NIVEDITA
JOURNAL INFORMATICS
e-ISSN : xxx-xxx
p-ISSN : xxx-xxx

Vol. 01, No. 1, Desember 2024

ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI WEBSITE KAMPUNG KB MENGGUNAKAN ISO 31000

Zuriatul Mawaddah[1], Nur Shabrina Nasution[2], Nur Via Ananta[3], Megawati[4]

[1,2,3,4]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi UIN Sultan Syarif Kasim, Riau, Indonesia

email: [1]12150323375@students.uin-suska.ac.id, [2]12150321423@students.uin-suska.ac.id, [3]12150321996@students.uin-suska.ac.id, [4]megawati@uin-suska.ac.id

Abstract

The application of information technology on the Kampung KB website plays an important role in supporting the Population, Family Planning and Family Development (KKBPK) program. However, the use of this technology also presents risks that need to be managed ef ectively to ensure service continuity and reliability. This study aims to analyze information technology risk management on the Kampung KB website using the ISO 31000 framework. The methods used include risk identification, risk analysis, and risk evaluation to determine handling priorities. The results showed that the main risks faced were related to data security, limited human resources in technology management, and technical disruptions in infrastructure. Risk control recommendations are given to improve security, optimize human resource training, and strengthen technology infrastructure. This research is expected to be a reference for the Kampung KB website manager in implementing.

Keywords: *Risk Management, Information Technology, ISO 31000, Kampung KB, Data Security*

Abstrak

Penerapan teknologi informasi pada website Kampung KB memainkan peran penting dalam mendukung program Kependudukan, Keluarga Berencana, dan Pembangunan Keluarga (KKBPK). Namun, teknologi ini juga menghadirkan risiko yang memerlukan pengelolaan khusus. Penelitian ini bertujuan untuk mengelola risiko TI pada situs web Kampung KB dengan menggunakan kerangka kerja ISO 31000. Metode penelitian mencakup identifikasi risiko, analisis risiko, dan evaluasi risiko berdasarkan standar ISO 31000. Hasil penelitian menunjukkan bahwa risiko utama yang dihadapi meliputi kebocoran data pengguna akibat serangan siber, kegagalan server karena overload, dan kurangnya pelatihan teknis pada sumber daya manusia. Rekomendasi mitigasi yang diusulkan meliputi penerapan enkripsi data, teknologi load balancing, dan program pelatihan berkala untuk staf TI. Dengan implementasi strategi ini, tingkat risiko dapat dikurangi secara signifikan, sehingga mendukung keberlanjutan operasional website Kampung KB. Penelitian ini memberikan kontribusi pada literatur manajemen risiko TI serta menjadi referensi praktis bagi pengelola Kampung KB dan pemerintah daerah dalam meningkatkan keamanan dan efisiensi sistem digital.

Kata kunci: Manajemen Risiko, Teknologi Informasi, ISO 31000, Kampung KB, Keamanan Data.

Diajukan: 11 Desember 2024; Diterima: 21 Januari 2025

PENDAHULUAN

Perkembangan Teknologi Informasi (TI) memberikan dampak signifikan pada berbagai sektor, termasuk pemerintahan dan pelayanan masyarakat. Sistem berbasis web, seperti website Kampung KB, memainkan peran penting dalam mendukung program strategis BKKBN, seperti KKBPK. Website ini dirancang untuk menyediakan informasi serta layanan digital guna meningkatkan efisiensi kerja, transparansi, dan aksesibilitas data bagi masyarakat [2].

Namun seperti teknologi lainnya, website Kampung KB menghadapi berbagai risiko. Risiko ini mencakup ancaman keamanan data akibat serangan siber, kegagalan perangkat keras, dan kesalahan manusia dalam pengelolaan data. ISO 31000, sebagai standar internasional dalam manajemen risiko, menyediakan kerangka kerja yang sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko tersebut[9]. Dalam penelitian ini, pendekatan ISO 31000 diterapkan untuk memetakan risiko spesifik, seperti gangguan operasional akibat overload server, serta untuk memberikan rekomendasi mitigasi yang relevan.

Digitalisasi pelayanan publik oleh pemerintah, khususnya pada program Kampung KB, membutuhkan pendekatan pengelolaan risiko yang proaktif. Ancaman terhadap sistem berbasis web tidak hanya berasal dari gangguan teknis tetapi juga faktor eksternal, seperti serangan siber yang semakin kompleks[10]. Menurut penelitian Atmojo & Manuputty (2020), pengelolaan risiko yang efektif melalui ISO 31000 dapat membantu organisasi sektor publik mengidentifikasi potensi risiko yang kritis dan menyiapkan mitigasi yang relevan.

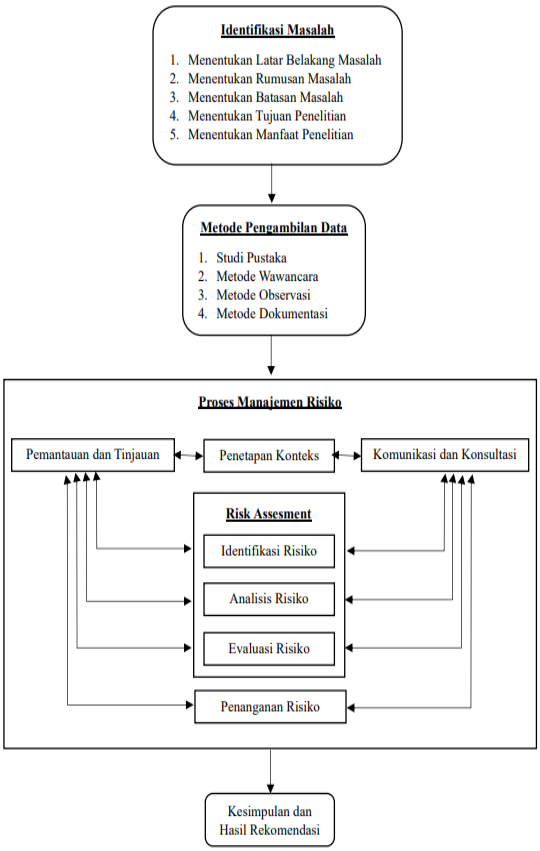
Selain itu, implementasi teknologi informasi di Kampung KB juga menghadapi tantangan sumber daya manusia yang terbatas. Kurangnya pelatihan teknis bagi pengelola sistem sering kali menjadi penyebab utama kesalahan manusia (human error), yang berdampak pada stabilitas sistem. Dengan analisis yang lebih mendalam, penelitian ini bertujuan untuk memberikan solusi yang aplikatif, sehingga mendukung efisiensi operasional dan meningkatkan kepercayaan masyarakat terhadap layanan digital pemerintah.

Menurut Hutagalung (2022), penerapan ISO 31000 pada sektor publik telah terbukti efektif dalam meningkatkan ketahanan sistem TI terhadap berbagai ancaman. Selain itu, penelitian oleh Ulfa & Immawan (2021) menunjukkan bahwa standar ini dapat diadaptasi untuk berbagai skala organisasi, termasuk pemerintah daerah. Hal ini relevan dalam konteks Kampung KB, di mana pendekatan berbasis bukti diperlukan untuk mengelola risiko yang kompleks.

Implementasi standar ISO 31000 juga relevan untuk mendukung visi BKKBN dalam membangun sistem informasi yang andal dan berkelanjutan. Berdasarkan kajian oleh Utamajaya et al. (2021), penerapan manajemen risiko yang sistematis tidak hanya meningkatkan keamanan data tetapi juga memperkuat kepercayaan pemangku kepentingan terhadap inisiatif digital pemerintah.

METODE

Penelitian ini menggunakan metode kualitatif dengan pendekatan partisipatif, yang melibatkan divisi TI sebagai responden utama. Data dikumpulkan melalui wawancara, kuesioner, dan studi literatur, mengacu pada kerangka kerja ISO 31000. Pendekatan ini didukung oleh referensi dari penelitian sebelumnya, seperti studi Hutabarat & Manuputty (2020) tentang penerapan ISO 31000 dalam analisis risiko TI pada organisasi sektor publik. Tahapan penelitian dapat dilihat pada Gambar 1 dibawah ini.



Gambar 1. Metodologi Penelitian

Identifikasi Masalah

Tahap ini merupakan langkah awal yang dilakukan dengan mempelajari topik yang diangkat oleh peneliti. Masalah yang akan diidentifikasi oleh peneliti adalah sebagai berikut:

Mengidentifikasi Latar Belakang Masalah

Pada tahap awal ini, peneliti akan mengenali dan menjelaskan permasalahan yang berkaitan dengan manajemen risiko pada situs web Kampung KB.

1. Menetapkan Rumusan Masalah
   Peneliti akan merumuskan masalah penelitian, yaitu bagaimana cara melakukan analisis manajemen risiko pada situs web Kampung KB.
2. Menetapkan Batasan Masalah
   Berikutnya, peneliti akan menetapkan ruang lingkup masalah dengan memusatkan perhatian pada risiko-risiko yang berpotensi terjadi pada situs web Kampung KB, serta faktor-faktor yang memengaruhi risiko tersebut, menggunakan pendekatan metode ISO 31000 di BKKBN Provinsi Riau.
3. Menetapkan Tujuan Penelitian
   Tujuan penelitian ini adalah untuk melaksanakan analisis manajemen risiko pada situs web Kampung KB dengan merujuk pada standar ISO 31000.
4. Menetapkan Manfaat Penelitian
   Penelitian ini diharapkan mampu memberikan manfaat bagi BKKBN Provinsi Riau sesuai dengan tujuan yang ingin dicapai.

Metode Pengumpulan Data

Teknik pengumpulan data mengacu pada cara yang digunakan untuk memperoleh data atau informasi yang dibutuhkan agar peneliti dapat mengungkap kebenaran terkait topik yang diteliti. Dalam penelitian ini, metode pengumpulan data yang digunakan mencakup studi literatur, wawancara, observasi, dan dokumentasi.

Proses Manajemen Risiko ISO 31000

Menurut ISO 31000, proses manajemen risiko terdiri dari beberapa langkah penting, sebagai berikut:

1. Komunikasi dan Konsultasi (Communication and Consultation)
   Komunikasi dan konsultasi dengan para pemangku kepentingan merupakan aspek yang sangat penting dalam penelitian ini. Para pemangku kepentingan memainkan peran utama dalam memberikan evaluasi terhadap risiko berdasarkan pemahaman mereka mengenai potensi risiko yang mungkin terjadi.
2. Penetapan konteks (Establishing the Context)
   Pada tahap ini, terdapat empat konteks yang harus ditentukan: konteks internal, eksternal, konteks manajemen risiko, dan kriteria risiko. Penentuan konteks yang akurat sangat penting untuk mengarahkan pengelolaan dan evaluasi risiko.
3. Penilaian Risiko ISO 31000: 2009
   Penilaian risiko menurut ISO 31000 mencakup tiga langkah utama: identifikasi risiko, analisis risiko, dan evaluasi risiko.
   a. Identifikasi Risiko (*Risk Identification*)
      Pada tahap ini, proses identifikasi dilakukan melalui wawancara langsung dengan pihak yang berwenang. Langkah-langkah identifikasi risiko mencakup beberapa tahapan, di antaranya:
      1) Mengidentifikasi infrastruktur teknologi informasi yang dimiliki oleh organisasi
         a) Mengenali teknologi informasi yang diterapkan dalam organisasi
         b) Mengidentifikasi berbagai ancaman yang dapat memengaruhi teknologi informasi tersebut
         c) Menggali potensi risiko yang dapat muncul akibat ancaman tersebut
         d) Menganalisis dampak yang mungkin dirasakan oleh organisasi sebagai konsekuensi dari risiko tersebut
      2) Analisis Risiko (*Risk Analiysis*)
         Penelitian ini mengadopsi analisis risiko kualitatif, yaitu suatu pendekatan yang efisien dan sederhana untuk menilai dampak (*impact*) serta kemungkinan terjadinya (*likelihood)* suatu risiko. Analisis kualitatif digunakan untuk menentukan prioritas dalam penanganan risiko, dengan mengukur dan menggabungkan potensi terjadinya risiko serta dampaknya. Pendekatan ini efektif dan efisien dalam hal biaya, memungkinkan organisasi untuk fokus pada risiko yang memiliki probabilitas dan dampak yang lebih signifikan. Setelah memahami

kemungkinan dan dampaknya, evaluasi dilakukan untuk mengidentifikasi risiko mana yang memerlukan perhatian lebih lanjut.

Tabel 1. Kriteria *Likehood*

Likehood		**Keterangan**	**Frekuensi**
Rating	**Kriteria**		
1	*Rare*	Risiko sangat jarang terjadi	>2 tahun
2	*Unlikely*	Risiko jarang terjadi	1 – 2 tahun
3	*Possible*	Risiko terkadang terjadi	7 – 12 bulan / tahun
4	*Likely*	Risiko sering terjadi	4 -6 bulan/ tahun
5	*Certain*	Risiko hampir pasti terjadi	1 -3 bulan / tahun

Tabel 2. Kriteria *Impact*

Impact Rating	**Kriteria**	**Keterangan**
1	*Insignificant*	Tidak mengganggu kelancaran operasional atau kegiatan perusahaan.
2	*Minor*	Proses bisnis dan aktivitas terganggu, namun perusahaan masih dapat melaksanakan fungsi utama atau kegiatan inti tanpa hambatan.
3	*Moderate*	Gangguan pada proses bisnis menyebabkan sebagian aktivitas tertunda dan mengalami keterlambatan dalam pelaksanaannya.
4	*Major*	Mengganggu sebagian besar proses bisnis dan kegiatan perusahaan.
5	*Catastrophic*	Proses bisnis terganggu secara total, mengakibatkan seluruh aktivitas perusahaan terhenti dan tujuan bisnis tidak tercapai.

3) Evaluasi Risiko Evaluasi (Risk Evaluation)

Pada tahap ini, evaluasi risiko dilakukan dengan membandingkan risiko yang telah dihitung dengan kriteria risiko yang telah ditentukan. Kriteria risiko rendah menunjukkan risiko yang dapat diterima, moderat menunjukkan risiko yang perlu diperhatikan, dan tinggi menunjukkan risiko yang tidak dapat diterima. Selain itu, penentuan prioritas dilakukan untuk langkah mitigasi atau penanganannya.

Tabel 3. *Matrix* Evaluasi Resiko

LIKEHOOD						
	Certain / Pasti Terjadi (5)	Moderate	Moderate	High	High	High
	Likely / Sering (4)	Low	Moderate	High	High	High
	Possible/ Kadang (3)	Low	Low	Moderate	High	High
	Unlikely / Jarang (2)	Low	Low	Moderate	Moderate	High
	Rare / Sangat Jarang (1)	Low	Low	Low	Moderate	Moderate
		Insignificant / Sangat Kecil (1)	Minor / Kecil (2)	Moderate / Biasa (3)	Major / Besar (4)	Catastrophic / Sangat Besar (5)
		IMPACT				

Keterangan Warna :

H : *High Risk* (Risiko Tinggi)

M : *Moderate Risk* (Risiko Sedang)

L : *Low Risk* (Risiko Rendah)

Tabel 4. Level Resiko

Level Risiko	Keterangan
High Risk - Risiko Tinggi	Risiko yang mengancam dan perlu ditangani segera.
Moderate Risk - Risiko Sedang	Risiko ini perlu dipantau dan memerlukan penanganan yang terus-menerus.
Low Risk - Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena memiliki tingkat pengaruh yang paling rendah.

1) Penanganan Risiko (*Risk Treatment*)
Pada tahap ini, berbagai strategi diterapkan untuk mengelola risiko, di antaranya:
   a) *Transfer* (Pembagian Risiko)
   Strategi ini bertujuan untuk memindahkan dampak negatif dari risiko kepada pihak lain, bukan untuk menghilangkannya sepenuhnya.
   b) Mitigasi (Pengurangan Risiko)
   Tujuan dari strategi mitigasi adalah untuk mengurangi kemungkinan terjadinya risiko dan dampaknya hingga mencapai tingkat yang dapat diterima. Pengurangan ini dapat dievaluasi melalui empat jenis kontrol:
      - Kontrol preventif (pencegahan), untuk mengurangi kemungkinan terjadinya hasil yang tidak diinginkan.
      - Kontrol korektif (perbaikan), untuk memperbaiki hasil yang tidak sesuai yang sudah terjadi.
      - Kontrol direktif (pengarahan), untuk mencapai hasil yang diinginkan, kontrol ini penting dalam proses tersebut.
      - Kontrol deteksi, digunakan untuk mendeteksi kapan hasil yang tidak diinginkan terjadi, terutama setelah risiko terjadi, dengan tujuan hanya untuk mengidentifikasi dampak yang merugikan.
   c) *Avoidance* (Penghindaran Risiko)
   Pendekatan ini digunakan untuk menghilangkan kemungkinan terjadinya risiko yang dapat memberikan dampak besar bagi perusahaan.
   d) Toleransi (Penerimaan Risiko)
   Metode ini diterapkan untuk risiko yang masih dalam batas toleransi perusahaan, yaitu risiko yang tidak memerlukan tindakan lanjutan atau jika biaya penanganannya lebih besar dibandingkan dengan manfaat yang didapat.
2) Pemantauan dan Tinjauan (*Monitoring and Review*)
Proses manajemen risiko secara keseluruhan perlu dipantau dan dievaluasi. Ini mencakup berbagai aspek seperti lingkungan, proses, organisasi, strategi, dan pemangku kepentingan. Setiap hasil pemantauan dan evaluasi ulang harus didokumentasikan sebagai bukti bahwa langkah-langkah tersebut telah dilaksanakan dan digunakan sebagai bagian dari kerangka manajemen risiko yang telah ditentukan sebelumnya.

HASIL DAN PEMBAHASAN

Penelitian ini mengadopsi metode ISO 31000 yang mencakup lima langkah utama dalam proses manajemen risiko meliputi komunikasi dan konsultasi, penentuan konteks, penilaian risiko, penanganan risiko, dan pemantauan serta tinjauan. Fokus analisis dalam penelitian ini terletak pada proses penilaian

risiko, yang meliputi proses pengidentifikasian, analisis, serta evaluasi risiko yang terkait dengan situs web Kampung KB.

Komunikasi dan Konsultasi

Langkah awal pada manajemen risiko dengan ISO 31000 ini ialah dengan melakukan observasi serta wawancara kepada pihak BKKBN. Wawancara dilaksanakan berdasarkan RACI yang telah ditentukan sebelumnya.

Menentukan Konteks

Website Kampung KB didukung infrastruktur TI yang memadai, meliputi server hosting, koneksi jaringan stabil, serta sistem pengelolaan data berbasis web. Namun, terdapat tantangan dalam pengelolaan operasional, seperti perlunya peningkatan kompetensi teknis sumber daya manusia (SDM) dan penguatan tata kelola dokumen operasional untuk mendukung konsistensi proses pengelolaan sistem.

Penilaian Risiko

Dalam proses penilaian risiko ini terdapat 3 tahapan, yaitu pengidentifikasian risiko, analisis risiko, serta evaluasi risiko

1. Identifikasi Risiko

1) Identifikasi Aset

Setiap aset yang diidentifikasi, seperti data pengguna, perangkat keras, dan perangkat lunak, berperan penting dalam mendukung kelancaran operasional website Kampung KB. Gangguan pada perangkat keras, seperti server, dapat menyebabkan layanan website terhenti, sementara kebocoran data berpotensi merusak kepercayaan pengguna. Untuk lebih jelasnya berikut merupakan table yang menunjukkan detail asset-aset dari website Kampung KB :

Tabel 5. Identifikasi Aset *Website Kampung KB*

Kategori Aset	Detail Aset
Data dan Informasi	1. Data pengguna (nama, NIK, data keluarga) 2. Data program KB (target, capaian, laporan aktivitas) 3. Data statistik kependudukan 4. Data akses dan aktivitas pengguna
Perangkat Lunak	1. Sistem informasi berbasis web (Kampung KB) 2. Sistem enkripsi untuk keamanan data
Perangkat Keras	1. Server utama dan server Cadangan 2. Komputer administrasi 3. Perangkat penyimpanan (hard drive, SSD) 4. Router dan perangkat jaringan 5. Jaringan internet dengan akses aman 6. Sistem firewall untuk melindungi jaringan
Sumber Daya Manusia	1. Tim pengelola website (administrator, teknisi, dan staf pendukung) 2. Operator lapangan untuk input data dan pemantauan

2) Identifikasi Kemungkinan Risiko

Risiko operasional seperti pemadaman listrik dan gangguan jaringan berdampak langsung pada aksesibilitas layanan. Risiko keamanan data, seperti kebocoran informasi, memerlukan langkah mitigasi strategis untuk melindungi data pengguna. Berikut merupakan table yang menunjukkan identifikasi kemungkinan risiko.

Tabel 6. Identifikasi adanya Kemungkinan Risiko

Faktor Risiko	ID Risiko		Kemungkinan Risiko
Alam Dan Lingkungan	**R01**	-	Gangguan operasional akibat bencana alam seperti banjir atau kebakaran.

Faktor Risiko	ID Risiko		Kemungkinan Risiko
	R02	-	Pemadaman listrik yang memengaruhi aksesibilitas server.
	R03	-	Kerusakan perangkat akibat debu atau kotoran.
Sumber Daya Manusia	**R04**	-	Kesalahan dalam pengelolaan data (human error).
	R05	-	Pelanggaran SOP yang menyebabkan gangguan pada sistem.
	R06	-	Kurangnya pelatihan teknis pada staf yang menangani sistem.
Sistem & Infrastruktur	**R07**	-	Kegagalan atau kerusakan perangkat keras seperti server atau komputer.
	R08	-	Overload pada server saat banyak pengguna mengakses secara bersamaan.
	R09	-	Gangguan jaringan yang menyebabkan website tidak dapat diakses.
	R10	-	Kerusakan perangkat lunak akibat bug atau crash.
Keamanan Data	**R11**	-	Kebocoran data pengguna akibat serangan siber atau akses tidak sah.
	R12	-	Kehilangan data akibat kegagalan penyimpanan (disk full atau disk error).
Ancaman Siber	**R13**	-	Serangan malware, virus, atau program jahat lainnya.
	R14	-	Peretasan yang menyebabkan manipulasi atau pencurian data penting.

2. Analisis Risiko

Setelah proses identifikasi risiko pada tahap sebelumnya, langkah berikutnya adalah melaksanakan analisis risiko. Pada tahapan ini, penilaian akan dilakukan terhadap kemungkinan risiko yang telah diidentifikasi sebelumnya . Berikut merupakan table penilaian kemungkinan risiko menggunakan likehood dan impact.

Tabel 7. Penilaian Kemungkinan Risiko dengan *Likehood* dan *Impact.*

ID Risiko	Kemungkinan Risiko	Likehood	Impact	Penjelasan
R01	Gangguan operasional akibat bencana alam (banjir, kebakaran).	2 (Jarang)	5 (Kritis)	Risiko jarang terjadi, namun jika terjadi dapat menyebabkan kerusakan besar.
R02	Pemadaman listrik.	3 (Kadang)	4 (Signifikan)	Pemadaman listrik cukup sering terjadi di wilayah tertentu dan berdampak pada akses.
R03	Kerusakan perangkat akibat debu atau kotoran.	3 (Kadang)	3 (Moderat)	Debu dapat mengurangi efisiensi perangkat, memerlukan perawatan atau penggantian.
R04	Kesalahan dalam pengelolaan data (human error).	4 (Sering)	3 (Moderat)	Kesalahan manusia sering terjadi tetapi berdampak sedang pada kelancaran operasional.
R05	Pelanggaran SOP.	2 (Jarang)	3 (Moderat)	Pelanggaran SOP jarang terjadi, tetapi memengaruhi efisiensi kerja.
R06	Kurangnya pelatihan teknis pada staf.	3 (Kadang)	3 (Moderat)	Pelatihan yang kurang menghambat efektivitas kerja staf TI.

ID Risiko	Kemungkinan Risiko	Likehood	Impact	Penjelasan
R07	Kegagalan atau kerusakan perangkat keras (server, komputer).	3 (Kadang)	4 (Signifikan)	Kerusakan perangkat keras dapat mengganggu layanan.
R08	Overload pada server.	4 (Sering)	4 (Signifikan)	Server sering overload pada jam sibuk, menyebabkan gangguan akses.
R09	Gangguan jaringan.	4 (Sering)	4 (Signifikan)	Jaringan sering bermasalah, menghambat akses website.
R10	Kerusakan perangkat lunak (bug atau *crash*).	3 (Kadang)	4 (Signifikan)	Bug perangkat lunak dapat membuat website tidak dapat diakses.
R11	Kebocoran data pengguna.	2 (Jarang)	5 (Kritis)	Kebocoran data jarang terjadi tetapi memiliki dampak sangat besar.
R12	Kehilangan data akibat kegagalan penyimpanan.	3 (Kadang)	4 (Signifikan)	Penyimpanan gagal dapat mengakibatkan data hilang atau rusak.
R13	Serangan malware, virus, atau program jahat lainnya.	3 (Kadang)	5 (Kritis)	Serangan siber kadang terjadi dan berdampak kritis jika berhasil.
R14	Peretasan data penting.	2 (Jarang)	5 (Kritis)	Peretasan jarang terjadi tetapi sangat merugikan jika berhasil.

Berdasarkan kategori impact dapat diketahui bahwa risiko pada layanan website Kampung KB meliputi antara lain adalah gangguan layanan teknis yang menghambat akses pengguna, ancaman keamanan data yang merusak kepercayaan masyarakat serta eterlambatan pengambilan keputusan berbasis data.

3. Evaluasi Risiko

Langkah akhir dari penilaian risiko merupakan tahap evaluasi risiko. Pada tahap ini, digunakan referensi berbentuk matriks risiko yang mengelompokkan risiko ke dalam tiga tingkat, yaitu rendah (low), sedang (medium), dan tinggi (high). Risiko yang sebelumnya telah dinilai berdasarkan nilai likelihood (kemungkinan) dan nilai impact (dampak) akan dilakukan klasifikasi lebih lanjut sesuai dengan kategori dalam matriks tersebut.Berikut merupakan tabel evaluasi risikonya:

Tabel 8. Matrix Evaluasi Risiko

Likelihood	*Insignificant (1)*	*Minor (2)*	*Moderate (3)*	*Major (4)*	*Catastrophic (5)*
Certain (5)	-	-	-	-	-
Likely (4)			R04	R08, R09	-
Possible (3)	-	-	R03, R06, R07	R02, R10, R12	R13
Unlikely (2)	-	R05	-	-	R01, R11, R14
Rare (1)	-	-	-	-	-

Setelah berbagai risiko yang teridentifikasi dipetakan dalam matriks evaluasi yang didasarkan pada likelihood (kemungkinan) dan impact (dampak), risiko tersebut setelah itu akan dikelompokkan ke dalam tingkat risiko (level of risk) yang terdiri dari tiga kategori: tinggi (high), sedang (medium), dan rendah (low). Berikut merupakan tabel risk level kemungkinan risiko.

Tabel 9. Risk Level Kemungkinan Risiko

ID Risiko	Likehood	Impact	Risk Level
R01	2	5	High
R02	3	4	Moderate
R03	3	3	Moderate

ID Risiko	Likehood	Impact	Risk Level
R04	4	3	Moderate
R05	2	3	low
R06	3	3	Moderate
R07	3	3	Moderate
R08	4	4	High
R09	4	4	High
R10	3	4	Moderate
R11	2	5	High
R12	3	4	Moderate
R13	3	5	High
R14	2	5	High

4. Perlakuan Risiko

Setelah tahap pengidentifikasian risiko dilakukan, prose selanjutnya adalah melakukan pengelolaan risiko. Pada tahapan ini, penulis akan memberikan solusi terkait cara-cara untuk menangani risiko yang mungkin muncul pada situs web Kampung KB. Tujuan dari langkah ini adalah untuk mengurangi risiko serta mengambil tindakan preventif guna menghindari masalah potensial di masa depan. Berikut adalah tabel usulan penanganan risiko yang diusulkan.

Tabel 10. Usulan Perlakuan Risiko

ID Risiko	Kemungkinan Risiko	Kategori Risiko	Usulan Perlakuan Risiko
R01	Gangguan operasional akibat bencana alam.	High	Membuat rencana pemulihan bencana (*disaster recovery plan*), seperti lokasi server Cadangan.
R02	Pemadaman listrik.	Moderate	Menggunakan sumber daya listrik cadangan seperti UPS atau generator.
R03	Kerusakan perangkat akibat debu atau kotoran.	Moderate	Menjadwalkan pembersihan dan perawatan perangkat keras secara berkala.
R04	Kesalahan dalam pengelolaan data (human error).	Moderate	Memberikan pelatihan teknis kepada staf terkait tata kelola data yang benar.
R05	Pelanggaran SOP	Low	Menyusun dan menyosialisasikan SOP yang lebih jelas kepada seluruh staf.
R06	Kurangnya pelatihan teknis pada staf.	Moderate	Menyediakan program pelatihan dan sertifikasi untuk staf TI dan pengguna sistem.
R07	Kegagalan atau kerusakan perangkat keras.	Moderate	Menyediakan perangkat keras cadangan dan kontrak perawatan dengan vendor.
R08	Overload pada server.	High	Meng-upgrade kapasitas server dan menggunakan teknologi load balancing.
R09	Gangguan Jaringan	High	Menggunakan koneksi internet dengan failover otomatis dan meningkatkan monitoring jaringan.

ID Risiko	Kemungkinan Risiko	Kategori Risiko	Usulan Perlakuan Risiko
R10	Kerusakan perangkat lunak.	Moderate	Melakukan pengujian perangkat lunak secara berkala dan menerapkan patch updates.
R11	Kebocoran data pengguna.	High	Mengimplementasikan enkripsi data, otentikasi dua faktor, dan monitoring akses data.
R12	Kehilangan data akibat kegagalan penyimpanan.	Moderate	Membuat sistem pencadangan data secara otomatis (*automated backup system*).
R13	Serangan malware atau virus.	High	Memasang antivirus terbaru, firewall, dan melakukan scanning berkala.
R14	Peretasan data penting.	High	Meningkatkan keamanan aplikasi dengan teknologi SSL, IDS/IPS, dan audit keamanan berkala.

KESIMPULAN

Tujuan penelitian ini adalah menganalisis pengelolaan risiko pada website Kampung KB menggunakan kerangka kerja ISO 31000. Berdasarkan hasil analisis, beberapa risiko utama berhasil diidentifikasi, dianalisis, dan dievaluasi, meliputi risiko keamanan data, gangguan teknis, serta potensi ancaman dari sumber daya manusia dan lingkungan. Setiap risiko dikelompokkan ke dalam kategori risiko rendah *(low*), sedang *(moderate)*, dan tinggi *(high)*, dengan fokus mitigasi diberikan pada risiko-risiko dengan dampak signifikan.

Proses identifikasi menunjukkan bahwa risiko utama, seperti gangguan jaringan (R09), overload pada server (R08), dan serangan *malware* (R13), memiliki dampak besar terhadap operasional website. Melalui tahapan analisis risiko, risiko-risiko ini diberikan prioritas untuk mitigasi dengan usulan langkah strategis, seperti penggunaan teknologi load balancing, penggandaan penyedia layanan internet, dan pembaruan sistem keamanan.

Pada tahap monitoring dan review, diketahui bahwa sebagian besar perlakuan risiko yang telah diterapkan mampu mengurangi dampak risiko. Simulasi pemulihan bencana menunjukkan kesiapan sistem cadangan, meskipun penambahan lokasi server di wilayah lain diperlukan untuk mengurangi risiko gangguan regional. Selain itu, pemberian pelatihan kepada staf operasional terbukti efektif dalam mengurangi kesalahan manusia (human error), yang sebelumnya menjadi salah satu sumber risiko moderat.

Kesimpulan penelitian ini Implementasi kerangka kerja ISO 31000 telah terbukti efektif dalam proses identifikasi, mitigasi, dan pemantauan risiko. Proses ini mendukung kelangsungan operasional website Kampung KB dan meningkatkan kepercayaan masyarakat terhadap layanan digital BKKBN.

Sebagai rekomendasi, perlu dilakukan evaluasi berkelanjutan terhadap risiko baru yang mungkin muncul seiring dengan perkembangan teknologi dan kebutuhan pengguna. Selain itu, peningkatan kapasitas infrastruktur, penguatan SOP, serta pengembangan sistem keamanan data perlu terus ditingkatkan untuk mendukung layanan yang lebih handal di masa depan.

DAFTAR PUSTAKA

[1] Aisyah, A. P., & Dahlia, L. (2022). Enterprise Risk Management Berdasarkan ISO 31000 Dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti. Jurnal Akuntansi Dan Manajemen, 19(2), 78-90

[2] Asir, M., Yuniawati, R. A., Mere, K., Sukardi, K., & Anwar, M. A. (2023). Peran manajemen risiko dalam meningkatkan kinerja perusahaan: studi manajemen sumber daya manusia. Entrepreneurship Bisnis Manajemen Akuntansi (E-BISMA), 32-42.

[3] Atmojo, S. A., & Manuputty, A. D. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office. JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), 7(3), 546-558. DOI : https://doi.org/10.35957/jatisi.v7i3.525

[4] Badan Kependudukan dan Keluarga Berencana Nasional (BKKBN), "Tentang Kampung KB," Kampung KB. [Tautan Online]. Tersedia: https://kampungkb.bkkbn.go.id/tentang. [Tanggal Akses: 08-Des-2024]

[5] Hutabarat, F. M., & Manuputty, A. D. (2020). Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000. Jurnal Bina Komputer, 2(1), 52-65.

[6] Hutagalung, L. E. (2022). Analisa Manajemen Risiko Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rumah Sakit Xyz Menggunakan Iso 31000. Teika, 12(01), 23-33. DOI : https://doi.org/10.36342/teika.v12i01.2820

[7] Ulfa, A. A., & Immawan, T. (2021). Analisis Manajemen Risiko Dengan Penerapan ISO 31000 Pada Proses Machining (Studi Kasus: Perusahaan AB). Integrasi: Jurnal Ilmiah Teknik Industri, 6(2), 42-52.

[8] Utamajaya, J. N., Afrina, A., & Fitriah, A. N. (2021). Analisis Manajemen Risiko Teknologi Informasi Pada Perusahaan Toko Ujung Pandang Grosir Penajam Paser Utara Menggunakan Framework Iso 31000: 2018. Sebatik, 25(2), 326-334. DOI : https://doi.org/10.46984/sebatik.v25i2.1430

[9] Lutfirahman, A. M., Ibrahim, E. F., & Hiswara, I. A. J. Analisis Manajemen Risiko Dinas Komunikasi Dan Informatika Surabaya Berdasarkan Iso.

[10] Sari, S. K., Anggryani, L., Hidayat, R., & Marzuki, S. N. (2024). Tantangan Dan Solusi Dalam Pengawasan Risiko Di Perbankan Syariah Pada Era Cyber: Tinjauan Literatur Bank Syariah Indonesia. *Jurnal Lan Tabur*, *6*(1), 91-109.