

ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PT JAKARTA NOTEBOOK MENGGUNAKAN FRAMEWORK ISO 31000

Siti Nur Kholifah¹, Yulhendri^{2*}

Sistem Informasi, Universitas Esa Unggul

Jl. Arjuna No.09 Kebon Jeruk, Jakarta Barat 11510

lilyy.sitink@gmail.com , yulhendri@esaunggul.ac.id

Abstract

Information technology (IT) risk management is a systematic process of identifying, assessing, and managing IT risks that can affect the achievement of organizational goals. ISO 31000 is an international standard that can be used as a framework for risk management. This research aims to analyze IT risk management at PT Jakarta Notebook using the ISO 31000 framework. This research uses a qualitative research method with a case study approach. Research data was obtained through interviews, observations, and documentation. The results showed that PT Jakarta Notebook already has a fairly good IT risk management process. However, there are still some things that need to be improved, such as: Establishing a clearer risk management context, More comprehensive risk assessment, and More effective implementation of risk mitigation measures..

Article History

Submitted: 11 januari 2024

Accepted: 16 januari 2024

Published: 17 January 2024

Key Words

Risk Management, ISO 31000, Risk Analysis, Information Technology, Risk Assessment

Abstrak

Manajemen risiko teknologi informasi (TI) merupakan suatu proses yang sistematis dalam mengidentifikasi, menilai, dan mengelola risiko TI yang dapat mempengaruhi pencapaian tujuan organisasi. ISO 31000 merupakan suatu standar internasional yang dapat digunakan sebagai kerangka kerja dalam manajemen risiko. Penelitian ini bertujuan untuk menganalisis manajemen risiko TI pada PT Jakarta Notebook menggunakan framework ISO 31000. Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan studi kasus. Data penelitian diperoleh melalui wawancara, observasi, dan dokumentasi. Hasil penelitian menunjukkan bahwa PT Jakarta Notebook telah memiliki proses manajemen risiko TI yang cukup baik. Namun, masih terdapat beberapa hal yang perlu ditingkatkan, seperti: Penetapan konteks manajemen risiko yang lebih jelas, Penilaian risiko yang lebih komprehensif, dan Penerapan tindakan mitigasi risiko yang lebih efektif.

Sejarah Artikel

Submitted: 11 januari 2024

Accepted: 16 januari 2024

Published: 17 January 2024

Kata Kunci

Manajemen Risiko, ISO 31000, Analisis Risiko, Teknologi Informasi, Penilaian Risiko.

I. PENDAHULUAN

Dalam era digital yang berkembang pesat, perusahaan di seluruh dunia mengandalkan teknologi informasi sebagai tulang punggung operasional mereka. PT Jakarta Notebook, sebagai salah satu pemain utama dalam industri teknologi informasi, telah menjadi penyedia solusi dan layanan TI yang penting bagi berbagai jenis bisnis. Namun, seiring dengan kemajuan teknologi, perusahaan seperti PT Jakarta Notebook dihadapkan pada risiko-risiko yang semakin kompleks dan beragam dalam operasional teknologi informasi (TI).

JakartaNotebook adalah Online Store yang berdiri sejak tahun 1999 dan melayani pembelian seciara daring dari tahun 2003 hingga sekarang. Visi Jakartanotebook yaitu menjadi perusahaan terbesar di bidang penjualan barang IT secara daring, dan misi yaitu memberi konsumen pengalaman berbelanja melalui daring dengan menawarkan harga murah dan nyaman bagi konsumennya baik di kota maupun

pelosok. Seperti logo JakartaNotebook.com, perusahaan ini berusaha menyediakan barang termurah, terunik dan terlengkap agar konsumen merasa puas.

Situs e-commerce dibedakan menjadi tiga yang pertama adalah Business to business (B2B) seperti contohnya ralali.com, indonet-work.com, dan indotrading.com. Kedua adalah Costumer to costumer (C2C) seperti bukalapak.com, OLX.com, dan tokopedia.com. Terakhir adalah Business to costumer (B2C) seperti zalora.co.id, lazada.co.id, dan jakartanotebook.com. Toko online yang berbasis B2C di Indonesia memiliki ragam kategori produk yang dijual, seperti contohnya fashion, makanan, peralatan rumah tangga, elektronik, dan gawai. Jakartanotebook.com merupakan salah satu toko online B2C yang telah melayani penjualan online sejak tahun 2003 dengan menjual berbagai produk elektronik dan gawai beserta perlengkapannya dengan harga yang cukup murah. Kategori produk yang ditawarkan adalah notebook, peripheral, gawai, fotografi, software, display, dan networking. Selain memiliki banyak kategori produk yang dijual, jakartanote-book.com juga menawarkan promo dan layanan belanja online sehingga lebih menarik, seperti contohnya layanan gratis ongkos kirim, diskon mencapai 90%, dan diskon pada saat acara-acara tertentu misalnya tahun baru, hari kemerdekaan, atau hari natal. Pesaing yang cukup besar bagi jakartanotebook.com adalah bhinneka.com. Menurut similarweb.com jakartanotebook.com berada pada peringkat 351 di Indonesia dari situs online yang dapat di akses dengan jumlah 2,85 juta pengunjung sampai bulan Juli 2017. Namun dengan berbagai macam produk dan layanan yang ditawarkan, kunjungan ke situs jakartanotebook.com belum dapat melebihi pesaingnya bhinneka.com. Seharusnya dengan berbagai layanan yang diberikan mampu memunculkan niat dari konsumen untuk berbelanja di jakartanotebook.com.

Namun, semakin kompleksnya lingkungan teknologi informasi dan semakin kuatnya ancaman terhadap keamanan data serta operasional TI membuat PT Jakarta Notebook dan perusahaan sejenisnya dihadapkan pada risiko yang semakin tinggi. Untuk mengatasi tantangan ini, manajemen risiko menjadi kunci dalam memastikan kelangsungan operasional, kepatuhan, dan kepercayaan pelanggan.

Manajemen risiko adalah pendekatan yang terstruktur dan komprehensif untuk mengidentifikasi, menilai, mengelola, dan memonitor risiko yang mungkin mempengaruhi pencapaian tujuan organisasi. Salah satu standar internasional yang diakui secara luas dalam manajemen risiko adalah ISO 31000. Standar ini menyediakan panduan untuk mengembangkan dan mengimplementasikan kerangka kerja manajemen risiko yang efektif.

Penelitian ini bertujuan untuk menganalisis manajemen risiko berbasis ISO 31000 pada aspek operasional teknologi informasi di PT Jakarta Notebook. Penerapan manajemen risiko yang tepat dalam operasional TI akan membantu organisasi untuk mengidentifikasi dan mengelola risiko dengan lebih baik, sehingga dapat meminimalkan dampak negatifnya pada operasional dan mencapai tujuan bisnis yang lebih baik.

II. TINJAUAN PUSTAKA

a. Risiko

Risiko merupakan hasil dari kombinasi antara kemungkinan dan tingkat keparahan suatu peristiwa. Besarnya risiko dipengaruhi oleh beberapa faktor, seperti tingkat paparan, lokasi, pengguna, jumlah, dan kerentanan unsur yang terlibat. Manajemen risiko adalah suatu serangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memonitor, dan mengendalikan risiko yang timbul dari kegiatan operasional suatu perusahaan. Tujuan dari penerapan manajemen risiko adalah mengurangi risiko-risiko beragam yang terkait dengan bidang yang telah dipilih, hingga tingkat yang dapat diterima oleh masyarakat. Risiko tersebut dapat berasal dari berbagai jenis ancaman yang muncul dari lingkungan, teknologi, manusia, organisasi, dan politik. Di sisi lain, implementasi manajemen risiko melibatkan segala cara yang tersedia bagi manusia, terutama bagi entitas manajemen risiko seperti manusia, staf, dan organisasi. Risiko selalu terkait dengan ketidakpastian, sehingga dalam setiap kegiatan, baik di bidang keuangan, manajemen perusahaan, maupun dalam kehidupan sehari-hari, risiko tidak dapat dihindari. Oleh karena itu, diperlukan suatu pendekatan, yang disebut manajemen risiko, untuk mengelola risiko tersebut sehingga dapat diubah menjadi peluang, atau bahkan dapat menjadi ancaman bagi perusahaan lain.

b. Manajemen Risiko

Manajemen risiko merupakan usaha manajemen dalam mengelola risiko pada aktivitas operasional perusahaan, melibatkan analisis risiko, evaluasi risiko, dan perencanaan penanganannya. Dengan pelaksanaan manajemen risiko yang efektif, perusahaan dapat menjaga nilai (mengamankan nilai) dan meningkatkan nilai (menciptakan nilai) perusahaan. Peran dari manajemen risiko diharapkan mampu mengantisipasi perubahan lingkungan yang cepat, mengembangkan tata kelola perusahaan, mengoptimalkan manajemen strategis, menjaga keamanan sumber daya dan aset yang dimiliki organisasi, serta mengurangi pengambilan keputusan reaktif oleh manajemen puncak. Manajemen risiko dalam konteks Keamanan Teknologi Informasi (TI) adalah suatu proses untuk memahami faktor-faktor potensial yang dapat menyebabkan kegagalan dalam menjaga kerahasiaan, integritas, atau ketersediaan sistem informasi. Sebagai contoh, salah satu risiko keamanan TI dapat muncul dalam bentuk kesalahan informasi yang dihasilkan oleh sistem, yang dapat berdampak negatif pada pengolahan informasi terkait.

c. ISO 31000

ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang di modifikasi oleh International Organization for Standardization (ISO). Pada penerapannya, ISO 31000 dapat diterapkan dalam berbagai jenis usaha publik atau swasta serta mampu menyiapkan prinsip dan tahapan mengelola risiko sehingga bisa digunakan sebagai gambaran dalam manajemen risiko guna menerapkan manajemen risiko yang lebih efektif. Tujuan dari ISO sendiri adalah untuk memberikan prinsip-prinsip dan pedoman untuk manajemen risiko yang diakui secara universal. ISO 31000 adalah panduan penerapan risiko yang terdiri atas tiga elemen: prinsip (principle), kerangka kerja (framework), dan proses (process). Prinsip manajemen risiko adalah dasar praktik atau filosofi manajemen risiko. Secara keseluruhan, versi ISO 31000:2018 menyederhanakan versi sebelumnya tahun 2009. Perubahan tersebut terlihat dari perubahan nama dari "prinsip dan pedoman" menjadi hanya "pedoman," dan jumlah halaman yang berkurang dari 24 halaman menjadi 16 halaman. Diagram yang menggambarkan hubungan antara prinsip, kerangka kerja, dan proses manajemen risiko juga mengalami perubahan. Pada versi 2009, ketiga elemen ini digambarkan sebagai rangkaian unsur yang berurutan, sementara pada versi 2018, ketiganya digambarkan sebagai sistem terbuka yang saling berhubungan.

III. METODELOGI

Peneliti menggunakan metode penelitian Studi Kasus dengan pendekatan kualitatif. Pendekatan ini digunakan untuk menggambarkan dan menguraikan data dan fakta yang terkait dengan objek studi kasus ke dalam bentuk kata-kata. Salah satu jenis pendekatan kualitatif yang diterapkan adalah metode penelitian Studi Kasus, di mana fokus penelitian hanya terpusat pada satu objek tertentu. Dengan menggunakan metode ini, peneliti dapat dengan mudah mengumpulkan data yang diperlukan untuk memecahkan permasalahan yang muncul pada objek studi kasus. Penelitian ini melibatkan beberapa tahapan sesuai dengan manajemen risiko dari framework ISO 31000:2018. Untuk menjalankan penelitian ini, informasi yang diperlukan diperoleh melalui wawancara dengan pihak internal yang terkait dan observasi langsung di lokasi PT. Jakarta Notebook yang berlokasi di Kedoya, Jakarta Barat.

Peneliti menerapkan metode analisis data yang melibatkan tahapan-tahapan dari Risk Assessment hingga Risk Treatment. Pendekatan ini dilakukan dengan mempertimbangkan dengan cermat cakupan, konteks, dan kriteria risiko. Langkah-langkah untuk memastikan kelancaran penelitian mencakup memperhitungkan scope, context, dan criteria dari risiko, berkomunikasi dan berkonsultasi dengan pihak terkait, mengevaluasi track record serta melakukan pelaporan. Selanjutnya, peneliti melakukan monitoring dan review guna memastikan keseluruhan penelitian berjalan dengan baik.



Gambar 1

Tahap awal adalah risk assessment (penilaian risiko) yang melibatkan 3 langkah, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko.

- Identifikasi risiko adalah langkah untuk mengidentifikasi segala risiko yang mungkin mempengaruhi perusahaan dalam mencapai tujuannya.
- Analisis risiko melibatkan cara dan langkah-langkah yang mendalam untuk memahami risiko-risiko yang ada. Analisis dapat dilakukan dengan berbagai tingkat rinci, tergantung pada tujuan, ketersediaan informasi, dan sumber daya yang tersedia.
- Evaluasi risiko adalah tahap untuk menentukan manajemen risiko terhadap tingkatan risiko dengan menggunakan kriteria yang telah ditentukan. Hasil evaluasi risiko perlu dicatat, dikomunikasikan, dan divalidasi di tingkat organisasi yang sesuai.

Tahap kedua adalah risk treatment (perlakuan risiko), yang melibatkan upaya untuk menyelesaikan pilihan yang dapat mengurangi atau mengatasi semua kemungkinan dampak dari risiko yang ada dan menerapkan perlakuan yang sesuai

IV. HASIL DAN PEMBAHASAN

4.1 Komunikasi dan Konsultasi Risiko

Komunikasi dan Konsultasi risiko membantu peneliti untuk memahami perusahaan (mengetahui profil perusahaan, visi, misi dan tujuan, proses bisnis dan struktur organisasi), mengetahui risiko yang pernah terjadi dan mengumpulkan data penelitian (preferensi risiko, kebijakan/cara mengelola risiko, dan lain sebagainya), komunikasi dan konsultasi risiko memiliki tujuan untuk membantu perusahaan dalam memahami risiko serta memiliki pandangan yang sama dengan peneliti terkait dengan proses manajemen risiko yang akan dilakukan. Selain dilakukan dengan dosen, komunikasi dan konsultasi risiko ini pun dilakukan oleh pihak perusahaan, yaitu dengan branch manager, supervisor, karyawan front-office, dan karyawan backoffice PT JakartaNotebook selama proses manajemen risiko berlangsung.

4.2 Skope, Konteks, dan Kriteria

Manajemen risiko antara satu perusahaan dengan perusahaan lain memiliki ciri khas yang berbeda-beda sesuai dengan kebutuhan penggunaannya dalam melakukan asesmen risiko. Oleh karena itu, peneliti melakukan penetapan skope, konteks, dan kriteria penilaian tingkat risiko untuk mendapatkan proses manajemen risiko yang khas sesuai dengan studi kasus penelitian.

Adapun skope pada pelaksanaan analisis manajemen risiko yang ditentukan oleh peneliti yaitu untuk menganalisis manajemen risiko teknologi informasi pada PT. Jakarta Notebook. Peneliti memilih

skope untuk meneliti kantor pusat karena memiliki konteks atau tujuan untuk mengetahui apakah kantor pusat sudah melaksanakan teknologi informasi dengan baik sehingga mendukung visi dan misi perusahaan. Setelah menetapkan skope dan konteks, peneliti menentukan kriteria risiko dengan menetapkan kriteria likelihood yang terdiri atas 5 kriteria (certain, likely, possible, unlikely, dan rare) dengan nilai dan keterangan periode waktu pada masing-masing kriteria yang berfungsi sebagai skala pengukuran frekuensi waktu terjadinya sebuah risiko. Selain itu, peneliti juga menentukan kriteria impact yang dibedakan menjadi 5 nilai kategori dampak yang akan terjadi pada suatu risiko (catastrophic, major, moderate, minor, dan insignificant).

4.3 Asesmen Risiko

Setelah menentukan skope analisis, konteks atau tujuan analisis, dan kriteria risiko yang akan digunakan. Tahap selanjutnya, peneliti melakukan asesmen/penilaian terhadap risiko. Dalam melakukan asesmen risiko, peneliti melakukan 4 tahapan, yaitu mengidentifikasi aset yang akan dilindungi dari risiko yang mungkin terjadi, mengidentifikasi risiko yang mungkin dapat terjadi, menganalisis risiko menggunakan kriteria risiko yang telah ditentukan pada tahap sebelumnya, dan mengevaluasi risiko berdasarkan pemetaan matriks evaluasi risiko.

4.3.1 Tahap Identifikasi Risiko (Risk Identification)

Tahap pertama yang dilakukan dalam tahap penilaian resiko (risk assessment) adalah proses identifikasi resiko (risk identification) atau identifikasi aset yang berhubungan dengan website Jakarta Notebook. Dalam proses ini dilakukan wawancara dengan business analyst dan developer dari website ini.

- **Identifikasi Aset**

Tahap ini dilakukan identifikasi mengenai aset website Jakarta Notebook yang meliputi aset data, aset software, hingga aset hardware Perusahaan.

Table 1. Identifikasi Aset

Komponen Sistem Informasi	Aset
Data	Data barang, data supplier, data transaksi, data pelanggan
Software	Website Jakarta Notebook
Hardware	Server Database, Personal computer (PC), Server web service,

- **Identifikasi Kemungkinan Risiko**

Setelah melakukan identifikasi aset perusahaan, tahap kedua merupakan identifikasi risiko yang mungkin akan/pernah terjadi yang mengancam aset perusahaan. Berdasarkan hasil wawancara dengan narasumber untuk mengetahui kejadian-kejadian yang pernah terjadi dan mengancam aset perusahaan, hasil observasi dan berdasarkan dokumen/catatan perusahaan, peneliti menentukan identifikasi risiko berdasarkan 3 faktor risiko, yaitu alam dan lingkungan, manusia, serta sistem dan infrastruktur. Selain menentukan risiko berdasarkan 3 faktor, peneliti juga mengidentifikasi risiko tersebut berdasarkan penyebab/alasan pemilihan risiko dan dampak jika risiko tersebut terjadi. Hal tersebut dilakukan sebagai alasan mengapa risiko tersebut dipilih dalam identifikasi risiko yang mungkin akan/pernah terjadi. Hasil penentuan risiko yang mungkin akan/pernah terjadi berdasarkan 3 faktor beserta identifikasi penyebab/alasan dan dampak risiko tersebut tercantum dalam hasil identifikasi risiko pada Tabel 2.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	Kode Risiko	Kemungkinan Risiko
Lingkungan / Alam	R1	Banjir
	R2	Kebakaran
	R3	Gempa Bumi

	R4	Petir
Sistem & Infrastruktur	R5	Listrik Padam
	R6	Server Down
	R7	Serangan Virus, Malware, Malicious Program
	R8	Terputusnya koneksi jaringan
	R9	Server Error
	R10	Bug pada website
	R11	Data Corrupt
	R12	Overhead
Manusian (SDM)	R13	Kurang memahami alur kerja system
	R14	Human Error
	R15	Pencurian data pada website

- **Identifikasi Dampak Risiko**
Tahap berikutnya dilakukan tahap identifikasi risiko, dengan mencari dampak-dampak yang dihasilkan dari kemungkinan risiko yang telah di temukan dari risiko yang telah diidentifikasi sebelumnya.

Tabel 3. Identifikasi Dampak Risiko

Kode Risiko	Kemungkinan Risiko	Dampak
R1	Banjir	Terjadi kerusakan infrastruktur dan menghambat aktivitas bisnis Perusahaan.
R2	Kebakaran	- Kerusakan sarana dan prasarana perusahaan - Kerugian materiil - Menghambat aktivitas perusahaan
R3	Gempa Bumi	Terjadi kerusakan infrastruktur dan proses bisnis Perusahaan terhenti.
R4	Petir	Mengalami kerusakan infrastruktur pada perusahaan dan mengalami kerugian secara finansial.
R5	Listrik Padam	Seluruh aktifitas pada perusahaan terhenti.
R6	Server Down	Tidak dapat mengakses website Jakarta Notebook dan database sehingga menghambat aktivitas dan mengakibatkan kerugian secara finansial.
R7	Serangan Virus, Malware, Malicious Program	Mengakibatkan data corrupt atau adanya bug di sistem Jakarta Notebook
R8	Terputusnya koneksi jaringan	Kerusakan aset perusahaan terutama data dan hardware, serta dapat berdampak pada kebocoran data dan

		informasi internal perusahaan yang dapat menyebabkan penyalahgunaan informasi. Sehingga risiko ini dapat menghambat hampir seluruh aktivitas perusahaan
R9	Overload	Kehilangan data dan proses loading terhambat karena log database, log temp dan log temp database terisi penuh.
R10	Bug pada website	Menimbulkan error pada kinerja sistem, menyebabkan crash pada System.
R11	Data Corrupt	Dapat mengalami kehilangan data
R12	Overhead	Kinerja hardware kurang maksimal, karena rusaknya hardware yang harus menanggung suhu panas yang terus menerus.
R13	Kurang memahami alur kerja system	Kinerja bisnis menjadi tidak maksimal
R14	Human Error	Kerusakan aset perusahaan terutama aset data dan hardware yang dapat menghambat proses bisnis sehingga sebagian aktivitas terganggu.
R15	Pencurian data pada website	Perusahaan mengalami kerugian finansial karena kehilangan asetnya

4.3.2 Tahap Analisis Risiko (Risk Analys)

Proses selanjutnya merupakan tahap analisis risiko. Disini peneliti melakukan penilaian terhadap kemungkinan-kemungkinan risiko yang telah diidentifikasi sebelumnya, dengan memperhatikan dua aspek yaitu, likelihood dan impact.

Tabel 4. Kriteria Kemungkinan (Likelihood)

Likelihood		Deskripsi	Frekuensi Kejadian
Nilai	Kriteria		
1	Rare	Suatu risiko yang hampir tidak pernah terjadi	> 2 Tahun
2	Unlikely	Suatu risiko yang jarang terjadi	1 – 2 Tahun
3	Possible	Suatu risiko yang kadang terjadi	7 – 12 Bulan
4	Likely	Suatu risiko yang sering terjadi	4 – 6 Bulan
5	Certain	Suatu risiko yang pasti terjadi	1 – 2 Bulan

Tabel 5. Dampak Risiko (Impact)

Kriteria	Deskripsi	Level / Nilai
----------	-----------	---------------

Insignificant	Risiko yang dampaknya tidak mengganggu proses bisnis dan jalannya aktivitas dari Perusahaan	1
Minor	Risiko yang dampaknya sedikit menghambat proses bisnis dan aktivitas Perusahaan.	2
Moderate	Risiko yang dampaknya menghambat sebagian jalannya bisnis dan aktivitas perusahaan	3
Major	Risiko yang menghambat seluruh proses bisnis dan aktivitas perusahaan	4
Catastrophic	Risiko yang dampaknya dapat menghentikan proses bisnis dan aktivitas perusahaan secara total.	5

Setelah menentukan likelihood dan impact, selanjutnya merupakan penilaian terhadap kemungkinan risiko yang akan muncul pada website Jakarta Notebook. Detail Nilai Risiko dengan Likelihood dan Impact dapat dilihat pada Tabel 6.

Tabel 6. Penilai Risiko Dengan Likelihood dan Impact

Kode Risiko	Kemungkinan Risiko	Likelihood	Impact
R1	Banjir	1	3
R2	Kebakaran	1	5
R3	Gempa Bumi	2	5
R4	Petir	2	1
R5	Listrik Padam	3	3
R6	Server Down	4	4
R7	Serangan Virus, Malware, Malicious Program	1	3
R8	Terputusnya koneksi jaringan	5	3
R9	Overload	4	2
R10	Bug pada website	5	3
R11	Data Corrupt	1	4
R12	Overhead	3	1
R13	Kurang memahami alur kerja system	4	1
R14	Human Error	4	3
R15	Pencurian data pada website	2	2

4.3.3 Tahap Evaluasi Risiko (Risk Evaluation)

Kemungkinan Risiko yang telah diidentifikasi dan di analisis kemudian dimasukkan dalam sebuah matrik evaluasi risiko yang ditentukan berdasarkan likelihood (kemungkinan) dan impact (dampak), Matrik risiko tersebut didapatkan dari parameter evaluasi risiko yang sudah ditentukan sebelumnya. Matrik risiko tersebut dapat dilihat pada tabel 7.

Tabel 7. Evaluasi Risiko

Likelihood	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
	Impact		1	2	3	4	5
		Insigficant	Minor	Moderate	Major	Catastrophic	

Setelah itu kemungkinan resiko-resiko yang sudah di tentukan nilai likelihood dan impact nya akan di masukan kedalam matrix evaluasi resiko disesuaikan dengan pemetaan pada tabel tersebut. Pada tabel. 8 dibawah ini merupakan hasil dari kemungkinan resiko-resiko yang sudah di masukan kedalam tabel matrix evaluasi resiko sesuai dengan kriteria likelihood dan kriteria impact yang sudah ditentukan pada tahap sebelumnya.

Tabel 8. Matrik Evaluasi Risiko Berdasarkan Kemungkinan (Likelihood) dan Dampak (Impact)

Likelihood	Certain	5			R8 R10		
	Likely	4	R13	R9	R14	R6	
	Possible	3	R12		R5		
	Unlikely	2	R4	R15			R3
	Rare	1			R1 R7	R11	R2
	Impact		1	2	3	4	5
		Insigficant	Minor	Moderate	Major	Catastrophic	

Selanjutnya merupakan hasil pengelompokan dari ke-15 kemungkinan-kemungkinan risiko yang akan terjadi pada website Jakarta Notebook. Kemungkinan tersebut diurutkan berdasarkan level yang paling tinggi (High), sedang (Medium) dan rendah (Low). Detail tingkatan risiko dapat dilihat pada Tabel 9

Tabel 9. Evaluasi Level Kemungkinan Risiko berdasarkan Likelihood dan Impact

Kode Risiko	Kemungkinan Risiko	Likelihood	Impact	Level Risiko
R1	Banjir	1	3	Low
R2	Kebakaran	1	5	Medium
R3	Gempa Bumi	2	5	Medium
R4	Petir	2	1	Low
R5	Listrik Padam	3	3	Medium
R6	Server Down	4	4	Medium
R7	Serangan Virus, Malware, Malicious Program	1	3	Low
R8	Terputusnya koneksi jaringan	5	3	High
R9	Overload	4	2	Medium
R10	Bug pada website	5	3	High
R11	Data Corrupt	1	4	Medium
R12	Overhead	3	1	Low
R13	Kurang memahami alur kerja system	4	1	Medium
R14	Human Error	4	3	Medium
R15	Pencurian data pada website	2	2	Low

4.4 Perlakuan Risiko (Risk Treatment)

Perlakuan Risiko merupakan upaya untuk mengurangi atau menghilangkan dampak dari kemungkinan risiko yang akan terjadi, yang dimana pada tahap ini akan diberikan usulan yang dapat digunakan dan

diterapkan guna meminimalisir kemungkinan risiko yang akan terjadi, sehingga dapat bermanfaat untuk kelancaran proses bisnis dari Perusahaan, risk treatment disusun berdasarkan level risiko yang sudah diidentifikasi sebelumnya, dari level risiko yang tinggi (high) ke level risiko yang rendah (low), detail usulan tersebut dapat dilihat pada tabel 10 berikut:

Tabel 10. Risk Treatment (Perlakuan Risiko)

Kode Risiko	Kemungkinan Risiko	Level Risiko	Perlakuan Risiko
R8	Terputusnya koneksi jaringan	High	Melapor kepada pihak penyedia layanan internet dan jika masih bermasalah setelah beberapa kali pelaporan, maka dapat mengganti ISP yang lebih baik.
R10	Bug pada website	High	Melakukan cek pada sistem, melakukan pengujian sistem secara berkala, ada Staff IT bagian customer service yang menangani masalah bug di system.
R2	Kebakaran	Medium	Meletakkan server di tempat yang lebih aman, menyediakan APAR di titik sekitar server.
R3	Gempa Bumi	Medium	Menyediakan server cadangan di tempat / lokasi lain yang lebih aman.
R5	Listrik Padam	Medium	Memasang Uninterruptible Power Supply (UPS) dan Generator Set dengan daya yang sesuai dengan kebutuhan perusahaan.
R6	Server Down	Medium	Melakukan pengecekan secara berkala pada sistem dalam satu hari, adanya backup plan (penerbitan polis secara offline, kemudian akan terupload otomatis jika sudah kembali online
R9	Overload	Medium	Melakukan refresh penggunaan db log, temp, dan RAM. Serta melakukan pengecekan terhadap database perusahaan.
R11	Data Corrupt	Medium	Melakukan backup data secara berskala
R13	Kurang memahami alur kerja system	Medium	Mempelajari alur kerja dan kegunaan sistem, mengadakan training mengenai penggunaan system.
R14	Human Error	Medium	Memberikan pelatihan untuk menanamkan ketelitian dan memberikan teguran lisan atau tulisan jika terlalu sering melakukan kesalahan.
R1	Banjir	Low	Menaruh server di tempat yang sulit dijangkau oleh banjir (di tempat yang lebih tinggi), Memiliki cadangan server di tempat yang berbeda.
R4	Petir	Low	Memasang alat penangkal petir, Melakukan pencadangan pada server utama secara otomatis ke dalam server cadangan

R17	Serangan Virus, Malware, Malicious Program	Low	Menyediakan antivirus, melakukan update dan monitoring software dan database antivirus.
R12	Overhead	Low	Memasang air conditioner di setiap ruangan supaya suhu tetap stabi
R15	Pencurian data pada website	Low	Melakukan reset password secara berkala. Memasang dan memantau CCTV di gedung perusahaan

V. Penutup Kesimpulan

Berdasarkan penelitian yang sudah dilakukan yang berdasar pada ISO 31000 pada system website di PT. Jakarta Notebook yang dilakukan menggunakan tahapan yang terdiri dari tahap identifikasi risiko (risk identification), analisis risiko (risk analys) dan evaluasi risiko (risk evaluation) serta tahap perlakuan risiko (risk tretment), maka dari penelitian tersebut di dapatkan 15 kemungkinan risiko dapat sewaktu-waktu bisa mengganggu kinerja Website maupun mengganggu proses bisnis yang terdapat di PT Jakarta Noteboo. Terdapat 2 kemungkinan risiko dengan tingkat high meliputi Terputusnya koneksi jaringan dan Bug pada website. Kemudian terdapat 8 kemungkinan risiko dengan tingkat Medium meliputi Kebakaran, Gempa Bumi, Listrik Padam, Server Down, Overload, Data Corrupt, Kurang memahami alur kerja system, dan Human Error. Kemudian juga terdapat 5 kemungkinan risiko dengan tingkat Low yang meliputi Banjir, Petir, Serangan Virus, Malware, Malicious Program, Overhead, dan Pencurian data pada website.

VI. DAFTAR PUSTAKA

- Al-Mhdawi, M. K. S., Qazi, A., Alzarrad, A., Dacre, N., Rahimian, F., Buniya, M. K., & Zhang, H. (2023). Expert Evaluation of ChatGPT Performance for Risk Management Process based on ISO 31000 Standard. *SSRN Electronic Journal, Esrel*, 1–6. <https://doi.org/10.2139/ssrn.4504409>
- Andika, D., & Wijaya, A. (2022). Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2018 Pada Pt. Trust Lerin vital Timur. *Jurnal Mnemonic*, 5(2), 111–118. <https://doi.org/10.36040/mnemonic.v5i2.4778>
- Andry, J. F., Liliana, L., Tannady, H., & Arief, A. S. (2022). Data Centre Risk Analysis Using ISO 31000:2009 Framework. *Journal of Physics: Conference Series*, 2394(1). <https://doi.org/10.1088/1742-6596/2394/1/012032>
- Asmarawati, S. G., & Pangeran, P. (2021). ISO 31000-Based Risk Management and Balanced Scorecard to Improve Company Performance: A Case Study at Indonsian YNK Tour and Travel Company. *International Journal of Multicultural and Multireligious Understanding*, 8(3), 376. <https://doi.org/10.18415/ijmmu.v8i3.2341>
- Ayuningtyas, M., & Tanaem, P. F. (2022). Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000. *Journal of Information Systems and Informatics*, 4(1), 92–105. <https://doi.org/10.51519/journalisi.v4i1.225>
- Citra Christian, H., & Sitokdana, M. N. N. (2022). *June25 th , 2 Satya Wacana*. 9(1). <http://jurnal.mdp.ac.id>
- Ecleas, J. (2021). Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 8(1), 209–224. <https://doi.org/10.35957/jatisi.v8i1.601>
- Harefa, W. (2022). Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 9(1), 407–420. <https://doi.org/10.35957/jatisi.v9i1.1478>
- 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. <https://doi.org/10.33557/binakomputer.v2i1.792>
- Mahardika, K. B., Wijaya, A. F., & Cahyono, A. D. (2019). Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000: 2018 (Studi Kasus: Cv. Xy). *Sebatik*, 23(1), 277–284. <https://doi.org/10.46984/sebatik.v23i1.572>
- Miftakhatun, M. (2020). Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000. *Journal of Computer Science and Engineering (JCSE)*, 1(2), 128–146. <https://doi.org/10.36596/jcse.v1i2.76>
- Natalie, D. P., & Manuputty, A. D. (2022). Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk. *JURIKOM (Jurnal Riset Komputer)*, 9(5), 1290. <https://doi.org/10.30865/jurikom.v9i5.4797>
- Nugraha, U. (2017). Design of information systems for population data collection based on client-server at Bagolo village. *AIP Conference Proceedings*, 1855(June 2017). <https://doi.org/10.1063/1.4985526>
- Nugroho, R. L., & Pangeran, P. (2021). Improving the Performance of the Balanced Scorecard Through Implementing Iso 31000 Risk Assessment At Shofa Pharmacy. *EUREKA: Social and Humanities*, 1, 23–36. <https://doi.org/10.21303/2504-5571.2021.001635>
- Pangestu, R. H., Cahyono, A. D., & Tanaem, P. F. (2021). Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Menggunakan ISO 31000. *Journal of Computer and Information Systems Ampera*, 2(1), 43–57. <https://doi.org/10.51519/journalcisa.v2i1.59>
- Prabowo, D., & Wijaya, A. F. (2022). Risk Management Analysis on KKM LKF FTI UKSW Website Using ISO 31000 Framework. *Journal of Information Systems and Informatics*, 4(1), 65–76. <https://doi.org/10.51519/journalisi.v4i1.219>
- Pradana, M. F., Raharjanti, R., Murtini, S., & Ardiansah, M. N. (2022). Framework ITIL V3: Analisis Tingkat Kematangan Manajemen Insiden pada Perusahaan Ekspedisi. *Jutisi : Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, 11(2). <https://doi.org/10.35889/jutisi.v11i2.916>
- Putra, L. F., & Profita, A. (2022). Analisis Risiko Website Telkom Emas Data Validation Menggunakan Iso 31000. *PROFISIENSI: Jurnal Program Studi Teknik Industri*, 10(2), 175–183. <https://doi.org/10.33373/profis.v10i2.4725>
- Rahardian, T. F., & Wijaya, A. F. (2022). Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000. *Journal of Information Systems and Informatics*, 4(2), 442. <http://journal-isi.org/index.php/isi>
- Rahmawati, A., & Wijaya, A. F. (2019). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP. *Jurnal SITECH: Sistem Informasi Dan Teknologi*, 2(1), 13–20. <https://doi.org/10.24176/sitech.v2i1.3122>
- Sanjaya, I. G. A. S., Sasmita, G. M. A., & Sri Arsa, D. M. (2020). Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city). *International Journal of Computer Network and Information Security*, 12(4), 30–40. <https://doi.org/10.5815/ijenis.2020.04.03>
- Soumeru, L., Rahardja, Y., & Wijaya, A. F. (2016). Analisis Manajemen Layanan Teknologi Informasi Menggunakan Framework ITIL V3 Domain Service Operation (Studi Kasus: PT Telekomunikasi Indonesia, Tbk. Semarang). *Artikel Ilmiah Universitas Kristen Satya Wacana*.
- 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. <https://doi.org/10.46984/sebatik.v25i2.1430>
- Wicaksono, A. Y. (2020). Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division. *International Journal of Science, Engineering, and Information Technology*, 4(2), 198–202. <https://doi.org/10.21107/ijseit.v4i2.6871>
- Yefany Syahputri, H., & Kitri, M. L. (2020). Enterprise Risk Management Analysis of Group XYZ Based

on ISO 31000:2018 Framework. *Asian Journal of Accounting and Finance*, 2(3), 1–12.
<http://myjms.moe.gov.my/index.php/ajafin>