Journal of Computer and Information Systems Ampera
Vol. 2, No. 2, May 2021 e-ISSN: 2775-2496
https://journal-computing.org/index.php/journal-cisa/index

Analisis Resiko Aplikasi Sistem Informasi Pengelolaan Data Umat Menggunakan ISO 31000 (Studi Kasus: Gereja Katolik Santo Paulus Miki Salatiga)

Diane Junianti[1], Charitas Fibriani[2]

[1] Sistem Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia.
Email: [1]682017405@student.ulsw.edu, [2]charitas.fibriani@uksw.edu.

Abstract

The People's Data Management Information System is an information system that manages people's data from the diocese, parish, regional, to environmental levels. This application is used to input data, update data, and delete data, the application of the Ummah Data Management Information System has risks that will hinder the application, such as unstable internet connections, the latest data and the readiness of human resources who operate the system. The purpose of the research is to minimize the possibility of risk, so ISO 31000 is used to determine the impact of risk, the level of risk, and the treatment of risk needed in a company or organization in conducting the analysis. It is hoped that the existence of ISO 31000 can overcome the risks that will occur now and in the future.

Keywords: NIST, Risk Assessment, Risk Management.

1. PENDAHULUAN

Pada masa modern ini berkembangnya Teknologi yang sangat pesat membuat hampir seluruh aspek bergantung kepada teknologi, seperti: media sosial, internetan. Internet sangat membantu dalam menjalankan tugas dan tanggungjawab terutama dalam menggembangkan sebuah organisasi atau perusahaan terutama di Gereja Katolik Santo Paulus Miki Salatiga [1]. Gereja Santo Paulus Miki Salatiga merupakan organisasi yang berkembang dalam bidang keagamaan, aplikasi Sistem Informasi Pengelolaan Data Umat merupakan bagian dari Sistem Pendataan Umat

Keuskupan Agung Semarang (KAS) yang dikembangkan sejak awal tahun 2020 oleh Tim IT KAS untuk mengelola data umat mulai dari Keuskupan, Paroki, Wilayah, sampai ke tingkat Lingkungan. Adanya aplikasi ini dapat membantu dalam mengumpulkan berbagai berkas terkait dengan pelayanan gereja mulai dari *input* data, *update* data dan *delete* data serta yang berhubungan dengan pendataan umat.

Manajemen risiko merupakan proses identifikasi untuk mengukur seluruh resiko dalam mengelola bisnis atau proyek sehingga dalam menghasilkan sebuah keputusan agar tercapainya sebuah sasaran dalam menjalankan proses bisnis, ada beberapa tahap dari manajemen risiko yaitu identifikasi resiko, analisis, dan penilaian resiko [2]. Pada tahap manajemen resiko diperlukannya pengelolaan informasi terkait dengan kepercayaan antar pihak manajemen dengan karyawan, kepercayaan merupakan elemen yang penting dalam membangun sebuah keamanan informasi di dalam lingkup teknologi informasi dengan begitu mempermudah dalam menerapkan perilaku keamanan informasi didalam perusahaan atau organisasi [3].

Alasan dari penerapan aplikasi Sistem Informasi Pengelolaan Data Umat dilakukan karena kebutuhan umat yang semakin meningkat setiap tahunnya dan tidak menutup kemungkinan dapat menyebabkan proses bisnis terganggu atau terhenti, ini salah satu cara proses bisnis berjalan dengan lancar adalah melalui ISO 31000 agar dapat memahami resiko saat ini dan kemungkinan resiko di masa depan. Kemungkinan resiko mengakibatkan terganggu atau berhentinya suatu proses bisnis, membuat cara agar proses bisnis dapat berjalan dengan lancar adalah melalui ISO 31000 untuk dapat melihat kemungkinan resiko apa saja yang akan terjadi saat ini dan yang akan datang. Mengatasi permasalahan maka dilakukannya analisis dampak resiko, level resiko, dan perlakuan terhadap risiko digunakannya metode ISO 31000 karena sesuai dengan kebutuhan yang diperlukan didalam organisasi atau perusahaan saat ini dan yang akan datang. Penelitian terdahulu tentang "Analisis teknologi informasi menggunakan ISO 31000" yang dilakukan tahun 2020, aplikasi yang digunakan berfungsi untuk mencatat buku pinjaman, daftar buku yang tersedia, jumlah buku, jatuh tempo peminjaman dan daftar peminjaman. Nama dari aplikasinya adalah SINTESA, dimana menghasilkan 18 kemungkinan resiko yang akan mengganggu kinerja dari aplikasi SINTESA yang telah diteliti [4].

Pada tahun 2019 penelitian dilakukan di PT Serasa Autoraya tentang "analisis resiko SAP menggunakan *Framework* ISO 31000", menghasilkan 15 kemungkinan resiko yang menghambat terjadinya aplikasi. Hasil dari penelitian dapat membantu dalam menyusun dokumentasi terkait dengan manajemen resiko, kemungkinan terbesar dari hasil penelitian ada dua yaitu listrik dan koneksi internet yang sangat mengganggu aktivitas pada suatu perusahaan [5]. Penelitian tentang "analisis resiko website SWIFTS" pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) tahun 2017 yang menggunakan *Framework* 31000", tujuan dilakukannya penelitian adalah mengelola sebuah kemungkinan resiko untuk menghasilkan sebuah resiko secara optimal dengan melakukan pencegahan, penanganan, pemeliharaan terhadap aset pendukung dan hasil dari penelitian kemungkinan resiko tersebut menghasilkan 34 kemungkinan resiko [6].

Penelitian terdahulu tentang "Analisis resiko aplikasi teknologi informasi aplikasi Vcare pada PT Visionet Data Internasional menggunakan ISO 31000 tahun 2020, aplikasi Vcare berfungsi untuk pendaftaran layanan pengadaan mesin dan pedagang, kontrak layanan, mengelola service, dan penarikan mesin EDC (*Electronic Data Capture*), hasil dari penelitian tersebut menghasilkan 20 kemungkinan resiko yang dapat mengganggu berjalannya sebuah aplikasi Vcare [7]. ISO 31000 digunakan untuk mengidentifikasi peluang, ancaman, dan efektif dalam menganalisis kemungkinan resiko. Menerapkan prinsip pada kerangka kerja ISO 31000 dan mewujudkan manajemen tata kelola serta evaluasi kesiapan dari prinsip ISO 31000 bagi perusahaan atau organisasi [8].
Analisis manajemen risiko menggunakan ISO 31000 adalah mengelola risiko secara keseluruhan terutama pada pencegahan, penanganan serta perbaikan manajemen risiko yang telah diterapkan. Menyiapkan secara jelas teknis yang dilakukan agar terarah dan efektif dalam menjalankan proses bisnis [9].

Edisi pertama pedoman manajemen risiko ISO 31000 diterbitkan oleh Organisasi Internasional untuk Standardisasi tahun 2009 adalah *framework* yang mendasarkan manajemen melalui *framework*, konsep dan *terminologi*. Setelah itu dibuatnya pembaharuan dikarenakan tidak adanya sertifikasi di tahun 2009, sekarang menjadi versi ISO 31000: 2018, versi ini menyajikan visi yang lebih lengkap dan strategis untuk manajer, menentukan prinsip-prinsip dan metodologi yang digunakan lebih akurat sehingga dapat melindungi nilai institusi [10]. Harus adanya kerjasama

untuk bisa menjalankan kerangka kerja yang telah diterapkan pada ISO 31000 yang melibatkan penerapan sistematis kebijakan, prosedur, kegiatan komunikasi, konsultasi, evaluasi, perlakuan, pemantauan, dan analisis. Kerangka kerja dari ISO 31000 membantu dalam mengambil keputusan dan pencapaian dalam mencapai tujuan yang telah direncanakan [11].

2. METODE

Framework ISO atau *International Organization for Standardization* (ISO) 31000, merupakan standar internasional yang menerapkan manajemen risiko. Tujuan dari *framework ISO* adalah untuk memberikan pedoman dan prinsip-prinsip manajemen risiko yang diakui oleh dunia. Pada gambar 1, menjelaskan kerangka kerja dari manajemen resiko. Berdasarkan *International organization for Standardization* (ISO 3100:2018), sebelum melakukan tahap 1 dan 2 tentukan dulu ruang lingkup, konteks dan kriteria manajemen. Terdapat 2 tahap pencarian informasi yaitu *Risk Assessment* (Penilaian Resiko) dan *Risk Treatment* (Perlakuan Risiko) [12].

Tahap pertama *Risk Assessment* ada 3 tahap: *Risk Identifikasi* (Identifikasi Resiko) adalah usaha untuk mengetahui resiko-resiko yang akan timbul didalam keberlangsungannya perusahaan atau organisasi, *Risk Analysis* (Analisis Resiko) adalah mengetahui level resiko yang akan mengancam aset dan membangun strategi perusahaan atau organisasi dan *Risk Evaluasi* (Evaluasi Resiko) adalah membantu dalam pengambilan keputusan berdasarkan hasil analisis resiko serta memperbaiki kesalahan yang telah dilakukan sebelumnya[13].

Tahap kedua *Risk Treatment* (Perlakuan Risiko) adalah proses merubah risiko untuk menanggulangi kemungkinan resiko yang akan terjadi. Pada tahap 1 harus adanya komunikasi serta konsultasi terkait dengan analisis yang dilakukan selanjutnya tahap 2 memantau secara rutin kinerja dalam menganalisis serta langka apa saja yang dilakukan agar dapat berjalan dengan lancar proses bisnisnya, setelah dilakukannya semua tahap proses terakhir adalah perekaman dan pelaporan hasil analisis yang dilakukan [14].

Data yang didapatkan melalui salah satu staf yang mengelola IT di Paroki Santo Paulus Miki Salatiga, jenis data yang digunakan adalah kuantitatif,

yang pertama melalui proses wawancara dari narasumber melalui via whatsapp dalam tahap wawancara membuat pertanyaan dalam word dikirim kepada narasumber dan dikirim kembali isi dari pertanyaan yang telah dibuat, tahap kedua adalah mengelola hasil dari wawancara untuk dijadikan sebuah analisis dengan mengikuti kerangka kerja dari ISO 31000:2018 [15].

3. HASIL DAN PEMBAHASAN

Pada tahap penilaian resiko Aplikasi Sistem Informasi Pengelolaan Data Umat dengan menggunakan analisis manajemen risiko 31000, ada 3 tahap yaitu: Identifikasi resiko, analisis resiko, dan evaluasi resiko. Tahap pertama yang dilakukan pada tahap penilaian risiko adalah identifikasi aset yang berhubungan dengan aplikasi Pendataan Umat Paroki Santo Paulus Miki Salatiga. Dengan melakukan wawancara dengan salah seorang staf IT pada aplikasi ini, proses identifikasi asset yaitu: Data, *Software* dan *Hardware* yang berhubungan dengan aplikasi.

Tabel 1. Identifikasi Aset Aplikasi Sistem Informasi Pengelolaan Data Umat

Komponen Sistem Informasi	Aset Aplikasi Sistem Informasi Pengelolaan Data Umat
Data	Data Umat, Data User
Software	Aplikasi Sistem Informasi Pengelolaan Data Umat
Hardware	*Personal Computer, Server Database*

Tabel 1 menjelaskan bahwa identifikasi aset aplikasi Pendataan Umat Paroki Santo Paulus Miki Salatiga menghasilkan Data, yang memiliki 2 aset yaitu Data Umat yang dikelompokan yaitu: nama, jenis kelamin, agama, pekerjaan, wilayah gereja, lingkungan gereja, NIK dan KK, Data User yaitu: nama lengkap dari data yang diinginkan. *Software* berbentuk Aplikasi Sistem Informasi Pengelolaan Data Umat dan hardware ada 2 aset yang pertama Personal computer yaitu: layar, keyboard, dan touchpad dan yang kedua Server database yaitu: mysql. Selanjutnya akan dilakukannya identifikasi kemungkinan-kemungkinan resiko yang akan menghambat

berjalanya aplikasi Pendataan Umat Paroki Santo Paulus Miki Salatiga. Terdapat 3 faktor yaitu: faktor Alam/Lingkungan, Manusia dan Sistem Infrastruktur yang menghambat berjalannya aplikasi Pendataan Umat Paroki Santo Paulus Miki Salatiga. Dapat dilihat pada tabel 2 Identifikasi kemungkinan resiko.

Tabel 2. Identifikasi Kemungkinan Resiko

Faktor	ID	Kemungkinan Resiko
Alam/Lingkungan	RE01	Petir
	RE02	Banjir
	RE03	Kebakaran
	RE04	Gempa bumi
Manusia	RE05	Penyalahgunaan hak akses
	RE06	Perubahan data umat
	RE07	*User interface* aplikasi yang sulit dipahami
	RE08	*Cybercrime*
	RE09	Pencurian perangkat/data
Sistem dan Infrastruktur	RE10	*Overload*
	RE11	*Overheat*
	RE12	Koneksi jaringan tidak stabil
	RE13	
	RE14	Koneksi jaringan terputus
	RE15	*Data corrupt*
	RE16	*Backup failure*
		Kerusakan hardware

Tabel 2 menjelaskan tahap identifikasi resiko, ditemukan ada 16 kemungkinan-kemungkinan resiko yang berasal dari faktor alam/lingkungan yaitu: RE01 ada Petir, RE02 ada Banjir, RE03 ada Kebakaran, dan RE04 ada Gempa bumi. Yang berasal dari Manusia yaitu: RE05 ada Penyalahgunaan hak akses, RE06 ada Perubahan data umat, RE07 ada *User interface* aplikasi yang sulit dipahami, RE08 ada *Cybercrime*, RE09 ada Pencurian perangkat/data serta sistem dan infrastruktur yaitu: RE10 ada *Overload*, RE11 ada *Overheat*, RE12 ada Koneksi jaringan yang tidak stabil, RE13 ada Koneksi jaringan terputus, RE14 ada *Data corrupt*, RE15 ada *Backup failure* dan RE16 ada *Kerusakan hardware*. Yang

menghambat Aplikasi Sistem Informasi Pengelolaan Data Umat Di Paroki Santo Paulus Miki Salatiga. Setelah mengetahui kemungkinan resiko dilakukan juga identifikasi dampak resikonya, dapat dilihat pada tabel Identifikasi dampak risiko.

Tabel 3. Identifikasi Dampak Risiko.

ID	Kemungkinan Resiko	Dampak
RE01	Petir	Kerusakan infrastruktur perusahaan
RE02	Banjir	Menghambat aktivitas bisnis perusahaan
RE03	Kebakaran	Kerusakan infrastruktur dan aktivitas perusahaan terhenti
RE04	Gempa Bumi	Aktivitas terhenti dan kerusakan infrastruktur perusahaan
RE05	Penyalahgunaan hak akses	Data user di salah gunakan
RE06	Perubahan data umat	Sulit mencari data yang diinginkan
RE07	*User interface* aplikasi yang sulit dipahami	User sulit mengerti cara penggunaan aplikasi
RE08	*Cybercrime*	Bocornya data/informasi gereja
RE09	Pencurian perangkat/data	Perusahaan akan mengalami kerugian
RE10	*Overload*	Jika database penuh maka akan berhenti secara tiba-tiba
RE11	*Overheat*	Hardware tidak dapat digunakan dan tidak bekerja secara optimal jika suhunya mengalami panas secara terus menerus

RE12	Koneksi jaringan tidak stabil	Menghambat akses aplikasi Pendataan Umat Paroki Santo Paulus Miki Salatiga
RE13	Koneksi jaringan terputus	Gagal melakukan update pada aplikasi Pendataan Umat Paroki Santo Paulus Miki Salatiga
RE14	*Data corrupt*	Perusahaan tidak mendapatkan data yang valid
RE15	*Backup failure*	Data yang diterima tidak akan lengkap
RE16	*Kerusakan Hardware*	Aktivitas perusahaan akan terhambat dan harus memindahkan data ke hardware yang baru

Tabel 3 menjelaskan tentang Identifikasi Dampak Risiko pada kemungkinan resikonya yaitu: Petir mengakibatkan kerusakan infrastruktur seperti bangunan rusak dan listrik yang mati atau konslet, banjir menyebabkan aktivitas bisnis perusahaan terhenti, kebakaran mengakibatkan kerusakan infrastruktur dan aktivitas perusahaan terhenti seperti gedung terbakar sehingga harus dilakukan perhentian kerja untuk sementara sampai ada kebijakan dari perusahaan atau organisasi, gempa bumi menyebabkan aktivitas terhenti dan kerusakan infrastruktur perusahaan seperti tidak ada jam kerja sampai ada kebijakan dari perusahaan dan gedung rusak, penyalahgunaan hak akses mengakibatkan data user disalah gunakan seperti digunakan untuk mencari keuntungan personal, perubahan data umat menyebabkan sulit mencari data yang diinginkan seperti nama, jenis kelamin, agama, pekerjaan, wilayah gereja, lingkungan gereja, NIK dan KK, *user interface* aplikasi yang sulit dipahami mengakibatkan user sulit mengerti cara penggunaan aplikasi seperti tidak adanya pelatihan dalam penggunaan aplikasi dan desain dari *user interface* yang tidak bisa dibaca oleh user.

Cybercrime menyebabkan bocornya data/informasi gereja seperti identitas umat, pencurian perangkat/data mengakibatkan perusahaan

akan mengalami kerugian seperti bocornya identitas, overload akan berdampak sangat fatal jika database penuh maka akan berhenti secara tiba-tiba sehingga terhambatnya proses bisnis perusahaan atau organisasi, overheat menyebabkan hardware tidak dapat digunakan dan tidak bekerja secara optimal jika suhunya mengalami panas secara terus menerus, koneksi jaringan tidak stabil akan menghambat akses aplikasi Sistem Informasi Pengelolaan Data Umat, koneksi jaringan terputus mengakibatkan gagal melakukan pembaruan pada aplikasi Sistem Informasi Pengelolaan Data Umat, data corrupt menyebabkan perusahaan tidak mendapatkan data yang lengkap sehingga menghambat berjalannya proses bisnis perusahaan atau organisasi, backup failure menyebabkan data yang diterima tidak lengkap akan mengakibatkan terhambatnya proses bisnis, dan kerusakan hardware mengakibatkan aktivitas perusahaan akan terhambat dan harus memindahkan data ke hardware yang baru sehingga membutuhkan waktu untuk bisa memindahkan data. Serta dampak yang dilakukan, selanjutnya tahap analisis resiko.

Setelah melakukan proses identifikasi, selanjutnya adalah proses analisis resiko. Pada tahap ini dilakukannya penilaian terhadap kemungkinan-kemungkinan resiko yang sudah di identifikasi pada proses sebelumnya dengan menggunakan tabel kriteria likelihood dan kriteria impact sebagai acuan untuk melakukan proses analisis resiko. Dapat dilihat pada tabel *Likelihood*.

Tabel 4. Likelihood

Likelihood			
Nilai	**Kriteria**	**Deskripsi**	**Frekuensi kejadian**
1	*Rare*	Resiko tersebut hampir tidak pernah terjadi	>2tahun
2	*Unlikely*	Resiko tersebut jarang terjadi	1-2 tahun
3	*Possible*	Resiko tersebut kadang terjadi	7-12 bulan
4	*Likely*	Resiko tersebut sering terjadi	4-6 bulan

5	*Certain*	Resiko tersebut pasti terjadi	1-3 bulan

Tabel 4 pada likelihood terdapat 5 kriteria berdasarkan kemungkinan resiko yang terjadi yaitu *Rare* merupakan resiko tersebut hampir tidak pernah terjadi lebih dari 2 tahun, *Unlikely* merupakan resiko yang jarang terjadi selama 1 sampai 2 tahun, *Possible* merupakan resiko yang kadang terjadi selama 7 sampai 12 bulan, *Likely* merupakan resiko yang sering terjadi selama 4 sampai 6 bulan, dan *Certain* merupakan resiko yang pasti terjadi selama 1 sampai 3 bulan.
Kriteria *Impact* merupakan tabel penilaian impact atau dampak yang akan terjadi jika kemungkinan-kemungkinan resiko terjadi di perusahaan. Pada Kriteria *Impact* terdapat 5 kriteria yang akan terjadi. Kriteria tersebut dibagi berdasarkan dampak yang tidak berpengaruh dan dampak yang paling berpengaruh dalam berjalannya proses bisnis perusahaan. Setelah kemungkinan resiko di identifikasi, selanjutnya adalah proses memasukan ke table impact sesuai dengan kriteria yang sudah ditentukan. Dapat dilihat pada tabel kriteria *impact*.

Tabel 5. Kriteria Impact

Impect

Nilai	Kriteria	Keterangan
1	*Insignificant*	Tidak mengganggu aktivitas gereja
2	*Minor*	Tidak menghambat dan mengganggu aktivitas gereja
3	*Moderate*	Mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja
4	*Major*	Hampir menghambat seluruh jalannya aktivitas gereja
5	*Catastrophic*	Mengakibatkan aktivitas terhenti karena proses

	bisnis mengalami gangguan total

Pada tabel 5 kriteria impact terdapat 5 kriteria yaitu Insignificant tidak mengganggu aktivitas gereja seperti beribadah, *Minor* tidak menghambat dan mengganggu aktivitas gereja seperti aktif dalam pelayanan gereja. *Moderate* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja seperti buat keributan di dalam gereja, *Major* hampir menghambat seluruh jalannya aktivitas gereja pemadaman listrik pada saat misa berlangsung, dan *Catastrophic* mengakibatkan aktivitas terhenti karena proses bisnis mengalami gangguan total seperti kegiatan yang berbau teroris (pengeboman) dan bencana alam (gempa bumi).

Setelah mendapatkan nilai kemungkinan *likelihood* dan dampak *impact* yang sudah ditentukan, maka selanjutnya akan dilakukan penilai terhadap kemungkinan-kemungkinan resiko yang ada pada aset terkait aplikasi Sistem Informasi Pengelolaan Data Umat yang sudah di identifikasi pada proses sebelumnya. Penilaian kemungkinan-kemungkinan resiko, dapat dilihat pada tabel penilaian kemungkinan risiko *likelihood* dan *impact.*

Tabel 6. Penilaian Kemungkinan Resiko Likelihood dan Impact

ID	Kemungkinan Resiko	*Likelihood*	*Impect*
RE01	Petir	1	2
RE02	Banjir	2	3
RE03	Kebakaran	1	5
RE04	Gempa bumi	1	5
RE05	Penyalahgunaan hak akses	2	1
RE06	Perubahan data umat	4	1
RE07	User interface aplikasi yang sulit dipahami	1	1
RE08	Cybercrime	2	2
RE09	Pencurian perangkat data	2	2
RE10	*Overload*	3	3
RE11	*Overheat*	3	3
RE12	Koneksi jaringan tidak stabil	3	3
RE13	Koneksi jaringan terputus	3	4
RE14	*Data corrupt*	1	2

RE15	*Backup failure*	1	1
RE16	*Kerusakan hardware*	3	2

Pada tabel 6 menunjukan setelah dimasukkannya 16 kemungkinan resiko yaitu: RE01 Petir didalamnya terdapat *likelihood* merupakan resiko tersebut hampir tidak pernah terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja, RE02 Banjir didalamnya terdapat *likelihood* merupakan resiko tersebut jarang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, RE03 Kebakaran didalamnya terdapat *likelihood* merupakan resiko tersebut hampir tidak pernah terjadi dan *impact* mengakibatkan aktivitas terhenti karena proses bisnis mengalami gangguan total, RE04 Gempa bumi di dalamnya terdapat *likelihood* resiko tersebut hampir tidak pernah terjadi dan *impact* mengakibatkan aktivitas terhenti karena proses bisnis mengalami gangguan total, RE05 Penyalahgunaan hak akses didalamnya terdapat *likelihood* merupakan resiko tersebut jarang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja, RE06 Perubahan data umat didalamnya terdapat *likelihood* resiko tersebut sering terjadi dan *impact* tidak mengganggu aktivitas gereja, RE07 *User interface* aplikasi yang sulit dipahami didalamnya terdapat *likelihood* merupakan resiko tersebut hampir tidak pernah terjadi dan impact tidak mengganggu aktivitas gereja, RE08 *Cybercrime* didalamnya terdapat *likelihood* merupakan resiko tersebut jarang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja.

RE09 Pencurian perangkat data didalamnya terdapat *likelihood* merupakan resiko tersebut jarang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja, RE10 *Overload* didalamnya terdapat *likelihood* merupakan resiko tersebut kadang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, RE11 *Overheat* didalamnya terdapat *likelihood* merupakan resiko tersebut kadang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, RE12 Koneksi jaringan tidak stabil didalamnya terdapat *likelihood* merupakan resiko tersebut kadang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, RE13 Koneksi jaringan terputus didalamnya terdapat *likelihood* merupakan resiko tersebut kadang terjadi dan *impact* hampir menghambat seluruh jalannya aktivitas gereja, RE14 *Data corrupt* didalamnya terdapat *likelihood* merupakan resiko tersebut hampir tidak pernah terjadi dan *impact* tidak

menghambat dan mengganggu aktivitas gereja, RE15 *Backup failure* didalamnya terdapat *likelihood* merupakan resiko tersebut hampir tidak pernah terjadi dan *impact* tidak mengganggu aktivitas gereja, dan RE16 *Kerusakan hardware* didalamnya terdapat *likelihood* merupakan resiko tersebut kadang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja.

Penilaian kemungkinan risiko *likelihood* dan *impact* sudah ditentukan level dari masing-masing kemungkinan resikonya mulai dari level 1 sampai level 5 selanjutnya dilakukan tahap evaluasi risiko. Pada tahap evaluasi resiko dari kemungkinan-kemungkinan resiko yang sudah dianalisis pada tahap sebelumnya, hasil dari identifikasi dimasuk ke dalam matrix evaluasi resiko berdasarkan kerangka kerja ISO 31000. Matix evaluasi resiko dibagi menjadi 3 berdasarkan level resiko (*risk level*) yaitu: *low, medium, dan high*. Kemungkinan resiko dari nilai *likelihood* dan nilai *impact* pada proses sebelumnya akan disesuaikan dengan matrix yang ada. Untuk melihat hasil penilaian dari *likelihood* dan *impact*, dapat dilihat pada Matrix Evaluasi Resiko berikut ini.

Table 7. Matrix Evaluasi Resiko

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*
			1	2	3	4	5
	Impect		*Insignificant*	*Minor*	*Moderate*	*Major*	*Catastrophic*

Tabel 7 menjelaskan tahap Matrik evaluasi resiko mulai dari *likelihood* ada 5 yaitu: *Certain* didalamnya terdapat *likelihood*, resiko tersebut sering terjadi dan evaluasi matriksnya masuk kategori sedang, *likely* didalamnya terdapat *likelihood*, resiko tersebut sering terjadi dan evaluasi matriksnya masuk kategori sedang, *possible* didalamnya terdapat *likelihood* resiko tersebut kadang terjadi dan evaluasi matriksnya masuk kategori rendah , *unlikely* didalamnya terdapat *likelihood* resiko tersebut jarang terjadi dan evaluasi matriksnya masuk kategori rendah, rare didalamnya terdapat *likelihood* resiko tersebut hamper tidak pernah terjadi dan evaluasi matriksnya masuk kategori rendah. Selanjutnya dari *impact* kita akan menentukan mulai dari 1 sama dengan *Insignificant* tidak mengganggu

aktivitas gereja, 2 sama dengan *Minor* yaitu tidak menghambat dan mengganggu aktivitas gereja, 3 sama dengan *Moderate* yaitu mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, 4 sama dengan *Major* yaitu hampir menghambat seluruh jalannya aktivitas gereja, 5 sama dengan *Catastrophic* yaitu mengakibatkan aktivitas terhenti karena proses bisnis mengalami gangguan total. Setelah dilakukannya matrix evaluasi risiko berdasarkan identitas yang dimiliki oleh kemungkinan resikonya dan dimasukan pada matrix evaluasi sesuai dengan kriteria *Likelihood* and *Impact*.

Tabel 8. Matrix Evaluasi Resiko Berdasarkan *Likelihood dan Impact*

Likelihood	*Certain*	5			RE12 RE13		
	Likely	4		RE07 RE06 RE10			
	Possible	3	RE11	RE16			RE04
	Unlikely	2		RE01 RE05 RE08 RE09			
	Rare	1	RE15	RE14	RE02		RE03
	Impect		1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

Tabel 8 menjelaskan bahwa setelah kemungkinan-kemungkinan resiko dimasukan kedalam matrik evaluasi berdasarkan *likelihood* dan *impact*, maka dibuat Level Risiko Berdasarkan Kemungkinan Resiko dikelompokkan menjadi 16 kemungkinan resiko dimasukan kedalam masing-masing level risiko dengan tingkat *high, medium, dan low*. Pada tingkat *high* ada RE12 ada koneksi jaringan tidak stabil, RE13 ada koneksi jaringan terputus, RE04 ada gempa bumi, tingkat medium ada RE07 *ada user interface* aplikasi yang sulit dipahami, RE06 ada perubahan data umat, RE16 ada *kerusakan hardware*, RE03 ada kebakaran, dan tingkat *low* ada RE11 ada *overheat*, RE01 ada petir, RE05 ada penyalahgunaan hak akses, RE08 ada *cybercrime*, RE09 ada pencurian perangkat data, RE14 ada *data corrupt*, RE15 ada *backup failure*, dan RE02 ada banjir. Untuk melihat level

risiko berdasarkan kemungkinan resikonya dapat dilihat pada tabel level risiko berdasarkan kemungkinan.

Tabel 9. Level Risiko Berdasarkan Kemungkinan Resiko

ID	Kemungkinan Resiko	*Likelihood*	*Impact*	*Risk Level*
RE12	Koneksi jaringan terputus	3	4	*High*
RE13	Koneksi jaringan tidak stabil	3	3	*High*
RE04	Gempa Bumi	1	5	*High*
RE07	*User interface* aplikasi yang sulit dipahami	1	1	*Medium*
RE10	*Overload*	3	3	*Medium*
RE03	Kebakaran	1	5	*Medium*
RE16	*Kerusakan hardware*	3	2	*Medium*
RE01	Petir	1	2	*Low*
RE02	Banjir	2	3	*Low*
RE09	Pencurian perangkat data	2	2	*Low*
RE08	*Cybercrime*	2	2	*Low*
RE11	*Overheat*	3	3	*Low*
RE05	Penyalahgunaan hak akses	2	1	*Low*
RE15	*Backup failure*	1	1	*Low*
RE06	Perubahan data umat	4	1	*Low*
RE14	*Data corrupt*	1	2	*Low*

Tabel 9 menghasilkan evaluasi resiko dapat dilihat pada Level Risiko Berdasarkan Kemungkinan Resiko, terdapat 16 kemungkinan resiko yang sudah dianalisis berdasarkan tingkat level resikonya. Terdapat 3 kemungkinan resiko yang masuk kedalam *level of risk tingkat high* yaitu Koneksi jaringan terputus untuk *likelihood* resiko tersebut kadang terjadi dan *impact* hampir menghambat seluruh jalannya aktivitas gereja, Koneksi jaringan tidak stabil untuk *likelihood* resiko tersebut kadang terjadi dan

impact mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, dan Gempa Bumi untuk *likelihood* resiko tersebut hampir tidak pernah terjadi dan impactnya mengakibatkan aktivitas terhenti karena proses bisnis mengalami gangguan total.

Terdapat 4 kemungkinan resiko yang masuk ke dalam *level of risk tingkat medium* yaitu *User interface* aplikasi yang sulit dipahami untuk *likelihood* resiko tersebut hampir tidak pernah terjadi dan *impact* tidak mengganggu aktivitas gereja, *Overload* untuk *likelihood* resiko tersebut kadang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, kebakaran untuk *likelihood* resiko tersebut hampir tidak pernah terjadi dan *impact* mengakibatkan aktivitas terhenti karena proses bisnis mengalami gangguan total, dan *kerusakan hardware* untuk *likelihood* resiko tersebut kadang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja. Serta terdapat 9 kemungkinan resiko yang masuk ke dalam *level of risk tingkat low* yaitu Petir untuk *likelihood* resiko tersebut hampir tidak pernah terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja, Banjir untuk *likelihood* resiko tersebut jarang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja.

Pencurian perangkat data untuk *likelihood* resiko tersebut jarang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja, *Cybercrime* untuk *likelihood* resiko tersebut jarang terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja, *Overheat* untuk *likelihood* resiko tersebut kadang terjadi dan *impact* mengganggu proses bisnis sehingga mengakibatkan terhambatnya aktivitas gereja, Penyalahgunaan hak akses untuk *likelihood* resiko tersebut jarang terjadi dan *impact* tidak mengganggu aktivitas gereja, *Backup failure* untuk *likelihood* resiko tersebut hampir tidak pernah terjadi dan *impact* tidak mengganggu aktivitas gereja , Perubahan data umat untuk *likelihood* resiko tersebut sering terjadi dan *impact* tidak mengganggu aktivitas gereja, dan *Data corrupt* untuk *likelihood* resiko tersebut hampir tidak pernah terjadi dan *impact* tidak menghambat dan mengganggu aktivitas gereja. Dari hasil analisis yang dilakukan dapat dilihat dari *level of risk tingkat high, level of risk medium dan level of low*, sudah kelihatan mana resiko yang tinggi, sedang, dan rendah berdasarkan kemungkinan resiko yang telah diteliti.

Selanjutnya dilakukan proses Perlakuan risiko. Dimana pada tahap ini akan diberi usulan-usulan atau tindakan terkait perlakuan kemungkinan-

kemungkinan resiko yang sudah dikelompokkan. Agar dalam menjalankan proses bisnis dapat berjalan dengan lancar sesuai dengan *SOP (Standar Operasional Prosedur)* yang diterapkan perusahaan atau organisasi. Untuk perlakuan risiko dapat dilihat pada tabel usulan perlakuan risiko.

Tabel 10. Usulan Perlakuan Risiko

ID	Kemungkinan Resiko	*Risk Level*	Tindakan Resiko
RE12	Koneksi jaringan terputus	*High*	Lapor ke bagian mantene jaringan perusahaan
RE13	Koneksi jaringan tidak stabil	*High*	Mengganti ISP (Internet service provider) yang baru
RE04	Gempa Bumi	*High*	Menyediakan server cadangan di tempat yang aman
RE07	*User interface* aplikasi yang sulit dipahami	*Medium*	Membuat tampilan user interface yang simple dan membuat petunjuk penggunaan aplikasinya.
RE10	*Overload*	*Medium*	Melakukan refresh db log, temp dan RAM setelah itu lakukan pengecekan secara teratur minimal seminggu sekali agar tidak adanya penumpukan masalah pada aplikasi
RE03	Kebakaran	*Medium*	Menyediakan server cadangan di tempat yang aman
RE16	*Kerusakan hardware*	*Medium*	Melakukan perawatan rutin terkait hardware
RE01	Petir	*Low*	Memasang alat penangkal petir pada perusahaan

RE02	Banjir	*Low*	Menyimpan aset perusahaan ditempat yang lebih tinggi dan memasang server cadangan di tempat tempat yang lebih aman
RE09	Pencurian perangkat data	*Low*	Memasang cctv pada ruangan yang penting dan selalu melakukan pengawasan
RE08	*Cybercrime*	*Low*	Mengganti password server secara berkala dan memasang cctv pada ruangan yang penting dan selalu melakukan pengawasan
RE11	*Overheat*	*Low*	Mengontrol suhu ruangan agar selalu dingin dan selalu melakukan service AC (air conditioner) minimal seminggu sekali
RE05	Penyalahgunaan hak akses	*Low*	Memberikan batasan user pada aplikasi dan memberikan konfirmasi login pada bagian pengelola IT
RE15	*Backup failure*	*Low*	Mengontrol penggunaan memory database jangan sampai penuh dan melakukan maintenance secara berkala
RE06	Perubahan data umat	*Low*	Lapor atau konfirmasi pada bagian IT yang mengelola tentang data umat

RE14	*Data corrupt*	*Low*	Melakukan backup secara berkala untuk mengantisipasi kemungkinan yang terjadi dan memproteksi PC dengan antivirus secara berkala untuk mencegah munculnya virus

Pada tabel 10 menjelaskan bahwa Usulan perlakuan resiko sudah dijabarkan dari kemungkinan resiko, *risk level* dan tindakan resiko. Ditentukan mulai dari tinggi, sedang dan rendah kemungkinan resikonya mulai dari Koneksi jaringan terputus menyebabkan tingginya resiko dan tindakan yang dilakukan adalah lapor ke bagian maintenance jaringan perusahaan, Koneksi jaringan tidak stabil menyebabkan tingginya resiko dan tindakan yang dilakukan adalah mengganti ISP *(Internet service provider)* yang baru agar stabil kembali jaringannya, Gempa Bumi menyebabkan tingginya risiko dan tindakan yang dilakukan adalah menyediakan server cadangan ditempat yang aman, *User interface* aplikasi yang sulit dipahami menyebabkan resiko sedang yang terjadi dan tindakan yang dilakukan adalah membuat tampilan *user interface* yang simple dan membuat petunjuk penggunaan aplikasinya.

Overload menyebabkan resiko sedang,dan tindakan yang dilakukan adalah melakukan *refresh db log*, suhu dan RAM (*Random Access Memory*) setelah itu lakukan pengecekan secara teratur minimal seminggu sekali agar tidak adanya penumpukan masalah pada aplikasi, Kebakaran menyebabkan resiko sedang dan tindakan yang dilakukan adalah menyediakan *server* cadangan ditempat yang aman, Kerusakan *hardware* menyebabkan resiko sedang dan tindakan yang dilakukan adalah melakukan perawatan rutin terkait *hardware*, Petir menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah memasang alat penangkal petir pada perusahaan, Banjir menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah menyimpan aset perusahaan ditempat yang lebih tinggi dan memasang server cadangan di tempat tempat yang lebih aman, Pencurian perangkat data menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah memasang cctv pada ruangan yang penting dan selalu melakukan pengawasan.

Cybercrime menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah mengganti password server secara berkala dan memasang cctv pada ruangan yang penting dan selalu melakukan pengawasan, *Overheat* menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah mengontrol suhu ruangan agar selalu dingin dan selalu melakukan service AC (air conditioner) minimal seminggu sekali, Penyalahgunaan hak akses menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah memberikan batasan user pada aplikasi dan memberikan konfirmasi login pada bagian pengelola IT, *Backup failure* menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah mengontrol penggunaan memori database jangan sampai penuh dan melakukan maintenance secara berkala, Perubahan data umat menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah lapor atau konfirmasi pada bagian IT yang mengelola tentang data umat, dan *Data corrupt* menyebabkan rendahnya resiko dan tindakan yang dilakukan adalah melakukan *backup* secara berkala untuk mengantisipasi kemungkinan yang terjadi dan memproteksi PC dengan antivirus secara berkala untuk mencegah munculnya virus.

4. KESIMPULAN

Kesimpulannya adalah terhambatnya proses bisnis membuat terhentinya pelayanan di dalam mengelola data umat, susahnya mencari informasi terkait data umat, tidak adanya data terbaru akan berdampak juga untuk bidang yang ada di Gereja Santo Paulus Miki Salatiga dan kurangnya sumber daya manusia yang mengelola aplikasi di Gereja Santo Paulus Miki Salatiga membuat proses bisnis tidak berjalan dengan lancar, mengatasi permasalahan dilakukannya Analisis Resiko Aplikasi Sistem Informasi Pengelolaan Data Umat Menggunakan ISO 31000 untuk melihat kemungkinan resiko yang membuat terhentinya proses bisnis, analisis yang dilakukan ada 2 tahap pencarian informasi yaitu *Risk Assessment* (Penilaian Resiko) dan *Risk Treatment* (Perlakuan Risiko. Pada tahap penilaian risiko melihat resiko apa saja yang akan muncul setelah itu susun strategis bagaimana cara agar tepat sasaran dan buat perbaiki jika gagal melakukan penilaian risiko. Tahap perlakuan risiko adalah merubah kemungkinan resiko yang akan terjadi sehingga perusahaan atau organisasi sudah mempunyai cadangan sebelum resiko terjadi dan tidak menghambat proses bisnis sehingga dapat berjalan dengan lancar.

DAFTAR PUSTAKA

[1] M. Miftah Khatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Echofon Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcsev1i2.76.

[2] A. R. Viyanto, O. S. Latuihamallo, F. M. Tua, and A. Gui, "Studi Kasus Pada Perusahaan Jasa," vol. 4, pp. 43–54, 2013.

[3] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus: i-Gracias Telkom University) Information Technology Risk Analysis Based on Risk Management Using Iso 31000 (Case Study: i-Gracias Telkom University)," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6201–6208, 2015.

[4] R. P. Pangestu and A. F. Wijaya, "View of Analisis Management Resiko Aplikasi SINTESA Pada Perpustakaan XYZ," vol. 2, no. 2, pp. 1–14, 2020, [Online]. Available: http://journal.binadarma.ac.id/index.php/binakomputer/article/view/804/529.

[5] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019, doi: 10.46984/sebatikv23i1.441.

[6] F. L. Nice and R. V. Imbar, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *J. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 1–11, 2017.

[7] F. M. Hutabarat and A. D. Manuputty, "Analisis Risiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komputer.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[8] N. U. Handayani, D. P. Sari, D. O. Irawan, and Z. Afdi, "Departemen Teknik Industri Universitas Diponegoro," vol. XII, no. 1, 2017.

[9] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[10] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000: 2018 (Studi Kasus: Cv. Xy)," *Sebatik*, vol. 23, no. 1, pp. 277–284, 2019, doi:

10.46984/sebatik.v23i1.572.

[11] G. H. S. Rampini, H. Takia, and F. T. Bersanetti, "Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes," *Procedia Manuf.*, vol. 39, pp. 894–903, 2019, doi: 10.1016/j.promfg.2020.01.400.

[12] I. P. A. E. Pratama and M. T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *J. Telemat.*, vol. 15, no. 2, pp. 63–70, 2020.

[13] Sermon Paskah Zagato and Melkior N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Di Organisasi Xyz Cabang Salatiga Menggunakan Iso 31000," *J. Mnemon.*, vol. 4, no. 1, pp. 1–9, 2021, doi: 10.36040/mnemonic.v4i1.2877.

[14] G. Mochammad Husein and R. V. Imbar, "Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 2, pp. 75–87, 2015, doi: 10.28932/jutisi.v1i2.368.

[15] A. Imansari, "Analisis Risiko Berdasarkan Aspek Waktu Dengan Metode Monte Carlo Pada Proyek Gedung Baru Di Universitas Brawijaya," *Naskah Terpublikasi Tek. Sipil*, 2019.