Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

MANAJEMEN RISIKO SISTEM INFORMASI UNIT ORGANISASI BPIW KEMENTERIAN PUPR MENGGUNAKAN FRAMEWORK ISO 31000:2018

Lisa Febriyanti[1], Mahdiyyah Febrinazahra[2], Kraugusteeliana[3], I Gede Susrama Masdiyasa
[1,2,3]S1 Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta,
[4]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur
lisafyi194@gmail.com[1], febrinazahra13@gmail.com[2], kraugusteeliana@upnvj.ac.id[3], gsusrama.if@upnjatim.ac.id[4]
Jalan RS. Fatmawati Raya, Pondok Labu, Cilandak, Jakarta Selatan, Jakarta 12450

Keywords:

Risk Management, Information Systems, ISO 31000:2018, Ministry of Public Works and Housing, BPIW Organizational Unit

Abstract

In the era of rapid globalization and digital transformation, the role of Information Technology (IT) in supporting operations and information management in government institutions has become increasingly crucial. As a government agency responsible for various infrastructure projects, the Ministry of Public Works and Public Housing (PUPR) requires reliable and secure information systems to support timely and accurate decision-making. This study aims to analyze and propose the application of the ISO 31000:2018 framework in the risk management of information systems in the BPIW (Information and Website Management Agency) Unit of the PUPR Ministry. This research employs a descriptive qualitative approach with data collection methods including literature review, interviews, observations, and documentation. The findings indicate that implementing ISO 31000:2018 can assist the BPIW Unit in effectively identifying, evaluating, and managing risks associated with information systems. Therefore, the application of ISO 31000:2018 is expected to enhance the security, availability, and integrity of the PUPR Ministry's information systems and support clean, effective, transparent, and accountable governance.

Kata Kunci:

Manajemen Risiko, Sistem Informasi, ISO 31000:2018, Kementerian PUPR, Unit Organisasi BPIW

Abstrak

Dalam era globalisasi dan transformasi digital yang semakin pesat, peran Teknologi Informasi (TI) dalam mendukung operasional dan pengelolaan informasi pada instansi pemerintah menjadi sangat krusial. Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR) sebagai lembaga pemerintah yang bertanggung jawab atas berbagai proyek infrastruktur memerlukan sistem informasi yang handal dan aman guna mendukung pengambilan keputusan yang tepat waktu dan akurat. Penelitian ini bertujuan untuk menganalisis dan mengusulkan penerapan *framework* ISO 31000:2018 dalam manajemen risiko sistem informasi di Unit Organisasi BPIW (Badan Pengelolaan Informasi dan Website) Kementerian PUPR. Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode pengumpulan data melalui studi literatur, wawancara, observasi, dan dokumentasi. Hasil penelitian menunjukkan bahwa penerapan ISO 31000:2018 dapat membantu Unit Organisasi BPIW dalam mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan sistem informasi secara efektif. Dengan demikian, penerapan ISO 31000:2018 diharapkan dapat meningkatkan keamanan, ketersediaan, dan integritas sistem informasi Kementerian PUPR, serta mendukung tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel.

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

1. Pendahuluan

Dalam era globalisasi dan transformasi digital yang pesat, Teknologi Informasi (TI) menjadi krusial bagi operasional instansi. Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR) berperan penting dalam pembangunan infrastruktur untuk pertumbuhan ekonomi dan kesejahteraan masyarakat Indonesia. Untuk mendukung pengambilan keputusan yang tepat dan akurat, Kementerian PUPR memerlukan sistem informasi yang handal dan aman [2].

Unit Organisasi BPIW (Badan Pengelolaan Informasi dan Website) di Kementerian PUPR bertanggung jawab atas sistem informasi seperti Bank Data BPIW dan SiPro, serta dua website resmi, yaitu Website BPIW dan Website P3TB. Sistem ini penting untuk tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel, serta meningkatkan kualitas pelayanan publik [4].

Namun, pengelolaan sistem informasi yang kompleks menghadapi tantangan manajemen risiko, termasuk ancaman keamanan cyber. Untuk mengatasi ini, diperlukan pendekatan sistematis dalam manajemen risiko, seperti kerangka kerja ISO 31000. ISO 31000 memberikan panduan dalam mengidentifikasi, mengevaluasi, dan mengelola risiko, termasuk risiko sistem informasi. Melalui penggunaan framework ISO 31000, organisasi dapat mengadopsi praktik terbaik ini untuk meningkatkan ketahanan terhadap ancaman cyber dan menjaga integritas serta ketersediaan sistem informasi [1][5].

Rumusan masalah dalam penelitian ini mencakup tantangan yang dihadapi oleh Unit Organisasi BPIW Kementerian PUPR dalam mengelola sistem informasi terkait manajemen risiko, keberlakuan framework ISO 31000 dalam konteks manajemen sistem informasi Kementerian PUPR, khususnya di Unit Organisasi BPIW, serta potensi dampak risiko yang dapat terjadi pada sistem informasi Kementerian PUPR jika tidak dikelola dengan pendekatan yang sistematis sesuai ISO 31000.

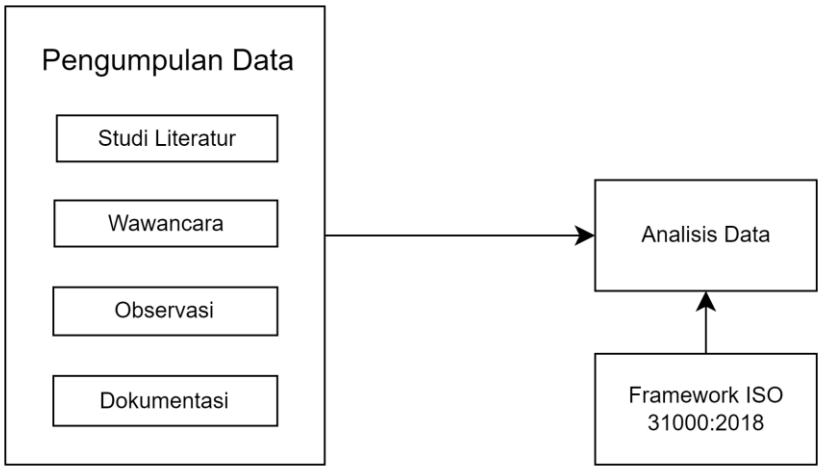
Penelitian ini bertujuan untuk menganalisis tantangan yang dihadapi oleh Unit Organisasi BPIW Kementerian PUPR dalam mengelola sistem informasi terkait manajemen risiko, mengidentifikasi keberlakuan framework ISO 31000 dalam manajemen sistem informasi Kementerian PUPR, khususnya di Unit Organisasi BPIW, serta mengevaluasi potensi dampak risiko yang mungkin terjadi pada sistem informasi Kementerian PUPR dan mengusulkan strategi pengelolaan risiko yang sesuai dengan prinsip-prinsip ISO 31000. Dengan memahami konteks operasional dan kebutuhan organisasi, penelitian ini akan mengeksplorasi bagaimana ISO 31000 dapat membantu BPIW mengelola risiko sistem informasi secara efektif, mendukung tata kelola pemerintahan yang baik, serta meningkatkan pelayanan publik. Penelitian ini diharapkan dapat meningkatkan keamanan, ketersediaan, dan integritas sistem informasi Kementerian PUPR, serta memperkuat hubungan antara pemerintah dan masyarakat.

2. Metodologi Penelitian

Metode penelitian yang diterapkan terdiri dari dua tahap utama, yakni pengumpulan data dan analisis data. Penelitian ini mengadopsi pendekatan deskriptif kualitatif, dengan proses pengumpulan data bertujuan untuk memperoleh informasi terkait dengan proses sistem informasi. Dalam penelitian, terdapat beberapa metode yang umum digunakan untuk mengumpulkan data, yaitu studi literatur, wawancara, observasi, dan dokumentasi. Informasi yang terkumpul kemudian dianalisis dengan

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

menggunakan framework ISO 31000:2018. Analisis data merupakan proses yang melibatkan pencarian dan penyusunan data secara terstruktur mulai dari identifikasi masalah hingga pembuatan kesimpulan. Proses ini bergantung pada data yang telah dikumpulkan melalui berbagai metode seperti studi literatur, wawancara, observasi, dokumentasi, dan lain sebagainya.

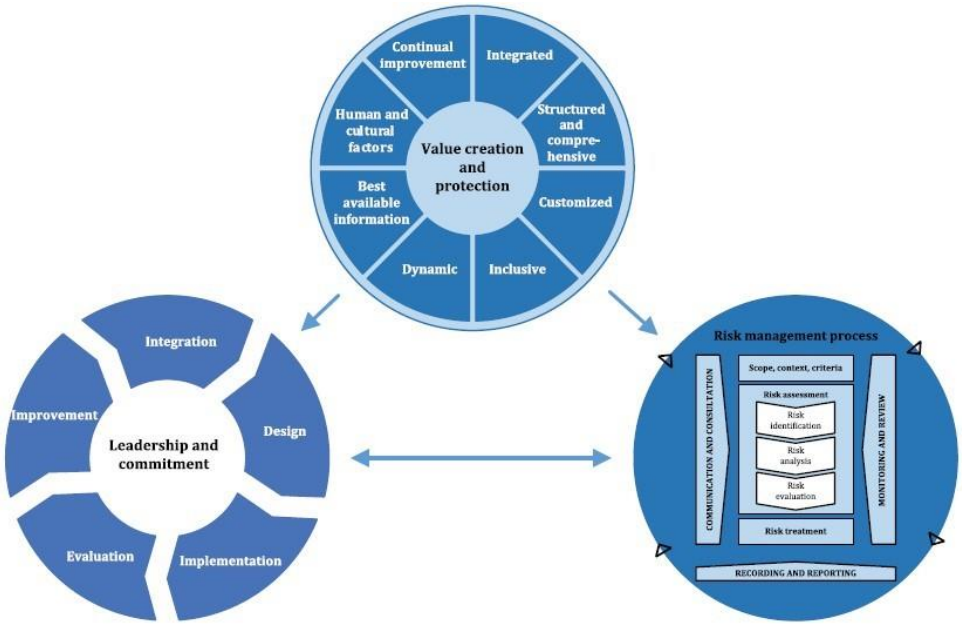


Gambar 1. Alur Metodologi Penelitian

3. Hasil dan Pembahasan

Pada bagian ini akan dibahas secara detail mengenai proses manajemen risiko dari hasil observasi, studi literatur, wawancara, dan dokumentasi. Proses manajemen risiko yang dilakukan berdasarkan dokumen ISO 31000 yang terdiri dari 5 klausul besar yang menjelaskan prinsip dan pedoman penerapan manajemen risiko, yaitu : i) klausul 1: Lingkup; ii) klausul 2: Terminologi dan Definisi; iii) klausul 3: Prinsip-Prinsip; iv) klausul 4: Kerangka Kerja; dan v) klausul 5: Proses [3]. Implementasi ISO 31000 memberikan landasan yang kuat untuk meningkatkan kemampuan organisasi dalam menghadapi tantangan dan peluang yang muncul dari lingkungan internal maupun eksternal mereka[6].

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi



Gambar 2. Hubungan Kerangka Kerja ISO 31000:2018
Sumber : International Organization for Standardization (2018). ISO 31000:2018 - Risk management.

3.1 Komunikasi dan Konsultasi

Usaha yang dilakukan oleh stakeholder dalam memahami berbagai macam risiko organisasi diperoleh dengan komunikasi dan konsultasi agar keputusan yang diambil tidak merugikan organisasi [11]. Dalam menganalisis manajemen risiko menggunakan framework ISO 31000 melalui metode observasi dan wawancara kepada ahli keamanan TI di Kementerian PUPR. Tahap ini dilakukan kepada bagian keamanan TI untuk membahas izin dalam melakukan analisis manajemen risiko, sehingga apa yang akan diperoleh dapat dipertanggungjawabkan kepada pihak Kementerian PUPR. Selanjutnya, melakukan komunikasi dan konsultasi untuk mendapatkan pemahaman lebih tentang organisasi, potensi risiko penggunaan dan keamanan sistem informasi organisasi BPIW di Kementerian PUPR sehingga dapat menjadi pertimbangan dalam mengambil keputusan pengelolaan manajemen risiko [2].

3.2 Cakupan, Konteks, dan Kriteria

3.2.1 Cakupan

Tujuan penelitian ini adalah menganalisa manajemen risiko sistem informasi unit organisasi BPIW di Kementerian PUPR untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya. Dalam mengidentifikasi dan mengukur potensi risiko berfokus pada sistem informasi unit organisasi BPIW yakni situs web P3TB.

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

3.2.2 Konteks

Peneliti menetapkan konteks manajemen risiko untuk mengatasi ancaman serangan web defacement yang dapat mengubah tampilan konten situs web menjadi situs judi online, menyebabkan kerugian reputasi dan finansial. Prosedur kerja manajemen risiko akan menggunakan klausul 5 dari framework ISO 31000 yaitu proses manajemen risiko yang mencakup komunikasi dan konsultasi, penetapan konteks organisasi, penilaian risiko, perlakuan risiko, pemantauan dan peninjauan, serta perekaman dan pelaporan. Aktivitas tersebut akan melibatkan analisis pendahuluan potensi bahaya, wawancara dengan ahli keamanan TI, dan penggunaan metode lain yang sesuai. Hasilnya akan berupa risk register yang memuat daftar peristiwa risiko beserta informasi pendukungnya [15]. Evaluasi efektivitas akan dilakukan secara terus-menerus untuk memastikan langkah-langkah mitigasi yang diambil efektif dalam mengurangi risiko dan menjaga keamanan situs web. Dengan demikian, Kementerian PUPR dapat lebih siap dalam menghadapi ancaman keamanan informasi dan menjaga integritas situs web mereka.

3.3.3 Kriteria

Kriteria risiko adalah kriteria yang digunakan dalam menghitung dan mengevaluasi sebuah eksposur risiko terhadap organisasi [3]. Kriteria yang digunakan untuk mengetahui eksposur kemungkinan sebuah risiko dapat diketahui melalui suatu kriteria pemeringkatan kualitatif sebagai berikut.

Tabel 1. Kriteria Risiko

No	Tingkat Eksposur Kemungkinan Risiko	Indikator
1	Rendah	Risiko sangat kecil kemungkinannya untuk terjadi dalam waktu 1 tahun kedepan
2	Sedang	Risiko bisa saja terjadi dalam waktu 1 tahun kedepan
3	Tinggi	Risiko sangat besar kemungkinannya untuk terjadi dalam waktu 1 tahun kedepan

3.3 Penilaian Risiko

3.3.1 Identifikasi Risiko

Identifikasi risiko dilakukan berdasarkan kejadian bahaya sebelumnya pada bulan september 2023, yaitu web defacement. Web defacement adalah serangan terhadap situs dengan mengubah tampilan konten situs tersebut dengan memanfaatkan

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

celah keamanan dalam situs web. Kondisi yang dialami kementerian PUPR yaitu penyerang mengganti halaman situs web P3TB menjadi situs judi *online*. Metode pencarian yang digunakan untuk mengidentifikasi risiko terkait adalah analisis pendahuluan potensi bahaya. Metode ini merupakan pendekatan induktif untuk mengidentifikasi potensi bahaya, situasi, dan kejadian berpotensi bahaya yang dapat menyebabkan kerugian bagi sistem informasi. Selain itu, pendekatan wawancara juga digunakan untuk mendukung identifikasi risiko, dimana ahli keamanan TI di Kementerian PUPR diwawancarai untuk mendapatkan pemahaman lebih dalam tentang potensi risiko terkait web defacement dan langkah yang diambil sebagai penanganan serta mengurangi dampaknya. Melalui metode Analisis pendahuluan potensi bahaya dan wawancara terstruktur, dapat dilakukan identifikasi risiko yang lebih komprehensif dan efektif. Metode ini meningkatkan kesiapan Kementerian PUPR dalam menghadapi potensi ancaman terkait keamanan sistem informasi, serta mengimplementasikan langkah-langkah perlindungan yang sesuai demi menjaga keamanan dan integritas situs web mereka. Proses identifikasi risiko menghasilkan suatu daftar peristiwa risiko dengan informasi pendukungnya yang dikenal dengan nama register risiko (*risk register*) [13][14]. Berikut merupakan tabel identifikasi risiko yang peneliti temukan:

Tabel 2. Risiko Teridentifikasi

ID	Risiko Teridentifikasi
1	Kerentanan Sistem Manajemen Konten (CMS)
2	Kurangnya Pembaruan Perangkat Lunak
3	Konfigurasi yang buruk
4	Penyalahgunaan atau pencurian kredensial administrator
5	Serangan berbasis web seperti SQL injection, cross-site scripting (XSS), atau serangan injeksi kode.
6	Kurangnya pemantauan dan deteksi terhadap aktivitas mencurigakan pada website.
7	Kebocoran informasi sensitif

3.3.2 Analisis Risiko

Analisis risiko dilakukan secara kualitatif dengan mendefinisikan peluang, dampak, dan tingkat risiko dengan tingkat signifikan, seperti “tinggi”, “sedang”, dan “rendah” serta mengevaluasi tingkat risiko yang dihasilkan terhadap kriteria kualitatif. Melalui hasil analisis risiko adalah peta risiko berupa matriks 3 x 3 sebagai berikut:

Tabel 3. Analisis Risiko

ID	Risiko Teridentifikasi	Dampak	Peluang Risiko	Tingkat Dampak	Pemilik Risiko
1	Kerentanan Sistem Manajemen Konten (CMS)	Modifikasi atau penghapusan konten website, pencurian data pengguna atau informasi	Sedang	Besar	Administrator Website

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

		sensitif, dan kerugian reputasi.			
2	Kurangnya Pembaruan Perangkat Lunak	Eksploitasi kerentanan.	Rendah	Sedang	Tim IT
3	Konfigurasi yang buruk	Kerentanan terhadap serangan, kerusakan atau pencurian data, dan gangguan layanan.	Tinggi	Besar	Tim IT
4	Penyalahgunaan atau pencurian kredensial administrator	Penghapusan atau modifikasi konten website, pencurian atau penyalahgunaan data, dan gangguan layanan.	Sedang	Besar	Administrator Website
5	Serangan berbasis web seperti SQL injection, cross-site scripting (XSS), atau serangan injeksi kode.	Pencurian data, modifikasi konten website, dan kerugian reputasi.	Rendah	Besar	Tim IT
6	Kurangnya pemantauan dan deteksi terhadap aktivitas mencurigakan pada website.	Serangan yang tidak terdeteksi, pencurian data, dan kerugian reputasi.	Rendah	Besar	Tim IT
7	Kebocoran informasi sensitif	Pencurian data, kerugian reputasi, dan sanksi hukum atau keuangan.	Rendah	Besar	Pengguna Akhir

Dalam memetakan potensi risiko berdasarkan hasil analisis risiko, peneliti mencoba memetakan agregat eksposur dampak risiko dari beberapa dampak yang dapat ditimbulkan dengan menggunakan pendekatan kualitatif [7].

3.3.3 Evaluasi Risiko

Tabel 4. Evaluasi Risiko

Peta Risiko					
Peluang	A	Tinggi			Risk- 3
	B	Sedang			Risk- 1 Risk- 4
	C	Rendah		Risk- 2	Risk- 5 Risk- 6 Risk- 7
			Kecil	Sedang	Besar
			Dampak		

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

Evaluasi ini dilakukan dengan identifikasi dan analisis risiko kemudian memetakannya dalam matriks peta risiko berdasarkan peluang dan dampak[8][9]. Berdasarkan hasil analisis risiko manajemen sistem informasi Kementerian PUPR maka risiko yang teridentifikasi, yaitu kerentanan sistem manajemen konten (CMS), konfigurasi atau layanan yang buruk, dan penyalahgunaan atau pencurian kredensial administrator memerlukan perlakuan risiko, khususnya bagi dampak operasional teknologi dan sistem informasi. Risiko dengan peta risiko sedang, seperti kurangnya pemantauan dan deteksi terhadap aktivitas mencurigakan, serangan berbasis web, dan kebocoran informasi sensitif memerlukan evaluasi lebih lanjut untuk menentukan tindakan yang sesuai. Sedangkan terkait dampak kurangnya pembaruan perangkat lunak, risiko teridentifikasi sudah dapat diterima karena kendali yang ada saat ini dinilai sudah efektif.

3.4 Perlakuan Risiko

Dalam era globalisasi yang terus berubah dan terkoneksi secara digital seperti sekarang ini, risiko keamanan informasi menjadi semakin penting bagi setiap organisasi. Risiko keamanan sistem informasi perusahaan menjadi fokus utama karena organisasi bergantung pada Sistem Manajemen Konten (CMS) yang rentan. Setiap celah keamanan dalam CMS dapat mengancam reputasi organisasi dan kepercayaan pengguna. Oleh karena itu, untuk mengatasi risiko ini, dapat memberikan langkah proaktif pada keunggulan teknologi dan keamanan.

Tabel 5. Perlakuan Risiko

ID	Risiko Teridentifikasi	Dampak	Perlakuan	Aktivitas	PIC	Waktu
1	Kerentanan Sistem Manajemen Konten (CMS)	Reputasi	Turunkan	Melakukan secure coding dan penetration testing setiap ada modul atau fitur bau.	Chief Information Security Officer (CISO)	Setelah penambahan fitur
2	Kurangnya Pembaruan Perangkat Lunak	Operasional	Terima	Rutin memperbarui perangkat	IT Manager	Setiap bulan
3	Konfigurasi yang buruk	Keamanan	Turunkan	Melakukan audit keamanan dan penyesuaian konfigurasi	Cybersecurity Specialist	Setiap semester
4	Penyalahgunaan atau pencurian kredensial administrator	Keamanan	Turunkan	Penerapan kebijakan keamanan yang ketat, penerapan SOP toleransi risiko, dan manajemen hak akses	IT Security Officer	Setiap perubahan struktur
5	Serangan berbasis web seperti SQL injection, cross-site scripting (XSS), atau serangan injeksi kode.	Keamanan	Turunkan	Penerapan tindakan mitigasi seperti penggunaan filter input, monitoring aktifitas mencurigakan, dan secure coding.	Web Developer	Setiap rilis perangkat lunak
6	Kurangnya pemantauan dan deteksi terhadap	Operasional	Turunkan	Penerapan sistem monitoring dan deteksi keamanan secara terus-	Network Security Analyst	Secara kontinyu

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 2 | Issue 2 | bulan September (2024)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

	aktivitas mencurigakan pada website.			menerus		
7	Kebocoran informasi sensitif	Legal	Turunkan	Penggunaan enkripsi data, pelatihan keamanan bagi staf, penerapan kebijakan kebocoran data	Legal and Compliance Officer	Setiap kali ada kejadian

Peneliti merekomendasikan untuk menerapkan strategi yang terdiri dari dua pilar utama: perlindungan dan pencegahan. Pertama, meningkatkan keamanan dengan mengadopsi praktik secure coding dan melakukan penetration testing secara teratur setiap kali ada penambahan fitur baru dalam CMS. Pendekatan ini memastikan bahwa setiap elemen baru yang diperkenalkan ke dalam sistem telah diuji dan diverifikasi untuk keamanannya sebelum diperkenalkan kepada pengguna. Namun, peneliti juga menyadari bahwa risiko keamanan tidak hanya berasal dari sumber internal, tetapi juga dari perubahan di lingkungan eksternal seperti ancaman serangan berbasis web seperti SQL injection atau cross-site scripting. Oleh karena itu, sebagai langkah pencegahan dapat menerapkan filter input yang kuat, memantau aktivitas mencurigakan secara terus-menerus, dan menerapkan praktik secure coding secara konsisten di seluruh infrastruktur. Kemudian, mengaudit keamanan dan menyempurnakan konfigurasi sistem secara berkala untuk memastikan bahwa tidak ada celah yang terbuka bagi pihak yang tidak sah. Dalam menghadapi risiko penyalahgunaan kredensial administrator, dapat mengimplementasikan kebijakan keamanan yang ketat, menerapkan SOP toleransi risiko, dan membatasi hak akses administrator hanya untuk tugas yang diperlukan. Melalui cara ini, dapat meminimalkan risiko akses tidak sah dan menjaga kontrol yang ketat atas sistem. Selain itu, dengan menyusun SOP toleransi risiko yang komprehensif dan jelas, organisasi dapat lebih baik mengelola risiko mereka dengan meminimalkan dampak negatifnya dan memaksimalkan peluang yang muncul. Selanjutnya, peneliti menyadari pentingnya pemantauan dan deteksi yang efektif terhadap aktivitas mencurigakan. Oleh karena itu, peneliti menginisiasi penerapan sistem monitoring dan deteksi keamanan secara terus-menerus. Dengan demikian, dapat mendeteksi dan merespons aktivitas mencurigakan dengan cepat, mengurangi risiko kerugian lebih lanjut. Terakhir, untuk melindungi informasi sensitif dari kebocoran, kami mengambil langkah-langkah untuk menerapkan enkripsi data, memberikan pelatihan keamanan bagi staf, dan menerapkan kebijakan kebocoran data yang ketat. Dengan menerapkan strategi ini, tidak hanya meningkatkan ketahanan organisasi terhadap risiko, tetapi juga memperkuat fondasi untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta layanan publik yang berkualitas dan terpercaya [4].

3.5 Pemantauan dan Tinjauan

Pemantauan dan tinjauan dilakukan setelah rekomendasi perlakuan risiko diterapkan oleh ahli TI unit BPIW. Tahap ini ditujukan untuk mendeteksi dan mengantisipasi adanya perubahan dalam hal konteks organisasi, profil risiko, level setiap risiko dan efektivitas mitigasi

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

risiko. Proses pemantauan dan tinjauan dilakukan dengan mengawasi sejauh mana rencana penanganan risiko, strategi, dan sistem manajemen risiko dapat berjalan efektif [10]. Pemantauan merupakan tindakan rutin untuk mengevaluasi kinerja aktual dari proses manajemen risiko dan membandingkannya dengan rencana yang telah ditetapkan atau harapan yang telah disusun [12]. Sementara itu, tinjauan adalah evaluasi berkala terhadap kondisi saat ini, dengan fokus khusus pada efektivitas pengendalian risiko keuangan atau pasar, serta cara untuk meningkatkan analisis risiko yang sedang dilakukan. Tujuan dari pelaksanaan pemantauan dan tinjauan yang berkesinambungan adalah untuk memberikan keyakinan yang memadai terhadap pencapaian tujuan dari penerapan sistem manajemen risiko secara menyeluruh. Dalam penelitian ini, hasil dari kegiatan pemantauan dan tinjauan akan berupa rekomendasi yang dapat membantu dalam memperkuat kapabilitas operasional sistem informasi di unit organisasi BPIW.

3.6 Pencatatan dan Pelaporan

Pencatatan dan pelaporan dilakukan setelah adanya hasil perlakuan risiko, rekomendasi yang diberikan untuk dilakukan pada sistem informasi. Hasil dari implementasi manajemen risiko sistem informasi diamati oleh ahli TI unit BPIW. Seluruh kegiatan yang dilakukan oleh peneliti melibatkan seluruh staff bagian yang terkait dengan pengelolaan keamanan TI. Pencatatan dan pelaporan diberikan kepada pihak BPIW dimana peneliti melakukan komunikasi dan melaporkan terkait kemungkinan risiko yang berpotensi menghambat proses sistem informasi, dan memberikan saran yang dapat dilakukan oleh organisasi untuk meminimalisir kemungkinan yang akan terjadi suatu saat nanti.

4. Kesimpulan dan Saran

Penerapan framework ISO 31000 dalam manajemen risiko sistem informasi di Unit Organisasi BPIW Kementerian PUPR menawarkan pendekatan sistematis untuk mengidentifikasi, mengevaluasi, dan mengelola risiko. Analisis menunjukkan beberapa risiko, termasuk kerentanan sistem manajemen konten (CMS), konfigurasi yang buruk, dan kebocoran informasi sensitif. Untuk mengatasi risiko ini, diperlukan perlakuan risiko yang tepat, seperti strategi keamanan yang mencakup praktik secure coding, monitoring keamanan yang terus-menerus, pengembangan SOP toleransi risiko, serta peningkatan kesadaran dan pelatihan keamanan bagi staf. Penerapan strategi-strategi ini dapat meningkatkan keamanan, ketersediaan, dan integritas sistem informasi, mendukung tata kelola pemerintahan yang bersih, efektif, transparan, serta pelayanan publik yang berkualitas dan terpercaya.

Penelitian ini menyarankan agar metode identifikasi risiko lain yang mungkin lebih efektif dalam konteks Unit Organisasi BPIW Kementerian PUPR digali lebih lanjut. Selain analisis kualitatif, penelitian selanjutnya dapat menggunakan pendekatan kuantitatif untuk mengevaluasi dampak dan peluang risiko lebih terperinci. Usulan kerangka kerja untuk evaluasi kontinu terhadap efektivitas perlakuan risiko yang diimplementasikan juga penting untuk memungkinkan perbaikan berkelanjutan dan adaptasi terhadap perubahan lingkungan. Dengan pengembangan lebih lanjut dalam aspek-aspek ini, penelitian mendatang diharapkan dapat memberikan pemahaman yang lebih mendalam dan solusi yang lebih efektif dalam manajemen risiko sistem informasi di Unit Organisasi BPIW Kementerian PUPR, serta kontribusi yang lebih besar terhadap praktik manajemen risiko secara keseluruhan.

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

Referensi

[1] Indonesia Security Incident Response Team on Internet Infrastructure (ID-CERT). (2021). Panduan manajemen risiko keamanan informasi. ID-CERT.

[2] ISACA. (2020). Information security management. ISACA.

[3] International Organization for Standardization (ISO). (2018). ISO 31000:2018 - Risk management. International Organization for Standardization.

[4] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB). (2020). Pedoman tata kelola teknologi informasi dan komunikasi pada instansi pemerintah. Kementerian PANRB.

[5] National Institute of Standards and Technology (NIST). (2018). NIST special publication 800-30 revision 1: Guide for conducting risk assessments. NIST.

[6] Atmojo, SA, & Manuputty, AD (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office. JATISI (Jurnal Teknik Informatika Dan …, jurnal.mdp.ac.id, <http://jurnal.mdp.ac.id/index.php/jatisi/article/view/525>

[7] Miftakhatun, M (2020). Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000. Journal of Computer Science and Engineering …, icsejournal.com, <https://icsejournal.com/index.php/JCSE/article/view/76>

[8] Lantang, GW, Cahyono, AD, & Sitokdana, MNN (2019). Analisis risiko teknologi informasi pada aplikasi sap di pt serasi autoraya menggunakan iso 31000. Sebatik, jurnal.wicida.ac.id, <https://jurnal.wicida.ac.id/index.php/sebatik/article/view/441>

[9] Wicaksono, AY (2020). Applying ISO: 31000: 2018 as risk management strategy on heavy machinery vehicle division. International journal of science …, download.garuda.kemdikbud.go.id, <http://download.garuda.kemdikbud.go.id/article.php?article=1766623&val=18875&title=Applying%20ISO310002018%20as%20Risk%20Management%20Strategy%20on%20Heavy%20Machinery%20Vehicle%20Division>

[10] Parviainen, T, Goerlandt, F, Helle, I, Haapasaari, P, & ... (2021). Implementing Bayesian networks for ISO 31000: 2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and …. Journal of …, Elsevier, <https://www.sciencedirect.com/science/article/pii/S0301479720314456>

[11] Fachrezi, MI (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000: 2018 Diskominfo Kota Salatiga. JATISI (Jurnal Teknik Informatika dan Sistem …, jurnal.mdp.ac.id, <https://jurnal.mdp.ac.id/index.php/jatisi/article/view/789>

[12] Setiawan, I, Sekarini, AR, & ... (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto. MATRIK: Jurnal …, journal.universitasbumigora.ac.id, <http://journal.universitasbumigora.ac.id/index.php/matrik/article/view/1093>

[13] Andika, D, & Wijaya, A (2022). Manajemen risiko teknologi informasi menggunakan framework ISO 31000: 2018 pada PT. Trust Lerinvital Timur. Jurnal Mnemonic, ejournal.itn.ac.id, <https://ejournal.itn.ac.id/index.php/mnemonic/article/view/4778>

[14] Sitanggang, PA, & Sitanggang, FA (2022). Analisis Implementasi Manajemen Risiko Berdasarkan SNI ISO 31000: 2018 (Studi Kasus: Sparepart Personal Computer Second Jambi). Eksis: Jurnal

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
*Volume 2 | Issue 2 | bulan **September** (2024)*
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

Ilmiah Ekonomi dan …, eksis.unbari.ac.id, <http://eksis.unbari.ac.id/index.php/EKSIS/article/view/293>

[15] Muryanti, E, & Hartomo, KD (2021). Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000. JATISI (Jurnal Teknik Informatika dan …, jurnal.mdp.ac.id, <https://jurnal.mdp.ac.id/index.php/jatisi/article/view/948>