**Journal of Information System, Applied, Management, Accounting and Research.**
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
**e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)**

# PENERAPAN ISO 31000 DALAM ANALISIS RISIKO PENGELOLAAN SISTEM INFORMASI TATA RUANG (SITR) JAWA TIMUR

**Alvina Waihda Ardhani[1*], Noor Wahyudi[2], Yunita Ardilla[3]**

Program Studi Sistem Informasi[123],
Fakultas Sains dan Teknologi[123],
Universitas Islam Negeri Sunan Ampel[123]

Correspondent Email: alvinawaihda@gmail.com

Author Email: alvinawaihda@gmail.com[1] n.wahyudi@uinsa.ac.id[2]
yunita.ardilla@uinsa.ac.id[3]

**Received:** September 30, 2025**. Revised:** October 20, 2025**. Accepted:** October 22,20025**. Issue Period:** Vol.9 No.4 (2025), Pp: 1465-1476

**Abstrak:** Perkembangan teknologi informasi dalam sektor pemerintahan menuntut adanya pengelolaan sistem yang efektif, aman, dan berkelanjutan. Sistem Informasi Tata Ruang (SITR) Jawa Timur memiliki peran strategis dalam penyediaan data spasial dan non-spasial yang mendukung transparansi informasi, perencanaan pembangunan, serta pengambilan keputusan berbasis data. Namun, ketergantungan tinggi pada sistem digital menimbulkan potensi risiko yang dapat mengganggu keandalan dan kualitas layanan publik, baik dari aspek teknis seperti gangguan keamanan dan infrastruktur, maupun dari aspek non-teknis seperti kompetensi sumber daya manusia. Penelitian ini bertujuan menganalisis risiko pada SITR Jawa Timur dengan kerangka kerja ISO 31000 melalui pendekatan kualitatif deskriptif menggunakan teknik Risk and Self Control Assessment (RSCA). Data dikumpulkan melalui wawancara terstruktur dengan staf IT dan observasi langsung di instansi pengelola, kemudian dianalisis melalui proses identifikasi, analisis, dan evaluasi risiko. Hasil penelitian menemukan 11 potensi risiko dengan klasifikasi 1 risiko tinggi terkait keamanan siber, 6 risiko tingkat sedang yang mencakup kelemahan manajemen data dan kompetensi SDM, serta 4 risiko tingkat rendah terkait operasional sistem. Temuan ini berkontribusi dalam pemetaan risiko yang lebih terstruktur dan penyusunan rekomendasi mitigasi strategis yang dapat memperkuat tata kelola teknologi informasi pemerintah, khususnya dalam pengelolaan sistem informasi geospasial untuk mewujudkan prinsip transparansi dan akuntabilitas good governance.

**Kata kunci:** Manajemen Risiko: Sistem Informasi Tata Ruang: ISO 31000

***Abstract:*** *The East Java Spatial Information System (SITR) plays a strategic role in providing spatial and non-spatial data to support information transparency, development planning, and data-driven decision-making. However, the high reliance on digital systems creates potential risks that may disrupt the reliability and quality of public services, both from technical aspects such as cybersecurity threats and infrastructure failures, and non-technical aspects such as human resource*

**DOI:** 10.52362/jisamar.v9i4.2104

**Journal of Information System, Applied, Management, Accounting and Research.**
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
**e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)**

*competence. This study aims to analyze risks in the East Java SITR using the ISO 31000 framework through a qualitative descriptive approach with the Risk and Self Control Assessment (RSCA) technique. Data were collected through structured interviews with IT staff and direct observations at the managing institution, then analyzed through the processes of risk identification, analysis, and evaluation. The findings identified 11 potential risks classified into one high risk related to cybersecurity, six medium risks covering data management weaknesses and staff competence, and four low risks associated with system operations. These findings contribute to a more structured risk mapping and provide strategic mitigation recommendations to strengthen government information technology governance, particularly in managing geospatial information systems to realize transparency and accountability in good governance*

***Keywords:*** *Risk Management: Spatial Information System: ISO 31000*

## I. PENDAHULUAN

Perkembangan teknologi informasi (TI) telah membawa transformasi besar dalam berbagai sektor, baik pada pemerintahan, pendidikan, bisnis, maupun layanan publik. Pemanfaatan TI yang semakin luas menjadikan organisasi semakin bergantung pada sistem informasi untuk mendukung operasional harian, pengambilan keputusan, hingga penyediaan layanan berbasis digital [6]. Namun, tingginya ketergantungan terhadap teknologi juga diiringi dengan munculnya beragam risiko, seperti kegagalan sistem, serangan siber, dan kesalahan manusia [7]. Oleh karena itu, berbagai penelitian menunjukkan pentingnya manajemen risiko TI untuk memastikan keberlanjutan dan keamanan sistem informasi [1].

Untuk menghadapi tantangan tersebut, penerapan manajemen risiko teknologi informasi menjadi sangat penting. Manajemen risiko berperan dalam mengidentifikasi, menganalisis, dan mengevaluasi potensi ancaman agar organisasi mampu menjaga keberlanjutan dan keamanan sistem [1]. Salah satu kerangka kerja yang banyak digunakan adalah ISO 31000 karena menyediakan prinsip, kerangka, dan proses sistematis untuk mengelola risiko secara efektif [4]. Beberapa penelitian sebelumnya juga membuktikan efektivitas ISO 31000 dalam penerapan manajemen risiko pada berbagai sistem informasi [5].

Sistem Informasi Tata Ruang (SITR) merupakan platform digital yang dirancang untuk mengelola, menyimpan, dan menyediakan data spasial maupun non-spasial terkait penataan ruang wilayah [8]. SITR Jawa Timur, yang dikelola oleh Dinas Perumahan Rakyat, Kawasan Permukiman, dan Cipta Karya Provinsi Jawa Timur, berfungsi sebagai sumber data tata ruang yang dapat dimanfaatkan masyarakat, instansi pemerintah, maupun pihak swasta [9]. Aplikasi Jatim Pintar sebagai manifestasi SITR memuat RTRW Provinsi Jawa Timur serta data spasial dari 38 Kabupaten/Kota yang dapat diakses secara luas oleh publik [10]. Kehadiran aplikasi ini berperan penting dalam mendukung transparansi informasi, perencanaan pembangunan, dan penerapan tata kelola pemerintahan yang baik (good governance) [15].

Meski memiliki manfaat strategis, SITR tetap menghadapi berbagai risiko yang dapat menghambat efektivitasnya. Risiko tersebut mencakup aspek teknis seperti gangguan keamanan, ketersediaan, dan integritas data, serta aspek non-teknis seperti keterbatasan kompetensi sumber daya manusia dan kepatuhan terhadap regulasi [11]. Oleh karena itu, analisis risiko berbasis ISO 31000 menjadi relevan untuk dilakukan. Hasil penelitian berhasil mengidentifikasi dan mengklasifikasikan 11 kategori risiko, dengan satu risiko tingkat tinggi yang berkaitan dengan keamanan siber, enam risiko tingkat sedang terkait manajemen data dan kompetensi SDM, serta empat risiko tingkat rendah yang berkaitan dengan operasional sistem [2].

Hasil penelitian berhasil mengidentifikasi dan mengklasifikasikan 11 kategori risiko berdasarkan tingkat keparahan dan probabilitas kejadiannya, dengan satu risiko tingkat tinggi yang berkaitan dengan keamanan siber akibat lemahnya perlindungan sistem dari ancaman peretasan dan virus yang berpotensi mengganggu integritas serta ketersediaan data, enam risiko tingkat sedang yang mencakup permasalahan dalam pengelolaan data dan keterbatasan kompetensi sumber daya manusia seperti kelalaian menjaga kerahasiaan informasi, kesalahan penggunaan sistem akibat kurangnya pelatihan, tidak adanya mekanisme cadangan data yang memadai, lemahnya prosedur pemeliharaan sistem, serta otorisasi akses yang tidak optimal, dan empat risiko tingkat

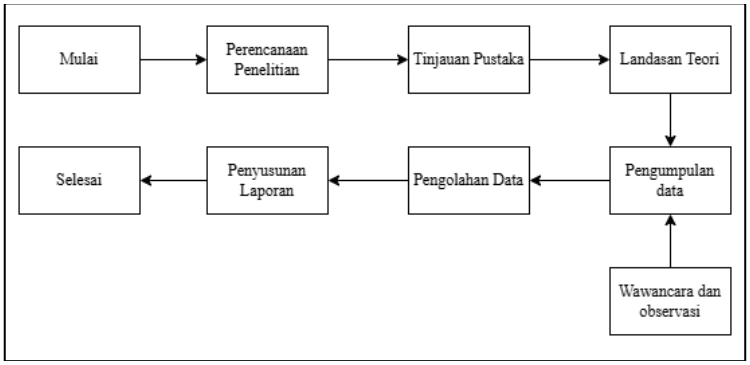
**DOI:** 10.52362/jisamar.v9i4.2104

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)

rendah yang lebih berhubungan dengan aspek operasional seperti kesulitan penggunaan sistem, error yang mengganggu pekerjaan, downtime berkepanjangan, dan keterbatasan akses layanan tertentu. Kontribusi utama penelitian ini adalah penyusunan kerangka analisis risiko berbasis ISO 31000 yang bersifat spesifik untuk sistem informasi geospasial pemerintah, di mana hasil identifikasi tidak hanya menggambarkan kondisi aktual risiko pada SITR Jawa Timur, tetapi juga disertai rekomendasi mitigasi strategis yang dapat langsung diimplementasikan oleh instansi pengelola, seperti penguatan keamanan siber melalui penerapan firewall, antivirus, dan pembaruan sistem secara berkala, penyusunan SOP yang lebih ketat, serta peningkatan kapasitas pegawai melalui pelatihan rutin agar kesalahan manusia dapat diminimalisasi. Dengan demikian, penelitian ini tidak hanya memberikan kontribusi teoretis melalui pengembangan kerangka manajemen risiko, tetapi juga kontribusi praktis berupa rekomendasi nyata yang diharapkan dapat dijadikan rujukan dalam perumusan kebijakan keamanan informasi serta peningkatan tata kelola TI di sektor publik, khususnya untuk sistem informasi geospasial yang memiliki peran strategis dalam mendukung transparansi, akuntabilitas, dan penerapan good governance di lingkungan pemerintahan.

## II. METODE DAN MATERI

Penelitian ini menggunakan pendekatan kualitatif dengan pemaparan data secara deskriptif. Pendekatan kualitatif dipilih untuk memahami secara mendalam tentang manajemen risiko yang dialami pada Sistem Informasi Tata Ruang (SITR) Jawa Timur. Adapun situasi sosial yang dideskripsikan adalah bagaimana manajemen risiko menggunakan kerangka kerja ISO 31000 dapat diterapkan di instansi tersebut untuk mengelola risiko keamanan aset teknologi informasi [12] dan sistem informasi secara menyeluruh [11]. Proses pengumpulan data dilakukan melalui wawancara langsung dengan pihak-pihak terkait yang berperan penting dalam manajemen sistem. Wawancara ini bertujuan untuk mengetahui kondisi sebenarnya di lapangan, serta untuk mengumpulkan informasi yang tidak dapat dijelaskan dengan pendekatan kuantitatif, seperti pandangan dan pengalaman pengguna. Selain wawancara, peneliti juga menggunakan observasi langsung di Dinas Perumahan Rakyat, Kawasan Permukiman dan Cipta Karya Provinsi Jawa Timur, tempat dilakukannya penelitian ini.




Gambar 1. Alur Penelitian

### 2.1. Sistem Informasi Tata Ruang (SITR)

Sistem Informasi Tata Ruang (SITR) merupakan platform digital yang dikembangkan untuk mengelola, mengarsipkan, dan menyajikan data spasial maupun non-spasial terkait penataan ruang wilayah, dimana SITR Jawa Timur dioperasikan oleh Dinas Perumahan Rakyat, Kawasan Permukiman dan Cipta Karya sebagai sarana penyediaan informasi penataan ruang meliputi RTRW, RDTR, dan data pemanfaatan ruang lainnya kepada masyarakat dan stakeholder terkait. Platform ini juga mendukung proses perizinan, monitoring, dan evaluasi penataan ruang, sehingga memerlukan implementasi manajemen risiko yang menyeluruh untuk menjamin kontinuitas dan reliabilitas sistem dalam memberikan pelayanan publik yang optimal.

### 2.2. Manajemen Risiko

Manajemen risiko adalah proses terstruktur dan sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang dapat memengaruhi pencapaian tujuan organisasi [1]. Proses ini bersifat iteratif dan

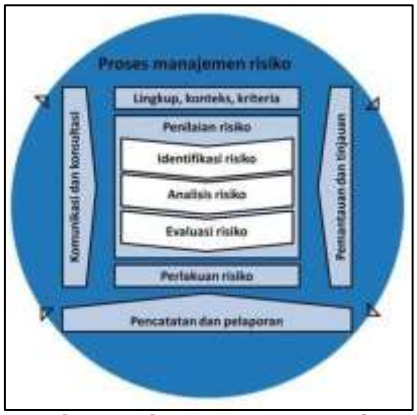
DOI: 10.52362/jisamar.v9i4.2104

**Journal of Information System, Applied, Management, Accounting and Research.**
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
**e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)**

membantu organisasi dalam menciptakan serta melindungi nilai [4]. Tujuannya adalah untuk memonitor operasional secara ketat untuk mencegah penyimpangan dan potensi kerugian [12]. Proses manajemen risiko melibatkan beberapa tahapan utama yang saling terkait [5]. Tahapan ini dimulai dari penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, hingga penanganan risiko [12]. Semua tahapan tersebut didukung oleh komunikasi, konsultasi, serta pemantauan dan tinjauan yang berkelanjutan [5]. Seluruh proses ini sangat penting untuk memastikan keberlanjutan dan efektivitas suatu sistem atau organisasi [7].

2.3. Standar ISO 31000

Sistem manajemen, terutama yang telah diakui secara internasional seperti ISO 31000, merupakan serangkaian praktik yang telah terbukti efektif dan dibentuk melalui pengalaman [4]. Standar ini dirancang untuk memberikan panduan umum serta prinsip dasar dalam pelaksanaan manajemen risiko, yang mencakup prinsip-prinsip, kerangka kerja, dan proses untuk membentuk sistem manajemen risiko yang terstruktur [12]. Prinsip-prinsip tersebut menjadi dasar bagi kerangka kerja dan prosesnya, sementara kerangka kerja berfungsi sebagai struktur pendukung dalam penerapan proses manajemen risiko [13]. ISO 31000 juga digunakan oleh perusahaan untuk menciptakan dan melindungi nilai perusahaan melalui pengelolaan risiko dalam setiap perencanaan dan pengambilan keputusan [12], serta untuk mencapai sasaran dan tujuan perusahaan, dan mendukung perbaikan kinerja [5]. Manajemen risiko merupakan penerapan terstruktur dari kebijakan, prosedur, dan praktik yang terintegrasi dengan struktur, operasional, serta proses dalam organisasi [11].



Gambar 2. Alur Manajemen Risiko

## III. PEMBAHASA DAN HASIL

3.1. Penetapan Lingkup

Lingkup manajemen risiko dalam penelitian ini mencakup seluruh aspek yang berkaitan dengan pengoperasian dan pengelolaan Sistem Informasi Tata Ruang (SITR) di Dinas Perumahan Rakyat, Kawasan Permukiman, dan Cipta Karya Provinsi Jawa Timur. Lingkup ini meliputi:Infrastuktur komponen SITR : Aplikasi web, server, jaringan, database, API. Penetapan tanggung jawab: Menetapkan batas-batas tanggung jawab dalam pengelolaan risiko yaitu Tim IT. Cakupan sistem merupakan batasan sistem yang dianalisis seluruh aspek teknik dan operasional dari SITR yang beroperasi di Dinas Perumahan Rakyat, Kawasan Permukiman dan Cipta Karya Provinsi Jawa Timur.

3.2. Konteks

Konteks manajemen risiko ditetapkan dengan memahami situasi dan kondisi di mana website SITR (Sistem Informasi Tata Ruang) beroperasi, termasuk faktor internal dan eksternal yang dapat mempengaruhi munculnya risiko dari fakto eksternal yaitu trend ancaman online, ekpetasi pengguna, standar keamanan siber, dan regulasi data pribadi. Sedangkan dari faktor internal yaitu infrastuktur IT DPRKPCK, kapasitas SDM pengelola sistem, dan kebijakan keamanan informasi.

**DOI:** 10.52362/jisamar.v9i4.2104

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)

3.3. Kriteria

Kriteria risiko SITR menggunakan dua parameter utama yaitu skala kemungkinan dari "Sangat Jarang" (>5 tahun sekali) hingga "Sangat Sering" (1-12 bulan) berdasarkan frekuensi historis, dan skala dampak dari "Tidak Berpengaruh" hingga "Sangat Besar" terhadap ketersediaan, keandalan, dan keamanan sistem. Kedua parameter diintegrasikan dalam matriks risiko 5x5 yang mengklasifikasikan risiko menjadi kategori Tinggi (merah), Sedang (kuning), dan Rendah (hijau), kemudian ditetapkan ambang batas risiko sebagai dasar prioritas penanganan dan alokasi sumber daya.Coba lagi Claude dapat membuat kesalahan. Periksa kembali setiap respons.

3.4. Penilaian Risiko

Penilaian risiko meupakan bagian penting dari proses anajemen risiko yang meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko. Pada bagian ini, akan dibahas hasil penilaian risiko yang telah dilakukan pada website Sistem Informasi Tata Ruang (SITR) di Dinas Perumahan Rakyat, Kawasan Permukiman, dan Cipta Karya Jawa Timur berdasarkan hasil wawancara dengan pihak pengelola.

3.5. Identifikasi Risiko

Identifikasi risiko pelayanan pada Sistem Informasi Tata Ruang (SITR) di Dinas Perumahan Rakyat, Kawasan Permukiman, dan Cipta Karya Jawa Timur dilakukan melalui metode analisis yang sistematis dengan pendekatan wawancara mendalam kepada staf yang memiliki tanggung jawab langsung dalam bidang pelayanan. Seluruh informasi dan data yang diperoleh dari hasil wawancara tersebut kemudian dikompilasi secara terstruktur dan dianalisis secara komprehensif untuk mengidentifikasi berbagai potensi risiko yang mungkin muncul dalam operasional sistem, serta menganalisis konsekuensi atau dampak negatif yang dapat ditimbulkan dari setiap jenis risiko yang telah teridentifikasi.

Tabel I. Identifikasi Kemungkinan Risiko

| Faktor | ID | Kemungkinan Risiko |
|---|---|---|
| Manusia | R01 | Pegawai kesulitan dalam menggunakan sistem |
| | R02 | Pegawai ceroboh menjaga kerahasiaan data |
| | R03 | Pegawai yang belum dilatih bisa salah menggunakan sistem |
| Sistem dan Infrastuktur | R04 | Sistem sering error dan mengganggu pekerjaan |
| | R05 | Sistem kadang tidak bisa diakses |
| | R06 | Tidak ada backup data dan data bisa hilang |
| | R07 | Sistem tidak memiliki perlindungan memadai terhadap serangan virus dan peretasan |
| | R08 | Akses data tidak terbatas sehingga meningkatkan risiko penyalahgunaan |
| | R09 | Tidak ada prosedur rutin untuk memastikan sistem berjalan dengan baik |
| | R10 | Sistem mengalami downtime dalam durasi yang cukup lama |
| | R11 | Pengaturan otorisasi akses pengguna belum dilakukan dengan baik |

Pada tabel 1 menampilkan hasil identifikasi risiko awal yang muncul pada pengelolaan Sistem Informasi Tata Ruang (SITR) Jawa Timur. Proses identifikasi dilakukan melalui wawancara dengan pihak pengelola sistem serta observasi langsung. Risiko yang teridentifikasi terbagi menjadi dua faktor utama, yaitu faktor manusia dan faktor sistem/infrastruktur. Dari faktor manusia, ditemukan beberapa risiko seperti kesulitan pegawai dalam menggunakan sistem (R01), kelalaian dalam menjaga kerahasiaan data (R02), serta kesalahan penggunaan sistem akibat kurangnya pelatihan (R03). Sementara itu, dari faktor sistem dan infrastruktur, risiko yang muncul mencakup gangguan teknis seperti sistem sering error (R04), downtime berkepanjangan (R10), hingga kelemahan mendasar berupa ketiadaan backup data (R06), keterbatasan perlindungan terhadap ancaman siber (R07), dan akses data yang tidak terbatas (R08). Identifikasi ini menjadi dasar penting untuk analisis lanjutan karena dapat memetakan sumber potensi masalah baik dari sisi teknis maupun non-teknis.

Tabel II. Identifikasi Dampak Risiko

DOI: 10.52362/jisamar.v9i4.2104

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)

| ID | Dampak |
|---|---|
| R01 | - Penurunan produktivitas kerja<br>- Kesalahan input data yang menyebabkan informasi tidak akurat<br>- Penundaan dalam penyelesaian tugas |
| R02 | - Kebocoran data sensitif<br>- Penyalahgunaan data oleh pihak yang tidak berwenang<br>- Kerugian finansial dan reputasi organisasi |
| R03 | - Data yang tidak akurat atau tidak lengkap<br>- Kesalahan operasional yang mengganggu fungsi sistem<br>- Kerusakan pada sistem akibat penggunaan yang tidak tepat |
| R04 | - Terhambat proses pelayanan<br>- Penumpukan pekerjaan<br>- Ketidakpuasan penggunaan layanan<br>- Menurunnya kepercayaan terhadap keandalan sistem |
| R05 | - Keterlambaan dalam pengambilan Keputusan<br>- Ketidakmampuan untuk mengakses data penting saat dibutuhkan |
| R06 | - Kehilangan data secara permanen<br>- Biaya dan waktu yang besar untuk pemulihan data |
| R07 | - Pencurian data sensitif<br>- Manipulasi data oleh pihak tidak bertanggung jawab<br>- Biaya besar untuk pemulihan sistem setelah serangan<br>- Gangguan pada integrasi dan ketersediaan sistem |
| R08 | - Pelanggaran privasi<br>- Kebocoran informasi rahasia<br>- Penyalahgunaan data untuk kepentingan pribadi |
| R09 | - Potensi kehilangan data penting<br>- Penurunan kinerja sistem secara bertahan<br>- Gangguan sistem yang mendadak dan sering |
| R10 | - Penundaan layanan<br>- Gangguan pada operasional sehari-hari |
| R11 | - Penyalahgunaan hak akses<br>- Kesulitan dalam melacak aktivitas pengguna<br>- Ketidaksesuaian dengan prinsip keamanan informasi |

Setelah mengidentifikasi dampak dari setiap risiko yang telah diidentifikasi pada Sistem Informasi Tata Ruang (SITR) Jawa Timur. Dampak tersebut bervariasi mulai dari gangguan operasional, seperti menurunnya produktivitas kerja dan keterlambatan layanan (R01, R04, R10), hingga konsekuensi serius berupa kebocoran data sensitif, kerugian reputasi, serta potensi kehilangan data permanen (R02, R06, R07). Beberapa risiko lain juga berdampak pada kualitas sistem, misalnya akses data yang tidak terbatas yang dapat menimbulkan penyalahgunaan (R08) serta otorisasi yang tidak memadai yang berisiko pada pelanggaran keamanan informasi (R11). Secara keseluruhan, tabel ini menegaskan bahwa dampak risiko SITR tidak hanya bersifat teknis, tetapi juga menyangkut aspek strategis organisasi, sehingga perlu mendapat perhatian khusus dalam analisis risiko selanjutnya.

3.6. Analisis Risiko

Setelah risiko teridentifikasi, langkah selanjutnya adalah melakukan analisis risiko untuk menentukan tingkat risiko berdasarkan kriteria likelihood (kemungkinan terjadinya risiko) dan impact (dampak jika risiko terjadi). Berikut adalah kriteria yang digunakan dalam analisis risiko:

Tabel III. Kriteria Likelihood

DOI: 10.52362/jisamar.v9i4.2104

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)

| Nilai | Kriteria | Deskripsi |
|---|---|---|
| 1 | Rare | Hampir tidak mungkin terjadi (lebih dari 2 tahun) |
| 2 | Unlikely | Kemungkinan kecil terjadi (1 – 2 tahun) |
| 3 | Possible | Mungkin terjadi (7 - 12 bulan) |
| 4 | Likely | Kemungkinan besar terjadi (4 - 6 bulan) |
| 5 | Certain | Hampir pasti terjadi (1-3 bulan) |

Tabel 3 menjelaskan parameter yang digunakan untuk mengukur tingkat kemungkinan terjadinya risiko (likelihood). Skala penilaian dibagi ke dalam lima tingkatan, mulai dari Rare (1) yang berarti hampir tidak mungkin terjadi atau lebih dari dua tahun sekali, hingga Certain (5) yang menunjukkan risiko hampir pasti terjadi dalam jangka waktu satu hingga tiga bulan. Kriteria ini penting karena membantu peneliti dan pihak pengelola dalam menilai probabilitas munculnya risiko berdasarkan pengalaman historis maupun kondisi operasional saat ini. Dengan adanya standar pengukuran ini, penilaian risiko dapat dilakukan secara objektif dan terukur, sehingga memudahkan proses evaluasi prioritas.

Tabel IV. Kriteria Impact

| Nilai | Kriteria | Keterangan |
|---|---|---|
| 1 | Rare | Tidak mengganggu layanan website, dampak minimal |
| 2 | Unlikely | Gangguan kecil pada website, masih dapat diakses |
| 3 | Possible | Gangguan sedang, beberapa fitur website tidak berfungsi |
| 4 | Likely | Gangguan signifikan, website sulit diakses atau tidak akurat |

Tabel 4 mendeskripsikan parameter untuk menilai besarnya dampak (impact) apabila suatu risiko benar-benar terjadi. Sama seperti likelihood, impact juga menggunakan skala 1–5. Pada level 1 (Tidak Signifikan), dampak risiko sangat kecil dan tidak mengganggu layanan SITR. Sebaliknya, pada level 5 (Sangat Signifikan), risiko dapat menyebabkan sistem tidak berfungsi sama sekali dan mengganggu pelayanan publik secara keseluruhan. Kriteria ini digunakan untuk menilai seberapa besar konsekuensi dari risiko yang telah teridentifikasi, sehingga pihak pengelola dapat memahami prioritas mana yang harus ditangani terlebih dahulu. Dengan demikian, tabel ini berfungsi sebagai acuan untuk mengukur bobot dampak yang dikombinasikan dengan likelihood dalam penilaian risiko.

Tabel V. Penilaian Kemungkinan Risiko

| Faktor | ID | Kemungkinan Risiko | *Likelihood* | *Impact* |
|---|---|---|---|---|
| Manusia | R01 | Pegawai kesulitan dalam menggunakan sistem | 2 | 2 |
| | R02 | Pegawai ceroboh menjaga kerahasiaan data | 3 | 4 |
| | R03 | Pegawai yang belum dilatih bisa salah menggunakan sistem | 2 | 3 |
| Sistem dan Infrastuktur | R04 | Sistem sering error dan mengganggu pekerjaan | 1 | 3 |
| | R05 | Sistem kadang tidak bisa diakses | 2 | 2 |
| | R06 | Tidak ada backup data dan data bisa hilang | 2 | 4 |
| | R07 | Sistem tidak memiliki perlindungan memadai terhadap serangan virus dan peretasan | 4 | 5 |
| | R08 | Akses data tidak terbatas sehingga meningkatkan risiko penyalahgunaan | 3 | 3 |
| | R09 | Tidak ada prosedur rutin untuk memastikan sistem | 2 | 4 |

DOI: 10.52362/jisamar.v9i4.2104

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)

| | | | | |
|---|---|---|---|---|
| | | berjalan dengan baik | | |
| | R10 | Sistem mengalami downtime dalam durasi yang cukup lama | 2 | 2 |
| | R11 | Pengaturan otorisasi akses pengguna belum dilakukan dengan baik | 2 | 3 |

Berdasarkan penilaian risiko sistem, terdapat 11 faktor risiko yang terbagi dalam dua kategori utama yaitu faktor manusia dan sistem infrastruktur. Risiko paling kritis adalah kurangnya perlindungan sistem terhadap serangan virus dan peretasan (R07) dengan tingkat kemungkinan tinggi (4) dan dampak sangat besar (5), diikuti oleh risiko kelalaian pegawai dalam menjaga kerahasiaan data (R02) dan tidak adanya sistem backup data (R06) yang keduanya memiliki dampak tinggi (4). Secara keseluruhan, organisasi menghadapi tantangan serius dalam aspek keamanan siber, pengelolaan data, dan kapasitas sumber daya manusia yang memerlukan perhatian segera untuk memitigasi potensi kerugian operasional dan keamanan informasi.

3.6. Evaluasi Risiko

Evaluasi risiko dilakukan untuk menentukan prioritas penanganan risiko berdasarkan tingkat risiko yang telah dianalisis. Dalam evaluasi risiko, digunakan matriks evaluasi risiko untuk memetakan risiko berdasarkan likelihood dan impact sebagai berikut:

Tabel VI. Matrix Evaluasi Berdasarkan Likelihood dan Impact

| Likelihood/Impact | 1 (Tidak Sigifikan) | 2 (Kurang Signifikan) | 3 (Cukup Signifikan) | 4 (Signifikan) | 5 (Kurang Signifikan) |
|---|---|---|---|---|---|
| 5 (Certain) | | | | | |
| 4 (Likely) | | | | | R07 |
| 3 (Possible) | | | R08 | R02 | |
| 2 (Unlikely) | | R01,R05,R010 | R03, R11 | R06, R09 | |
| 1 (Rare) | | | R04 | | |

Proses penilaian risiko telah mengidentifikasi 11 potensi risiko yang dikategorikan berdasarkan tingkat risikonya. Terdapat 1 risiko tingkat tinggi yaitu R07 (kurangnya perlindungan sistem terhadap serangan virus dan peretasan), 6 risiko tingkat menengah meliputi R02 (kelalaian pegawai dalam menjaga kerahasiaan data), R03 (kesalahan penggunaan sistem oleh pegawai yang belum terlatih), R06 (tidak adanya backup data), R08 (akses data tidak terbatas), R09 (tidak ada prosedur rutin sistem), dan R11 (pengaturan otorisasi akses yang kurang baik), serta 4 risiko tingkat rendah yaitu R01 (kesulitan penggunaan sistem), R04 (sistem sering error), R05 (sistem tidak dapat diakses), dan R10 (sistem downtime berkepanjangan). Usulan untuk masing-masing risiko dapat dilihat pada tabel 6.

3.6. Perlakuan Risiko

Berdasarkan wawancara dengan pihak terkait serta hasil evaluasi, berikut adalah rekomendasi perlakuan risiko untuk Siste Informasi Tata Ruang (SITR) di Dinas Perumahan Rakyat, Kawasan Permukiman dan Cipta Karya Provinsi Jawa Timur.

Tabel VII. Usulan Perlakuan Risiko

| ID | Deskripsi Risiko | Risk Level | Strategi | Tindakan Mitigasi |
|---|---|---|---|---|

DOI: 10.52362/jisamar.v9i4.2104

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 ( Printed) , Vol. 9 No.4 (November 2025)

| | | | | |
|---|---|---|---|---|
| R07 | Sistem tidak memiliki perlindungan memadai terhadap serangan virus dan peretasan | Tinggi | Reduce | Memasang antivirus dan firewall yang kuat, Memperbarui sistem keamanan secara ruti, Melakukan pengecekan secara berkala |
| R02 | Pegawai ceroboh menjaga kerahasiaan data | Sedang | Reduce | Memberikan pelatihan mengenaipentingnya kerahasiaan data dan membuat aturan yang jelas dan sanksi yang tegas bagi |
| R03 | Pegawai yang belum dilatih bisa salah menggunakan sistem | Sedang | Reduce | Mengadakan pelatihan bagi semua pengguna, Membuat panduan penggunaan yang mudah dimengerti |
| R06 | Tidak ada backup data dan data bisa hilang | Sedang | Reduce | Membuat sistem cadangan otomatis dan rutin, Implementasikan sistem backup otomatis dengan jadwal teratur dan simpan di lokasi terpisah |
| R08 | Akses data tidak terbatas sehingga meningkatkan risiko penyalahgunaan | Sedang | Reduce | Membatasi akses data berdasarkan jabatan dan juga kebutuhan kerja masing-masing pegawai |
| R09 | Tidak ada prosedur rutin untuk memastikan sistem berjalan dengan baik | Sedang | Reduce | Membuat jadwal pengecekan rutin untuk sistem dan tetapkan petugas khusus untuk memantau kinerja |
| R11 | Pengaturan otorisasi akses pengguna belum dilakukan dengan baik | Sedang | Reduce | Memperbaiki sistem pemberian izin akses dengan proses persetujuan yang jelas |
| R01 | Pegawai kesulitan dalam menggunakan sistem | Rendah | Reduce | Memberikan pelatihan tambahan dan membuat panduan yang lebih sederhana |
| R04 | Sistem sering error dan mengganggu pekerjaan | Rendah | Reduce | Memantau dan memperbaiki masalah secara berkala |
| R05 | Sistem kadang tidak bisa diakses | Rendah | Reduce | Memperbaiki koneksi jaringan dan menyiapkan solusi cadangan saat sistem bermasalah |
| R010 | Sistem mengalami downtime dalam durasi yang cukup lama | Rendah | Sharing | Membuat rencana cadangan saat sistem mati dan menginformasikan kepada para pengguna jika ada perbaikan jadwal |

Srategi perlakuan risiko yang disusun berdasarkan tingkat keparahan dan urgensi. Risiko dengan kategori tinggi, yaitu R07, diprioritaskan dengan strategi reduce melalui implementasi sistem keamanan yang lebih kuat, seperti pemasangan firewall, antivirus, dan pembaruan keamanan secara berkala. Risiko kategori sedang, seperti kelalaian pegawai (R02) dan tidak adanya backup data (R06), diatasi melalui pelatihan pegawai, penerapan SOP yang lebih ketat, serta penerapan sistem backup otomatis. Sementara itu, risiko dengan kategori rendah, seperti kesulitan penggunaan sistem (R01) dan sistem error (R04), ditangani dengan langkah-langkah sederhana berupa pelatihan tambahan dan pemeliharaan rutin. Narasi pada tabel ini menunjukkan bahwa setiap risiko tidak hanya diidentifikasi, tetapi juga diberi solusi konkret agar dapat diminimalisir dampaknya. Dengan demikian, hasil analisis tidak hanya bersifat diagnostik, tetapi juga aplikatif dalam memberikan rekomendasi strategis bagi pengelolaan SITR

**DOI:** 10.52362/jisamar.v9i4.2104

.

## IV. KESIMPULAN

Berdasarkan hasil analisis risiko pada Sistem Informasi Tata Ruang (SITR) Jawa Timur menggunakan kerangka kerja ISO 31000, penelitian ini berhasil mengidentifikasi 11 potensi risiko yang dihadapi oleh sistem. Temuan ini dikategorikan menjadi 1 risiko tingkat tinggi, 6 risiko tingkat sedang, dan 4 risiko tingkat rendah. Risiko paling kritis yang teridentifikasi adalah kurangnya perlindungan sistem terhadap serangan siber. Analisis lebih lanjut menunjukkan bahwa sumber utama dari risiko-risiko ini berasal dari faktor manusia dan infrastruktur sistem. Kurangnya kompetensi dan kesadaran pegawai dalam pengelolaan data serta kelemahan pada infrastruktur jaringan menjadi penyebab utama munculnya risiko. Penerapan ISO 31000 dapat menjadi panduan sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko-risiko tersebut secara komprehensif, memberikan landasan yang kuat untuk perbaikan berkelanjutan pada suatu instansi. Hasil penelitian ini diharapkan dapat menjadi landasan bagi Dinas Perumahan Rakyat, Kawasan Permukiman dan Cipta Karya Provinsi Jawa Timur dalam merancang strategi mitigasi yang efektif. Rekomendasi yang diberikan mencakup peningkatan keamanan siber, pelatihan rutin bagi pegawai, serta pengembangan prosedur operasional standar (SOP) yang lebih ketat. Selain itu, penelitian selanjutnya dapat berfokus pada implementasi teknologi keamanan spesifik atau mengukur efektivitas mitigasi risiko setelah rekomendasi ini diterapkan.

## REFERENSI

[1] A. Nikmat, «Analisis Manajemen Risiko Teknologi Informasi Pada Sistem Informasi Akademik (Siak) Universitas Muhammadiyah Sukabumi (Umm) Menggunakan Iso 31000», *J. Manaj. dan Teknol. Inf.*, libk. 14, zenb. 1, or. 49–58, 2024, doi: 10.59819/jmti.v14i1.3321.

[2] M. Miftakhatun, «Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000», *J. Comput. Sci. Eng.*, libk. 1, zenb. 2, or. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.

[3] M. A. P. M. Hutabarat eta S. Suharyadi, «Analisis Manajemen Risiko Pada Sistem Informasi Kurikulum Saraswati Menggunakan ISO 31000:2018», *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, libk. 10, zenb. 1, or. 89, 2025, doi: 10.30645/jurasik.v10i1.852.

[4] P. Kanantyo eta F. S. Papilaya, «Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)», *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, libk. 8, zenb. 4, or. 1896–1908, 2021, doi: 10.35957/jatisi.v8i4.1082.

[5] W. Harefa eta K. D. Hartomo, «Risk Management Analysis Using the ISO 31000 Framework in Warehouse Information Systems», *J. Informatics Eng. Inf. Syst.*, libk. 9, zenb. 1, 2022.

[6] A. F. Tamara, E. Ramadansyah, N. Husniyah, A. F. Nazya, eta S. S. Maesaroh, «Analisis Manajemen Risiko Bisnis (Studi pada Kedai Kopi dan Rempah Trem)», *J. Adm. Kant.*, libk. 10, zenb. 2, or. 204, 2023, doi: 10.51211/jak.v10i2.2053.

[7] R. I. Dewi eta I. Ilham, «Analisis Manajemen Risiko pada UMKM Menggunakan Iso 31000», *J. Bisnis, Manajemen, Dan Inform.*, libk. 20, zenb. 2, or. 124–135, 2023, doi: 10.26487/jbmi.v20i2.32130.

[8] I. Nurfauzi eta A. Suryani, «Analisis Manajemen Risiko Perpustakaan UIN Sunan Gunung Djati Bandung», *Media Pustak.*, libk. 32, zenb. 1, or. 43–57, 2025, doi: 10.37014/medpus.v32i1.5127.

[9] rahayu deny danar dan alvi furwanti Alwie, A. B. Prasetio, R. Andespa, P. N. Lhokseumawe, eta K. Pengantar, «Tugas Akhir Tugas Akhir», *J. Ekon. Vol. 18, Nomor 1 Maret201*, libk. 2, zenb. 1, or. 41–49, 2020.

[10] M. B. As Sajjad, S. D. Kalista, M. Zidan, eta J. Christian, «Analisis Manajemen Risiko Bisnis», *J. Akunt. Univ. Jember*, libk. 18, zenb. 1, or. 51, 2020, doi: 10.19184/jauj.v18i1.18123.

**DOI:** 10.52362/jisamar.v9i4.2104

[11] I. Setiawan, A. R. Sekarini, R. Waluyo, eta F. N. Afiana, «Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto», *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, libk. 20, zenb. 2, or. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[12] Irma Rahayu, David Setiadi, eta Dwi Yuniarto, «Manajemen Risiko Keamanan Aset Teknologi Informasi di DISKOMINFOSANDITIK Kabupaten Sumedang Menggunakan ISO 31000:2018», *J. Tek. Mesin, Ind. Elektro dan Inform.*, libk. 4, zenb. 1, or. 255–264, 2025, doi: 10.55606/jtmei.v4i1.4819.

[13] F. Zalnya Putri dan Iriani, «Analisis Manajemen Risiko Berbasis Iso 31000 Untuk Mengelola Risiko Operasional Di Bidang X Pada Perusahaan Dinas Xyz», *J. Ekon. Dan Bisnis Digit.*, libk. 01, zenb. 03, or. 433–444, 2024.

[14] J. J. Bando *et al.*, «Gambaran Penerapan Program Keselamatan Dan Kesehatan Kerja Rumah Sakit (K3Rs) Di Rumah Sakit Advent Manado. J KESMAS. 2020;9(2):33–40. Gambaran Penerapan Program Keselamatan», *J. KESMAS*, libk. 9, zenb. 2, or. 33–40, 2020.

[15] Geofanny, G.K. eta Tanaamah, A.R. (2022) «Sistem Manajemen Risiko Berbasis ISO 31000:2018 Di PT. Bawen Mediatama», *Jurnal Teknik Informatika dan Sistem Informasi* , 9(4), or. 2870–2878. Available at: http://jurnal.mdp.ac.id.

[16] E. M. Sari, «The Influence of Information System Implementation , ISO 9001 : 2018 , and Internal Quality Audit Intervention on the Performance of Private Universities», libk. 4, zenb. 2, or. 631–642, 2025.

[17] Afifah Azzahra, Putra Aditya, eta Sri Andayani, «Analisis Manajemen Risiko Sistem Informasi Akuntansi Pada PT. Batu Bara XYZ ISO 31000:2018», *J. Sist. Inf.*, libk. 5, zenb. 1, or. 41–50, 2024, doi: 10.32546/jusin.v5i1.2474.

[18] A. F. Putri eta A. H. Prasetyo, «Pedoman dan Asesmen Manajemen Risiko Pada PT Logistik Nasional Tahun 2022-2023», *J. Emerg. Bus. Manag. Entrep. Stud.*, libk. 2, zenb. 2, or. 176–195, 2022, doi: 10.34149/jebmes.v2i2.82.

[19] R. I. Liperda eta U. Ayu Septia Nieng, «Analisis Manajemen Resiko Aplikasi Mypertamina Dengan Menggunakan Iso 31000», *INFOTECH J.*, libk. 9, zenb. 2, or. 361–370, 2023, doi: 10.31949/infotech.v9i2.6232.

[20] B. P. Jurnal, D. Publikasi, A. P. Aisyah, eta L. Dahlia, «Jurnal Akuntansi dan Manajemen (JAM) Enterprise Risk Management Berdasarkan ISO 31000 Dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti», *BPJP) Sekol. Tinggi Ilmu Ekon. Indones. Jakarta*, libk. 19, zenb. 02, 2022, doi: 10.36406/jam.v19i01.483.

[21] S. R. Zulfitra eta A. Ayuningtyas, «Aplikasi Manajemen Risiko SPBE berbasis Website pada Dinas Komunikasi dan Informatika Kabupaten Gresik», *J. Teknol. dan Inf.*, libk. 13, zenb. 2, or. 138–151, 2023, doi: 10.34010/jati.v13i2.9484.

[22] Gina Patriani Manuputty, «Analisis Manajemen Risiko Berbasis Iso 31000 Pada Aspek Operasional Teknologi Informasi Pt. Schlumberger Geophysics Nusantara», *Pap. Knowl. . Towar. a Media Hist. Doc.*, libk. 3, zenb. April, or. 49–58, 2022.

[23] I. C. Lailly Az-Zahra eta I. D. Purnama Ningrum, *Laporan Kerja Praktik Analisis Manajemen Risiko Berdasarkan Iso 31000:2018 Pada Departemen Produksi Iii a Seksi Utilitas Di Pt. Petrokimia Gresik*, zenb. 2011910013. 2022. [Sarean]. Available at: https://repository.uisi.ac.id/4335/2/KERJA PRAKTIK - %28INANDA CLARA LAILLY AZ-ZAHRA%2C 2011910013%29 %26 %28INDAH DWI PURNAMA NINGRUM%2C 2011910014%29.pdf

**DOI:** 10.52362/jisamar.v9i4.2104

[24] M. S. Yusuf, C. A. Swastyastu, L. Syahadianti, eta R. N. T. Shanty, «Analisa Manajemen Risiko E-Learning Universitas Dr. Soetomo Surabaya Menggunakan Framework ISO 31000», *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, libk. 13, zenb. 1, or. 314, 2024, doi: 10.35889/jutisi.v13i1.1800.

[25] S. W. Putri, M. Ashari, M. Mardi, eta S. Fadli, «Analisa Manajemen Risiko Pada Aplikasi E-Smart Di BKPSDM Lombok Tengah Menggunakan ISO 31000», *Innov. J. Soc. ...*, libk. 4, or. 4614–4627, 2024, [Sarean]. Available at: http://j-innovative.org/index.php/Innovative/article/view/8323%0Ahttps://j-innovative.org/index.php/Innovative/article/download/8323/5718

**DOI:** 10.52362/jisamar.v9i4.2104