perak*. <https://maritim.bmkg.go.id>
- Bayu, B. I., Syamsul, S. M., & Widodo, W. R. (2024). Reputational risks management and mitigation: Empirical evidence from the wedding organizer sector. *Jurnal Siasat Bisnis*, 28(1), 71–87. <https://doi.org/10.20885/jsb.vol28.iss1.art5>
- Bistolen, B., Manesi, D., Haris Maulana, I., Agung Aulia, D., Yazı Pawana, F., Zakaria, B., Desi Nahak, F., Permesinan Kapal, P., Logistik Militer, F., & Perthanan, U. R. (2024). Sosialisasi Peran BMKG Bagi Nelayan Desa Harekakae Dalam Meningkatkan Produksi Perikanan Dan Keselamatan Dalam Berlayar. *Jurnal Abdi Masyarakat Vokasi (AMARASI)*, 1(1), 39–44.
- Euggelion Kevin Usmany. (2025). Information Security Planning with Risk Management Using ISO 31000:2018 at E-Commerce XYZ. *Journal of Information Systems Engineering and Management*, 10(33s), 75–89. <https://doi.org/10.52783/jisem.v10i33s.5460>
- Herlambang, A. A., Gani, A. A., & Alvianto, D. D. (2024). *Pendekatan ISO 31000: 2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April ISO 31000: 2018 Approach to Information Technology Risk Management in the Tracer Study at Universitas Sebelas April*. September, 5651–5660.
- Junior, F. X. M. R. M., Jimmy, J., & Tambotuh, C. (2025). *INFORMASI (Jurnal Informatika dan Sistem Informasi) Volume 17 No.1 / Mei / 2025*. 17(1), 1–18.
- Lathifah Agustina Wicahyani, N., & Salman, M. (2023). Penentuan Kriteria Dampak Risiko Keamanan Informasi, Mutu, dan Layanan Pada Layanan Jaringan Komunikasi di BMKG. *Smart Comp: Jurnalnya Orang Pintar Komputer*, 12(4). <https://doi.org/10.30591/smartcomp.v12i4.5990>
- Marhaditha, S., & Pangeran, P. (2022). Supply Chain Risk Management Based on ISO 31000:2018 - Balanced Scorecard to Improve Company Performance: Case Study on UD INTR Yogyakarta. *International Journal of Social Science Reserch and Review*, 5(11), 307–319. <http://dx.doi.org/10.47814/ijssrr.v5i11.705>
- Masita, I. (2022). Analysis of Risk Management Implementation In The Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya Using ISO 31000. *Robust: Research of Business and Economics Studies*, 2(2), 113. <https://doi.org/10.31332/robust.v2i2.3691>
- Maynard, R., Sinulingga, A., Raharjo, T., & Trisnawaty, N. W. (2024). *Jurnal Informatika Ekonomi Bisnis Risk Management Design and Analysis on Agile Development Project using ISO 31000 Integrated with ISO 27005: A Case Study of SiREV Application*. 6, 4–10. <https://doi.org/10.37034/infv.v6i4.1053>
- Mesin, J. T., Informatika, E., & April, U. S. (2025). *Manajemen Risiko Keamanan Aset Teknologi Informasi di DISKOMINFOSANDITIK Kabupaten Sumedang Menggunakan ISO*. 4.
- Pratama Dinatha, J., & Rangga, R. (2024). Analisis Manajemen Resiko Proyek Menggunakan Framework Iso 31000. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 8(3), 4276–4284. <https://doi.org/10.36040/jati.v8i3.9901>
- Putri, N. N., & Rudianto, C. (2025). *Penerapan Framework ISO 31000: 2018 dalam Menganalisis Manajemen Risiko pada Aplikasi e - Poin Implementation of ISO 31000: 2018 Framework in Risk Management Analysis of e -*

Poin Application. 14, 249–261.

- Veronika Trinovianti, A. Z. (2023). Jurnal Sistem Informasi dan Aplikasi. *Jurnal Sistem Informasi Dan Aplikasi (JSIA)*, 1(1), 50–64. <https://ejournal.uprvj.ac.id/jsia/article/view/5907>
- Yusuf, M. S., Swastyastu, C. A., Syahadianti, L., & Shanty, R. N. T. (2024). Analisa Manajemen Risiko E-Learning Universitas Dr. Soetomo Surabaya Menggunakan Framework ISO 31000. *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, 13(1), 314. <https://doi.org/10.35889/jutisi.v13i1.1800>