Jurnal Teknik Mesin, Industri, Elektro dan Informatika
Volume 4, Nomor 1, Tahun 2025
E-ISSN: 2963-7805; P-ISSN: 2963-8208, Hal. 255-264
DOI: https://doi.org/10.55606/jtmei.v4i1.4819
Available Online at: https://ejurnal.politeknikpratama.ac.id/index.php/jtmei

Manajemen Risiko Keamanan Aset Teknologi Informasi di DISKOMINFOSANDITIK Kabupaten Sumedang Menggunakan ISO 31000:2018

Irma Rahayu[1*], David Setiadi[2], Dwi Yuniarto[3]
[1,2,3]Universitas Sebelas April, Indonesia
E-mail: a22100069@mhs.stmik-sumedang.ac.id[1], david@unsap.ac.id[2], dwiyuniarto@unsap.ac.id[3]

Alamat: Jl. Angkrek Situ No. 19, Situ, Kab.Sumedang
**Korespondensi penulis: a22100069@mhs.stmik-sumedang.ac.id*

Abstract. *The Sumedang Regency Communication and Informatics, Coding and Statistics Service is a government agency that utilizes information technology to support its operational activities. This research examines how security risks are managed for information technology assets in the Department. The risk management approach used in this research refers to ISO 31000:2018. The main objective of this research is to evaluate the extent to which the implementation of the ISO 31000:2018 standard is effective in protecting IT assets and minimizing risks that could disrupt smooth operations. The methodology used includes identification, analysis, evaluation and risk management. The identification results show that there are 14 potential risks, consisting of 7 low level risks, 3 medium level risks, and 4 high level risks. Risks in the high category require more attention, especially those related to power outages, which are recommended to be overcome by installing an automatic generator.*

Keywords*: Asset Security, Information Technology, Risk Management.*

Abstrak. Dinas Komunikasi dan Informatika, Persandian, dan Statistik Kabupaten Sumedang merupakan lembaga pemerintah yang memanfaatkan teknologi informasi untuk mendukung kegiatan operasionalnya. Penelitian ini mengkaji bagaimana pengelolaan risiko keamanan terhadap aset teknologi informasi di Dinas tersebut. Pendekatan manajemen risiko yang digunakan dalam penelitian ini mengacu pada ISO 31000:2018. Tujuan utama dari penelitian ini adalah untuk mengevaluasi sejauh mana penerapan standar ISO 31000:2018 efektif dalam melindungi aset TI dan meminimalkan risiko yang dapat mengganggu kelancaran operasional. Metodologi yang digunakan mencakup identifikasi, analisis, evaluasi, dan pengelolaan risiko. Hasil identifikasi menunjukkan adanya 14 potensi risiko, terdiri dari 7 risiko dengan tingkat rendah, 3 risiko dengan tingkat menengah, dan 4 risiko dengan tingkat tinggi. Risiko dengan kategori tinggi memerlukan perhatian lebih, terutama terkait dengan masalah pemadaman listrik, yang disarankan untuk diatasi dengan pemasangan genset otomatis.

Kata kunci: Keamanan Aset, Manajemen Risiko, Teknologi Informasi

1. PENDAHULUAN

Kemajuan teknologi memiliki peran yang sangat penting bagi dunia bisnis. Namun, penerapan teknologi informasi di perusahaan juga membawa sejumlah tantangan dan potensi risiko. Risiko sendiri didefinisikan sebagai kemungkinan terjadinya peristiwa yang dapat menyebabkan kerugian atau mengganggu kelancaran proses bisnis perusahaan. Oleh sebab itu, dalam bidang teknologi informasi, penerapan manajemen risiko menjadi hal yang esensial untuk mengurangi risiko dan dampak yang ditimbulkannya (Yudha Andika & Fritz Wijaya, 2022).

Manajemen risiko yang diterapkan dalam perusahaan membuat aset teknologi informasi menjadi lebih bermanfaat dan berfungsi secara optimal. Meskipun tidak semua risiko dapat

Received Desember 29, 2024; Revised Januari 16, 2025; Accepted Februari 03, 2025; Online Available Februari 06, 2025

dihilangkan sepenuhnya, risiko terkait TI dapat diminimalkan sehingga memberikan efek positif berupa proses bisnis yang lebih efisien dan efektif. Perusahaan yang berkembang akan menyadari pentingnya pengelolaan risiko, terutama dalam perencanaan dan implementasi teknologi informasi. Pengelolaan ini mencakup berbagai sektor yang membutuhkan penerapan manajemen risiko TI secara maksimal, tidak hanya terbatas pada satu sektor saja (Rahmatika et al., n.d.).

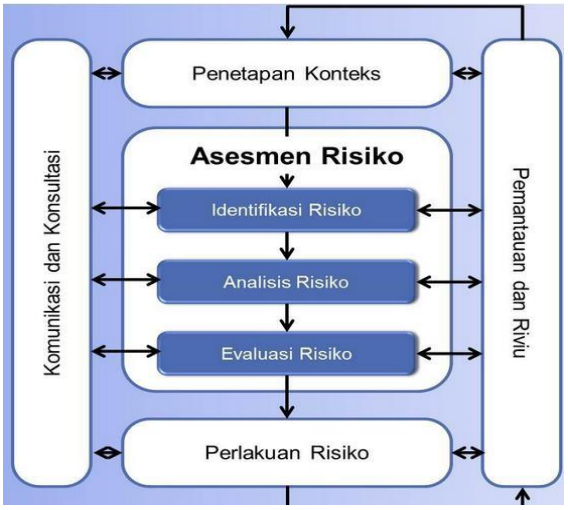
Dinas Komunikasi dan Informatika Persandian dan Statistik, yang beralamat di Jalan Angkrek No.103 Sumedang, merupakan lembaga pemerintahan di Kabupaten Sumedang, Provinsi Jawa Barat. Lembaga ini bertanggung jawab atas penyelenggaraan urusan pemerintahan di bidang komunikasi, informatika, statistik, dan persandian, termasuk menjalankan tugas pembantuan yang diberikan kepada daerah.

ISO 31000:2018, yang diluncurkan pada Februari 2018 untuk menggantikan ISO 31000:2009, adalah standar internasional yang menyediakan kerangka kerja terpadu untuk identifikasi, evaluasi, dan pengelolaan risiko. Standar ini mendukung keberlanjutan operasional dengan pendekatan sistematis dan proaktif dalam mencegah ancaman sekaligus meningkatkan efisiensi (Fachrezi et al., 2021). Dengan menerapkan prinsip-prinsip ISO 31000:2018, Dinas Komunikasi dan Informatika Persandian dan Statistik Kabupaten Sumedang dapat mengelola risiko keamanan aset TI dengan lebih efektif. Langkah ini diharapkan dapat mengurangi dampak buruk, ancaman keamanan siber, gangguan sistem, dan kebocoran data.

Penelitian ini bertujuan untuk mengeksplorasi penerapan ISO 31000:2018 dalam melindungi aset teknologi informasi di Dinas Komunikasi dan Informatika Persandian dan Statistik Kabupaten Sumedang. Melalui proses identifikasi dan analisis risiko yang komprehensif, diharapkan organisasi dapat meningkatkan perlindungan terhadap aset digitalnya.

2. METODE PENELITIAN

Untuk memastikan bahwa hasil yang diperoleh sesuai dengan tujuan yang diharapkan, metode penelitian merupakan langkah penting dalam proses penelitian. ISO 31000 berisi prinsip dan pedoman untuk mengelola risiko. Secara umum, tahapan berikut adalah tahapan utama dalam proses manajemen risiko (Fachrezi et al., 2021).



Gambar 1. Tahap Penelitian

Komunikasi dan Konsultasi

Tahap ini memegang peranan penting dalam mendukung proses manajemen risiko. Tujuannya adalah membantu para pemangku kepentingan memahami risiko yang ada, membuat keputusan yang tepat, serta menentukan cara penanganan risiko dengan efektif.

Penetapan Tujuan dan Konteks

Tahap ini bertujuan untuk menyelaraskan proses bisnis dengan risiko yang relevan dalam ruang lingkup yang telah ditetapkan. Penilaian risiko dilakukan berdasarkan konteks dan kriteria yang sudah ditentukan agar prosesnya berjalan secara efektif. Langkah ini juga memastikan penanganan ancaman dilakukan secara tepat (Patrick et al., 2022) .

Penilaian Risiko

Tahap ini bertujuan untuk mengidentifikasi berbagai risiko yang dapat mengancam keamanan aset teknologi informasi di Dinas Komunikasi dan Informatika Persandian dan Statistik Kabupaten Sumedang. Identifikasi dilakukan dengan menganalisis peluang terjadinya suatu risiko serta dampaknya terhadap keamanan aset tersebut. Risiko yang telah teridentifikasi kemudian diklasifikasikan ke dalam kategori rendah, menengah, atau tinggi dengan

menggunakan matriks manajemen risiko. Proses ini mencakup tiga langkah utama sebagai berikut:

1) Identifikasi Risiko

Langkah ini bertujuan untuk menemukan dan menjelaskan potensi risiko dengan menggunakan data atau informasi yang telah dikumpulkan sebelumnya.

2) Analisis Risiko

Tahap ini melibatkan penentuan tingkat kemungkinan terjadinya risiko berdasarkan frekuensi. Analisis ini bertujuan untuk memahami sifat dan karakteristik dari setiap risiko. Sebagai alat bantu, tabel kemungkinan digunakan untuk menilai seberapa sering risiko tersebut dapat terjadi dalam jangka waktu tertentu.

Tabel 1. *Likelihood*

Likelihood			
Rating	Kriteria	Keterangan	Frekuensi
1	*Rare*	Risiko hampir tidak pernah muncul	>2 tahun
2	*Unlikely*	Risiko jarang muncul	1 – 2 tahun
3	*Possible*	Risiko terjadi sesekali	7 – 12 bulan/tahun
4	*Likely*	Risiko sering muncul	4 – 6 bulan/tahun
5	*Almost Certain*	Risiko dipastikan akan terjadi	1 – 3 bulan/tahun

Sumber: (Hutagalung, 2022)

Selanjutnya, digunakan tabel dampak untuk menilai konsekuensi yang akan timbul jika risiko yang teridentifikasi benar-benar terjadi.

Tabel 2. *Impact*

Impact		
Rating	Kriteria	Keterangan
1	*Insignifican*	Risiko tidak memengaruhi kelancaran aktivitas bisnis.
2	*Miror*	Risiko memiliki dampak kecil pada proses bisnis.
3	*Moderate*	Risiko berdampak pada kelangsungan proses bisnis.
4	*Major*	Risiko memengaruhi beberapa aspek dalam proses bisnis.
5	*Catastrophic*	Risiko mengganggu keseluruhan proses bisnis.

Sumber: (Hutagalung, 2022)

3) Evaluasi Risiko

Pada tahap ini, hasil dari analisis risiko dibandingkan dengan standar risiko yang telah ditentukan sebelumnya.

4) Perlakuan Risiko

Tujuan dari penanganan risiko adalah untuk mengevaluasi berbagai alternatif dalam mengelola risiko, serta menerapkan strategi manajemen risiko yang efektif untuk mengendalikan risiko, mengurangi potensi kerugian, dan meningkatkan kinerja

organisasi.

5) Monitoring dan Review

Tahap ini merupakan bagian yang tidak terpisahkan dari proses manajemen risiko. Tujuan utamanya adalah untuk memastikan bahwa seluruh langkah dalam manajemen risiko dijalankan sesuai dengan rencana yang telah disusun.

3. HASIL DAN PEMBAHASAN

Identifikasi Risiko

Identifikasi risiko bertujuan untuk mencari, menemukan, dan menjelaskan berbagai risiko dengan memanfaatkan data yang diperoleh melalui wawancara. Berikut adalah rincian beberapa potensi risiko yang dapat dilihat di bawah ini:

Tabel 3. Identifikasi Risiko

Sumber Risiko	Kemungkinan Risiko
Alam/Lingkungan	Banjir
	Gempa Bumi
	Petir
	Kebakaran
	Listrik Padam
Manusia	*Human Eror*
	Akses tidak sah terhadap data dan informasi
	Kebocoran Informasi atau Data
	Serangan Virus/*Malware*
Sistem dan Infrastruktur	*Data Corrupt*
	Server Down
	Koneksi Internet Terputus
	Overload
	Overheat

Analisis Risiko

Setelah tahap identifikasi risiko selesai, langkah berikutnya adalah melakukan analisis risiko. Tujuan dari analisis ini adalah untuk mengidentifikasi risiko yang berpotensi terjadi. Risiko yang telah teridentifikasi kemudian dievaluasi berdasarkan kemungkinan terjadinya *(likelihood)* dan dampaknya *(impact).*

Dalam penilaian kemungkinan risiko, diberikan nilai frekuensi antara 1 hingga 5, di mana angka yang lebih tinggi menunjukkan frekuensi kejadian risiko yang lebih sering dan dampak yang lebih besar. Tabel berikut menunjukkan hasil penelitian mengenai frekuensi dan dampak risiko:

Tabel 4. Hasil Penelitian Frekuensi dan Dampak

Kode	Kemungkinan Risiko	Frekuensi	Dampak
A1	Banjir	1	3
A2	Gempa Bumi	2	2
A3	Petir	1	2
A4	Kebakaran	1	5
M1	Listrik Padam	3	5
M2	*Human Eror*	2	2
M3	Akses tidak sah terhadap data dan informasi	2	3
M4	Kebocoran Informasi atau Data	4	1
M5	Serangan Virus/*Malware*	2	3
S1	*Data Corrupt*	2	4
S2	*Server Down*	3	4
S3	Koneksi Internet Terputus	3	5
S4	*Overload*	2	4
S5	*Overheat*	2	2

Evaluasi Risiko

Pada tahap ini, hasil dari analisis risiko dibandingkan dengan kriteria risiko yang telah ditetapkan sebelumnya. Tujuan utama dari tahap ini adalah untuk menentukan tingkat prioritas risiko, apakah termasuk risiko tinggi atau rendah. Tabel berikut menunjukkan hasil dari evaluasi risiko:

Tabel 5. Matriks Evaluasi Risiko

Impact	***Likelihood (frekuensi)***				
	Rare	*Unlikely*	*Possible*	*Likely*	*Almost Certain*
Catastrophic	A4		M1, S3		
Major		S1, S4	S2		
Moderate	A1	M3		M5	
Minor	A3	A2, M2, S5			
Insignifican		M4			

Tabel 5 menyajikan perhitungan mengenai Likelihood dan Impact. Dari 14 potensi risiko yang ada, masing-masing dikelompokkan berdasarkan rasio dan kemudian dikategorikan ke dalam tiga tingkat: rendah *(low)*, menengah *(moderate)*, dan tinggi *(high)*.

Tabel 6. Klasifikasi Risiko Berdasarkan Tingkatannya

Kode	Kemungkinan Risiko	Frekuensi	Dampak	Level
A1	Banjir	1	3	Low Risk
A2	Gempa Bumi	2	2	Low Risk
A3	Petir	1	2	Low Risk
A4	Kebakaran	1	5	Low Risk
M1	Listrik Padam	3	5	High Risk
M2	*Human Eror*	2	2	Low Risk
M3	Akses tidak sah terhadap data dan informasi	2	3	Moderate Risk
M4	Kebocoran Informasi atau Data	2	1	Low Risk
M5	Serangan Virus/*Malware*	4	3	High Risk
S1	*Data Corrupt*	2	4	Moderate Risk
S2	*Server Down*	3	4	High Risk
S3	Koneksi Internet Terputus	3	5	High Risk
S4	*Overload*	2	4	Moderate Risk
S5	*Overheat*	2	2	Low Risk

Sebanyak 14 risiko yang teridentifikasi telah dievaluasi dan dikelompokkan berdasarkan tingkatannya, sebagaimana tercermin pada tabel 6 dalam tahap evaluasi risiko. Risiko tersebut terdiri dari 7 risiko dengan tingkat rendah *(low risk)*, 3 risiko dengan tingkat menengah *(moderate risk)*, dan 4 risiko dengan tingkat tinggi *(high risk)*.

Tabel 7. Urutan Risiko

1 - 5	*Low Risk*
6 – 11	*Moderate Risk*
12 – 17	*High Risk*
18 – 25	*Extreme Risk*

Perlakuan Risiko

Perlakuan risiko adalah saran Tindakan lajutan untuk menangani risiko yang ada (Patrick et al., 2022). Berikut table 6 untuk masing-masing perlakuan risiko:

Tabel 8. Perlakuan Risiko

Kode	Kemungkinan Risiko	Level	Perlakuan Risiko
A1	Banjir	Low Risk	Membersihkan saluran pembuangan air hujan secara berkala.
A2	Gempa Bumi	Low Risk	Memastikan bahwa semua perangkat terpasang dengan stabil dan aman. Disarankan untuk menggunakan rak server yang tahan guncangam.
A3	Petir	Low Risk	Memasang penangkal petir dan penangkal surge pada infrastruktur yang terhubung dengan perangkat IT.
A4	Kebakaran	Low Risk	Menempatkan APAR di dekat pusat data dan ruang server.
M1	Listrik Padam	High Risk	Sebaiknya genset otomatis menyala saat listrik padam.
M2	*Human Eror*	Low Risk	Meningkatkan kesadaran melalui pelatihan rutin tentang prosedur keamanan dan tata Kelola data.

Kode	Kemungkinan Risiko	Level	Perlakuan Risiko
M3	Akses tidak sah terhadap data dan informasi	Moderate Risk	Meningkatkan kontrol akses dengan menerapkan sistem enkripsi data.
M4	Kebocoran Informasi atau Data	Low Risk	Enkripsi data sensitive dan membatasi akses pengguna yang berwenang.
M5	Serangan Virus/*Malware*	High Risk	Memasang perangkat lunak antivirus dan rutin melakukan pemeriksaan virus pada setiap komputer.
S1	*Data Corrupt*	Moderate Risk	Melakukan backup data secara berkala dan memastikan penggunaan sistem penyimpanan yang handal dan aman.
S2	*Server Down*	High Risk	Menerapkan monitoring sistem secara real-time untuk menemukan masalah sebelum terjadi.
S3	Koneksi Internet Terputus	High Risk	Melakukan pemeriksaan terhadap ISP yang digunakan serta jaringan di lingkungan Dinas Komunikasi dan Informatika Persandian dan Statistik Kabupaten Sumedang
S4	*Overload*	Moderate Risk	Memantau kondisi server secara rutin untuk memastikan performanya tetap optimal, dan meningkatkan kepasasitas *bandwidth.*
S5	*Overheat*	Low Risk	Pastikan bahwa ruang server memiliki sistem pendingin (AC) yang memadai dan perawatan berkala.

4. KESIMPULAN

Dalam penelitian yang dilakukan di Dinas Komunikasi dan Informatika Statistik dan Persandian Kabupaten Sumedang mengenai manajemen risiko keamanan aset teknologi informasi dengan menggunakan standar ISO 31000:2018, ditemukan sebanyak 14 jenis risiko potensial. Dari jumlah tersebut, 7 risiko dikategorikan sebagai risiko rendah (low risk), yaitu banjir, gempa bumi, petir, kebakaran, kesalahan manusia, kebocoran data, dan overheating. Selanjutnya, terdapat 3 risiko dengan tingkat menengah (moderate risk), yaitu akses tidak sah ke data dan informasi, kerusakan data, dan kelebihan beban. Sementara itu, 4 risiko lainnya termasuk dalam kategori risiko tinggi (high risk), yaitu pemadaman listrik, serangan virus/malware, gangguan server, dan terputusnya koneksi internet.

Dengan demikian, dapat disimpulkan bahwa Dinas Komunikasi dan Informatika Statistik dan Persandian Kabupaten Sumedang perlu mengimplementasikan strategi pengelolaan risiko untuk mengurangi kemungkinan terjadinya dampak negatif dari risiko-risiko tersebut. Terutama untuk mengatasi masalah pemadaman listrik yang sering terjadi, disarankan untuk menyediakan generator set (genset) yang dapat menyala otomatis saat listrik

padam (Fachrezi et al., 2021).

DAFTAR PUSTAKA

Andika, D. Y., & Wijaya, F. A. (2022). Manajemen risiko teknologi informasi menggunakan framework ISO 31000:2018 pada PT. Trust Lerinvital Timur. *Jurnal Mnemonic, 5*(2).

Aprikasari, M., Benedicta, L., Adrielvino, A., & Ayunda, T. (2024). Penerapan ISO 31000:2018 untuk manajemen risiko IT pada sistem penerbitan PT. X. *7*(2). https://doi.org/10.55606/isaintek.v7i2.269

Buaty, N., Dewi, S. C., Dutasmara, R., & Legowo, M. B. (n.d.). Manajemen risiko teknologi informasi pada industri perbankan dengan ISO 31000:2018 framework. *Seminar Nasional Perbanas Institute 2023 "Environmental, Social, Governance (ESG) Investment and Social Responsibility."*

Fachrezi, M. I., Cahyono, A. D., & Tanaem, P. F. (2021). Manajemen risiko keamanan aset teknologi informasi menggunakan ISO 31000:2018 di Diskominfo Kota Salatiga. *Jurusan Sistem Informasi, 8*(2). http://jurnal.mdp.ac.id

Hutagalung, L. E. (2022). Analisa manajemen risiko sistem informasi manajemen rumah sakit (SIMRS) pada Rumah Sakit XYZ menggunakan ISO 31000.

Ivander, D. L., & Papilaya, F. S. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer analisis manajemen risiko teknologi informasi menggunakan framework ISO 31000:2018. *Media Online, 4*(2), 1042–1051. https://doi.org/10.30865/Klik.V4i2.1174

Lantang, G. W., Cahyono, A. D., & Sitokdana, M. N. N. (n.d.). Analisis risiko teknologi informasi pada aplikasi SAP di PT Serasi Autoraya menggunakan ISO 31000.

Liperda, R. I., & Nieng, A. S. (2023). Analisis manajemen risiko aplikasi MyPertamina dengan menggunakan ISO 31000. *INFOTECH Journal, 9*(2), 361–370. https://doi.org/10.31949/infotech.v9i2.6232

Mahardika, K. B., Wijaya, A. F., Cahyono, A. D., Studi, P., Informasi, S., Informasi, T., Kristen, U., & Wacana, S. (n.d.). Manajemen risiko teknologi informasi menggunakan ISO 31000:2018 (Studi Kasus: CV. Xy). *277–284*.

Patrick, V., Wijaya, P., & Manuputty, A. D. (2022). Manajemen risiko teknologi informasi pada BTSI UKSW menggunakan ISO 31000:2018. *9*(2), 1295–1307.

Pebriani, O. D., Zulfikar, D. H., Kom, S., Cs, M., Islam, U., Raden, N., & Palembang, F. (2022). SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada website SIMPEG di Kantor Kementerian Agama Kota Palembang. *183–190*. https://doi.org/10.31284/p.snestik.2022.2716

Rahmatika, A. N., Apriyadi, M. F., Kahfi, M. A., & Aibi, N. (n.d.). Analisis manajemen risiko teknologi informasi pada sistem informasi akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMM) menggunakan ISO 31000. *Jurnal Manajemen dan Teknologi Informasi (JMTI), 14*, 48–57. https://doi.org/10.59819

Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis manajemen risiko menggunakan ISO 31000 pada Smart Canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer), 7*(1), 91. https://doi.org/10.30865/jurikom.v7i1.1791

Setyaningrum, N. N., & Maria, E. (2024). Penerapan ISO 31000:2018 untuk manajemen risiko pada sistem informasi sekolah terpadu. *Jurnal Pendidikan Teknologi Informasi (JUKANTI), 7*.

Yolanda, B., Nasrullah, M., & Kusumawati, A. (2024a). Analisis manajemen risiko dengan menggunakan framework ISO 31000:2018 pada sistem informasi e-gudang Satpol PP Kota Surabaya.