SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK II - Surabaya, 26 Maret 2022
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2022.2716

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Website SIMPEG di Kantor Kementerian Agama Kota Palembang

Orik Dwi Pebriani[1], Dian Hafidh Zulfikar, S.Kom.,M.Cs[2]

Universitas Islam Negeri Raden Fatah Palembang[1,2]

e-mail: orikdwi421@gmail.com

ABSTRACT

The Personnel Management Information System (SIMPEG) is a part of a public agency that is very important to pay attention to for the success of public services. This information system is able to support administrative staffing at the Office of the Ministry of Religion of Palembang City. So the need for this system is very important. Therefore, IT Risk Management needs to be carried out to plan strategies for the success of public services and reduce risks that may occur. If a problem occurs on an ongoing basis, it will have an impact or risk on SIMPEG which will disrupt the information technology service process at the Palembang City Ministry of Religion Office. This study uses the ISO 31000 method, which has stages including communication and consultation, determining context, risk assessment (risk identification, risk analysis, risk evaluation) and risk treatment. From the results of the threat evaluation that has been carried out, there are 18 possible risks, in particular there are 3 high-level risks (power outage, server down, network connection is lost/unstabel), 7 low-level risks (fire, earthquake, access rights, hardware damage, overload damage, system crash, data corrupt) and 8 low levels (flood, human error, device/data theft, technical error, cybercrime, information accessed by irresponsible parties, overheating, malware virus attack) which can be used as guidelines in prevent, manage and maintain systems and technology assets for the future.

Keywords: *SIMPEG, Information Systems, IT Risk Management, ISO 31000.*

ABSTRAK

Sistem Informasi Manajemen Kepegewaian (SIMPEG) merupakan bagian di sebuah instansi publik yang sangat penting untuk diperhatikan demi keberhasilan pelayanan publik. Sistem informasi ini mampu mendukung keadministrasian kepegawaian di Kantor Kementerian Agama Kota Palembang. Sehingga

kebutuhan sistem ini sangat di pentingkan. Oleh karena itu, Manajemen Risiko TI perlu dilakukan untuk merencanakan strategi demi keberhasilan pelayanan publik dan mengurangi risiko yang mungkin terjadi. Jika terjadi permasalahan secara berkelanjutan, maka akan memberikan dampak ataupun risiko pada SIMPEG yang akan mengganggu proses layanan teknologi informasi di Kantor Kementerian Agama Kota Palembang. Penelitian ini menggunakan metode ISO 31000, yang memiliki tahapan meliputi komunikasi dan konsultasi, menentukan konteks, penilaian risiko(identifikasi risiko, analisis risiko, evaluasi risiko) dan perlakukan risiko. Dari hasil evaluasi ancaman yang telah dilakukan terdapat 18 kemungkinan risiko, terutama ada 3 risiko tingkat tinggi(Listrik padam, *server down*, koneksi jaringan terputus/tidak stabil), 7 risiko tingkat sedang(kebakaran, gempa bumi, penyalahgunaan hak akses, kerusakan hardware, *overload*, *sistem crash*, *data corrupt*) dan 8 tingkat rendah (banjir, *human error*, pencurian perangkat/data, kesalahan teknis, *cybercrime*, informasi diakses oleh pihak yang tidak bertanggung jawab, *overheat*, serangan virus *malware*) yang dapat digunakan sebagai pedoman dalam mencegah, mengelola dan mempertahankan sistem dan aset teknologi untuk masa yang akan datang.

Kata kunci: SIMPEG, Sistem Informasi, Manajemen Risiko TI, ISO 31000.

PENDAHULUAN

Penerepan teknologi informasi pada suatu instansi terutama Kantor Kementerian Agama Kota Palembang merupakan hal penting yang tidak bisa dipisahkan dari informasinya. Penerapan teknologi informasi tersebut menimbulkan *value* pada instansi, yaitu dengan adanya teknologi informasi dapat mempermudah semua aktivitas didalam instansi seperti dokumen-dokumen bersifat *hardfile* yang membutuhkan banyak tempat untuk meyimpannya bisa diubah dalam bentuk *softfile* dengan memanfaatkan teknologi informasi. Akan tetapi, selain *value* penerapan teknologi informasi tersebut juga menimbulkan berbagai risiko yang dapat mengancam aktivitas suatu instansi. Adapun salah satu penerapan teknologi informasi di Kantor Kementerian Agama Kota Palembang yaitu penggunaan website sistem informasi manajemen kepegawaian (SIMPEG WEB).

SIMPEG WEB adalah sistem informasi kepegawaian berbasis web, sistem ini untuk mendukung pendataan kepegawaian khususnya di lingkungan Kementerian Agama RI[1]. Untuk mengakses SIMPEG WEB ini sebelumnya pengguna harus melakukan registrasi secara manual, dengan mengajukan surat resmi permohonan pengguna (user id) kepada Bagian Data dan Informasi Biro Kepegawaian Kementerian Agama Pusat untuk diproses registrasinya. Ini dilakukan untuk mengontrol pengguna yang dapat mengakses sistem ini sehingga dapat dipertanggungjawabkan[1].

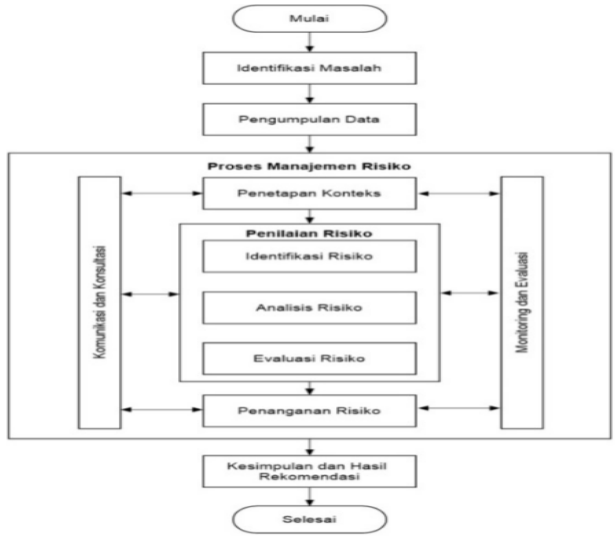
Risiko adalah hal yang tidak pasti dan mempunyai dampak negatif terhadap suatu tujuan atau keinginan yan akan dicapai[2]. Risiko bisa menjadi tantangan yang paling diperhatikan bagi setiap perusahaan, dimana setiap perusahaan harus bisa melakukan manajemen risiko dengan baik. Adanya manajemen risiko dalam pengelolaan suatu perusahaan adalah hal yang penting. Mengetahui risiko-risiko serta menyusun tindakan untuk meminimalisir atas kejadian risiko tersebut hingga membuat kebijakan mengatasi risiko adalah bagian dari manajemen risiko[2].

Berdasarkan identifikasi masalah diatas, penelitian ini memprioritaskan pada penggunaan website sistem informasi manajemen kepegawaian (SIMPEG WEB). Pada SIMPEG WEB sering terjadi permasalahan dan menimbulkan risiko yangmana ketika risiko tersebut terjadi pengguna masih bingung untuk mengatasi permasalahan tersebut. Risiko ini bisa saja berupa peristiwa atau kejadian yang mengakibatkan terganggu bahkan terhentinya layanan sistem informasi tersebut. Oleh karena itu,diperlukannya pengukuran risiko sistem informasi untuk menilai dan mengambil tindakan pada semua risiko sistem informasi dengan maksud untuk meningkatkan kemungkinan keberhasilan dan mengurangi kemungkinan kegagalan. Sesuai dengan requirements, kantor belum pernah melakukan pengukuran risiko pada website sistem informasi manajemen kepegawaian (SIMPEG WEB). Maka dari itu peneliti melakukan analisis manajemen risiko teknologi informasi pada SIMPEG WEB menggunakan ISO 31000. ISO

31000 merupakan standar penegelolan risiko yang terdiri atas tiga elemen: prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*). Prinsip manajemen risiko adalah dasar praktik atau filosofi manajemen risiko[2]. Kerangka kerja merupakan pedoman sistem manajemen risiko secara terstruktur dan sistematis. Proses adalah aktivitas pengelolaan risiko yang berurutan dan saling terkait. Secara umum, ISO 31000:2018 merupakan versi sederahan dari versi 2009. Kelebihan ISO 31000:2018 adalah dapat membantu organisasi dalam melakukan manajemen risiko lebih efektif. Hal ini dikarenakan dalam standar ini menyediakan prinsip, kerangka kerja, dan proses manajemen risiko yang dapat digunakan sebagai arsitektur manajemen risiko yang mampu menjamin penerapan manajemen risiko TI yang lebih efektif[2]. Hasil dari analisis manajemen risiko TI nantinya dapat mempermudah organisasi dalam mengelolah risiko yang terjadi.

METODE

Untuk melakukan penelitian ini, peneliti memiliki konsep penelitian yang dapat dilihat pada gambar 1 dibawah ini :



Gambar 1. Konsep Penelitian

Dari gambar diatas, dapat dijelaskan sebagai berikut :

1. Identifikasi Masalah

Merupakan tahap awal yang dilakukan dalam menentukan rumusan masalah, batasan masalahm tujuan dan manfaat dari penelitian yang dilakukan.

2. Metode Pengumpulan Data

Merupakan cara yang digunakan peneliti dalam menghimpun data dan informasi yang dibutuhkan dalam penelitian. Dalam tahap ini cara yang digunakan adalah studi kepustakaan.

3. Proses Manajemen Risiko ISO 31000

Proses manajemen resiko yang dilakukan mengacu pada Standar ISO 31000. Standar ini diterbitkan oleh International Organization for Standardization pada tanggal 13 November 2009 untuk digunakan dalam pelaksanaan manajemen risiko [3]. Di dalam ISO 31000 dijelaskan bahwa dalam proses manajemen risiko terdapat beberapa aktivitas sebagai berikut[4]:

a. Komunikasi dan Konsultasi (*Communication and Consultation*)

Tahap komunikasi dan konsultasi adalah menghimpun informasi dengan pemangku kepentingan untuk mendapatkan pandangan, pertimbangan, penilaian dan pendapat terhadap risiko yang didasarkan pada persepsi mereka terhadap risiko tersebut.

b. Penetapan konteks (*Establishing the Context*)

Terdapat empat konteks yang perlu ditentukan dalam penetapan konteks ,yaitu konteks eksternal, konteks internal, konteks manajemen risiko, dan kriteria risiko.

c. Assessment Risiko

ISO 31000 mendefinisikan asesment risiko sebagai keseluruhan proses identifikasi risiko, analisis risiko, dan evaluasi risiko.

d. Perlakuan Risiko (Risk Treatment)

Setelah diketahui hasil penilaian resiko maka perlu ditentuan perlakuan resiko (*risk* treatment). Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; *risk prevention* (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, risk *mitigation* (mitigasi *risiko*) dengan tujuan untuk mengurangi dampak dari risiko, risk *sharing* (berbagi risiko) dengan tujuan untuk membagi risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupun individu, dan risk *retention* (retensi risiko) dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko[5].

HASIL DAN PEMBAHASAN

Komunikasi dan Konsultasi

Kegiatan yang dilakukan yaitu melakukan observasi dan wawancara kepada pihak yang terkait di Kantor Kementerian Agama Kota Palembang. Tahap ini dilakukan kepada pegawai di bidang tata usaha kepegawaian yaitu Ibu Emi Kartika, untuk mengulas terkait izin melaksanakan manajemen risiko sehingga terdapat bukti yang kuat, sebagai dasar pertanggung jawaban untuk dilakukan manajemen risiko di Kantor Kementerian Agama Kota Palembang. Proses komunikasi dan konsultasi merupakan tahap awal mengelola risiko, karena mungkin ada prosedur untuk mengubah fakta dan ulasan tentang ancaman dan manajemennya.

Menentukan Konteks

Konteks pada Kantor Kementerian Agama Kota Palembang, meliputi :

a. Visi dan Misi : Visi dan misi kantor telah disebutkan sebelumnya, yang telah tertuang dalam Surat Keputusan Kepala Kantor Wilayah Kementerian Agama Provinsi Sumatera Selatan Nomor : Kpts./Kw.0.1/OT.01.3/296/2009.
b. Struktur Organisasi : Merupakan gambaran yang jelas berhubungan dengan posisi dan jabatan di dalam kantor.
c. Pegawai/SDM : Merupakan hal yang sangat penting di Kantor Kementerian Agama Kota Palembang.

Penilaian Risiko

Penilaian risiko pada website SIMPEG terapat tiga tahap yaitu identifikasi risiko (risk identification), analisis risiko (*risk analiysis)* dan evaluasi risiko *(risk evaluate).*

a. Identifikasi Risiko

1. Identifikasi Aset

Identifikasi aset pada website SIMPEG dilaksanakan melalui proses wawancara, observasi, studi pustaka, dan dokumentasi. Identifikasi aset diambil dari data,software hingga hardware yang berkaitan dengan website SIMPEG.

Tabel 1. Identifikasi Aset SIMPEG

Identifikasi Aset SIMPEG	
Data	Data Pengguna
Software	Sistem Informasi Manajemen Kepegawaian (SIMPEG)
Hardware	1. Komputer 2 Handphone. 3. Keyboard 4. Printer 5. Wifi 6. CPU

2. Identifikasi Kemungkinan Risiko

Tahap identifikasi kemungkinan risiko ini dilakukan untuk mengidentifikasi kemungkinan - kemungkinan risiko yang muncul pada aset - aset SIMPEG yang berasal dari banyak faktor seperti alam, manusia serta sistem dan infrastruktur.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko
Alam&Lingkungan	KR01	Kebakaran
	KR02	Listrik Padam
	KR03	Banjir
	KR04	Gempa bumi
Manusia/SDM	KR05	Penyalahgunaan hak akses
	KR06	*Human error*
	KR07	Pencurian perangkat atau data
	KR08	Kesalahan teknis
Sistem&Infrastruktur	KR09	*Cybercrime*
	KR10	Informasi diakses oleh pihak yang tidak bertanggung jawab
	KR11	*Server down*
	KR12	Kegagalan/rusaknya hardware
	KR13	Koneksi jaringan terputus
	KR14	*Overheat*
	KR15	*Overload*
	KR16	Sistem *crash*
	KR17	*Data corrupt*
	KR18	Serangan virus,*malware*

3. Identifikasi Dampak Risiko

Tahap selanjutnya adalah melakukan identifikasi dampak risiko. Tahap ini bertujuan untuk mengidentifikasi dampak seperti apa yang akan dialami jika kemungkinan risiko terjadi.

Tabel 3. Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak Risiko
R01	Kebakaran	Kerusakan sarana dan prasarana instansi, kerugian materiil, mengganggu aktivitas di instansi dan kehilangan aset-aset.
R02	Listrik Padam	Kerugian operasional instansi, kualitas server menurun, dan mengganggu proses kerja pegawai.
R03	Banjir	Aktivitas pegawai terhambat, alat rusak dan kerugian secara finansial.
R04	Gempa bumi	Aktivitas pegawai terhambat, alat rusak dan kerugian secara finansial.
R05	Penyalahgunaan hak akses	Manipulasi data dan kebocoran infromasi/data penting.
R06	Human error	Proses kerja terhambat dan data sulit untuk diakses.
R07	Pencurian perangkat / data	Kehilangan data dan kerugian dari segi finansial.
R08	Kesalahan Teknis	Pekerjaan terhambat.
R09	Cybercrime	Pencurian data.
R10	Informasi diakses oleh pihak yang tidak bertanggung jawab	Data dimanipulasi dan disebarkan ke pihak yang tidak bertanggung jawab.
R11	*Server down*	Menghambat pekerjaan dan tidak dapat mengakses website.
R12	Kegagalan/rusaknya hardware	Terhambat dalam mengakses website dan kerugian secara finansial.
R13	Koneksi jaringan terputus/tidak stabil	Gagal update data dan proses kerja terhambat.
R14	*Overheat*	Loading lambat, proses kerja terganggu dan alat mengalami kerusakan.
R15	*Overload*	Loading lambat, proses kerja terganggu, kinerja server menjadi lambat.
R16	Sistem *crash*	SOP tidak berjalan dengan baik.
R17	*Data corrupt*	Kehilangan/rusak data dan roses kerja terganggu.
R18	Serangan virus,*malware*	Proses kerja terganggu.

b. Analisis Risiko

Selanjutnya melakukan proses analisis risiko. proses ini akan dilakukan penilaian terhadap kemungkinan risiko yang telah diidentifikasi.

Tabel 4. Analisis Risiko

ID	Kemungkinan Resiko	*Likelihood*	*Impact*
R01	Kebakaran	1	5
R02	Listrik Padam	4	5
R03	Banjir	1	2
R04	Gempa bumi	1	5
R05	Penyalahgunaan hak akses	2	3
R06	Human error	3	2
R07	Pencurian perangkat atau data	2	2
R08	Kesalahan Teknis	3	2
R09	Cybercrime	1	3
R10	Informasi diakses oleh pihak yang tidak bertanggung jawab	2	2
R11	*Server down*	4	3
R12	Kegagalan/rusaknya hardware	3	3
R13	Koneksi jaringan terputus/tidak stabil	3	4
R14	*Overheat*	3	2
R15	*Overload*	3	3
R16	Sistem *crash*	2	4
R17	*Data corrupt*	2	3
R18	Serangan virus,*malware*	1	3

c. Evaluasi Risiko

Proses terakhir dalam penilaian risiko adalah evaluasi risiko. Evaluasi risiko adalah proses untuk menentukan risiko mana yang perlu diprioritaskan. Evaluasi risiko menggunakan acuan berupa matriks risiko, matriks tersebut dibedakan kedalam 3 risk level yaitu *low*, *medium*, dan *high*.

Tabel 5. Matriks Evaluasi Risiko

L I K E H O O D	*Certain* (5)					
	Likely (4)			R11		R02
	Possible (3)		R06, R08	R12, R15	R13	
	Unlikely (2)		R07, R14	R05, R17	R16	
	Rare (1)		R03, R10	R09, R18		R01, R04
		Insignificant (1)	*Minor* (2)	*Moderate* (3)	*Major* (4)	*Catastrophic* (5)
		IMPACT				

Tabel 6. Level Risiko

Level Risiko	Keterangan
High Risk (Risiko Tinggi)	Risiko yang berbahaya yang harus diatasi secepatnya
Moderate Risk (Risiko Sedang)	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan
Low Risk (Risiko Rendah)	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil

Hasil dari evaluasi risiko yaitu dari 18 kemungkinan risiko terdapat 3 kemungkinan risiko(Listrik padam, *server down*, koneksi jaringan terputus/tidak stabil) *level of risk* dengan tingkatan *high*, 7 kemungkinan risiko tingkatan *Moderate*(kebakaran, gempa bumi, penyalahgunaan hak akses, kerusakan hardware, *overload, sistem crash, data corrupt*), dan 8 kemungkinan risiko tingkatan *low* (banjir, *human error*, pencurian perangkat/data, kesalahan teknis, *cybercrime*, informasi diakses oleh pihak yang tidak bertanggung jawab, *overheat*, serangan virus *malware*).

Perlakuan Risiko

Tahap selanjutnya yaitu perlakukan risiko, dimana penulis memberikan saran untuk kemungkinan risiko yang ada pada website SIMPEG, dengan harapan dapat digunakan untuk melakukan pencegahan terhadap kemungkinan risiko yang mungkin akan terjadi.

Tabel 7. Perlakuan Risiko

ID	Kemungkinan Risiko	Level Risiko	Perlakuan Risiko
R02	Listrik Padam	High	Menyediakan genset dan harus memperbaiki sistem regenerasi genset, hendaklah bagian IT terlebih dahulu menyalakan genset, karena topangan daya sangat mempengaruhi proses bisnis.
R11	Server down	High	Melakukan pengecekan server secara berkala dan melakukan back up data.
R13	Koneksi jaringan terputus/tidak stabil	High	Melakukan monitoring jaringan secara berkala dan menambahkan router penguat sinyal agar sistem dapat diakses.
R01	Kebakaran	Moderate	Menyediakan alat pemadam kebakaran dan menyiapkan perencanaan penyediaan cadangan infrastruktur baik hardware /perangkat jaringan
R04	Gempa Bumi	Moderate	Menyiapkan perencanaan penyediaan cadangan infrastruktur baik hardware maupun perangkat jaringan
R05	Penyalahgunaan hak akses	Moderate	Mengganti password secara berkala dan membatasi user dalam mengakses website, memberikan akses kepada user yang dipercaya dan bertanggung jawab.
R12	Kegagalan/rusaknya hardware	Moderate	Melaporkan segera ke bagian teknisi jika hardware tidak bisa diperbaiki maka pengguna langsung mengurus permintaan barang baru sehingga tidak menghambat pekerjaan.
R15	*Overload*	Moderate	Melakukan monitoring berkala dan melakukan backup data sesuai standar.
R16	Sistem *crash*	Moderate	Membuat jadwal dan melakukan back up data secara berkala
R17	*Data corrupt*	Moderate	Membuat jadwal, melakukan pengecekan data dan back up data secara berkala.
R03	Banjir	Low	Tempatkan infrastruktur baik hardware maupun perangkat jaringan yang aman jauh dari kemungkinan banjir dan men yiap-kan perencanaan penyediaan cadangan infrastruktur baik hardware maupun perangkat jaringan.
R06	Human error	Low	Memberikan teguran lisan kepada pengguna jika masih melakukan kesalahan akan diberikan teguran secara tertulis, melakukan pelatihan terhadap pengguna dan melakukan pembagian tugas sesuai dengan kemampuan masing-masing.
R07	Pencurian perangkat atau data	Low	Melakukan perubahan password secara berkala, mempercaya data penting kepada pengguna yang bertanggung jawab, memperbanyak tenaga security dan memperbanyak titik pemasangan CCTV
R08	Kesalahan Teknis	Low	Mem pelatihan kepada penggunadan membuat SOP di bidang kerjanya.
R09	Cybercrime	Low	Menyediakan perlindungan security software yang up to date dan menginstals software anti virus
R10	Informasi diakses oleh pihak yang tidak bertanggung jawab	Low	Melakukan perubahan password secara berkala
R14	Overheat	Low	Melakukan perawatan perangkat dan menggunakan perangkat sesuai kebutuhan
R18	Serangan virus,malware	Low	Memasang antivirus yang terpercaya dan update

KESIMPULAN

Berdasarkan hasil penelitian manajemen risiko pada website sistem informasi manajemen kepegawaian (SIMPEG) di Kementerian Agama Kota Palembang menggunakan ISO 31000, disimpulkan bahwa untuk setiap aset dan perangkat pendukung sistem SIMPEG membutuhkan asupan listrik dan koneksi jaringan yang baik agar setiap perangkat bisa berjalan dengan lancar dan tidak menghambat pekerjaan. Untuk itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung sistem agar berjalan dengan optimal.

DAFTAR PUSTAKA

[1] S. Informasi and K. Berbasis, "Panduan Penggunaan Aplikasi Simpeg Web."

[2] K. B. Mahardika, A. F. Wijaya, and D. Cahyono, "Manajemen risiko teknologi informasi menggunakan iso 31000 : 2018 (studi kasus: cv. xy)," vol. 2018, pp. 277–284, 2018.

[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] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.

[5] G. M. Husein and R. V. Imbar, "Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT . Jabar Telematika (JATEL)," vol. 1, pp. 75–87, 2015.