JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 16-25

ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI CUPK MOBILE (STUDI KASUS : KSP ABC)

Kristoforus Charmindo Delazega Jayonata*[1)], Melkior N. N. Sitokdana[2)]
1. Universitas Kristen Satya Wacana, Indonesia
2. Universitas Kristen Satya Wacana, Indonesia

Article Info
Kata Kunci: Analisis Risiko; CUPK Mobile; ISO 31000; Manajemen Risiko

Keywords: CUPK Mobile; ISO 31000; *Risk Analysis; Risk Managemen*

Article history:
Received 2 November 2023
Revised 16 November 2023
Accepted 30 November 2023
Available online 1 March 2023

DOI :
https://doi.org/10.29100/jipi.v9i1.4291

* Corresponding author.
Kristoforus Charmindo Delazega Jayonata
E-mail address:
jayonata23@gmail.com

ABSTRAK
CUPK Mobile merupakan sebuah aplikasi yang digunakan oleh Koperasi Simpan Pinjam ABC (*KSP ABC*) untuk menunjang proses bisnis yang dijalankan. Aplikasi CUPK Mobile bertujuan untuk mempermudahkan nasabah dalam melakukan transaksi keuangan secara digital. Penelitian ini dilakukan bertujuan untuk mengetahui dan mengidentifikasi kemungkinan-kemungkinan risiko apa saja yang dapat mengganggu jalannya proses bisnis pada aplikasi CUPK Mobile. Penelitian dilakukan menggunakan metode ISO 31000 yang merupakan pendoman dalam analisis manajmen risiko dengan memiliki 3 tahapan besar yaitu identifikasi risiko (*Risk Identification*), analisis risiko (*Risk Analsyt*), dan evaluasi risiko (*Risk Evaluation*). Selanjutnya tahapan terahkir yaitu perlakuan risiko (*Risk Treatment*) untuk memberikan rekomendasi penanganan risiko yang telah teridentifikasi. Hasil dari penelitian ini terdapat 21 kemungkinan risiko, diantaranya terdapat 4 risiko yang memiliki *level risiko high*, 7 risiko yang memiliki *level risk medium*, dan 10 risiko yang memiliki *level low*. Penelitian yang telah dilakukan menghasilkan rekomendasi risiko, dengan begitu organisasi dapat melakukan penyelesaian dalam penanganan risiko yang dapat menghambat proses bisnis pada aplikasi CUPK Mobile.

ABSTRACT
CUPK Mobile is an application used by ABC Savings and Loan Cooperative (KSP ABC) to support its business processes. The CUPK Mobile application aims to facilitate customers in conducting digital financial transactions. This research is conducted to identify and assess the possible risks that may disrupt the business processes of the CUPK Mobile application. The research is conducted using the ISO 31000 method, which serves as a guideline for risk management analysis consisting of three major stages: risk identification, risk analysis, and risk evaluation. The final stage is risk treatment, which involves providing recommendations for handling the identified risks. The research findings reveal 21 potential risks, including 4 risks with a high-level risk, 7 risks with a medium-level risk, and 10 risks with a low-level risk. The research provides risk recommendations, enabling the organization to address the risks that may hinder the business processes of the CUPK Mobile application.

I. PENDAHULUAN

TEKNOLOGI berkembang dengan sangat pesat pada era globalisasi saat ini[1]. Perkembangan teknologi yang pesat ini memunculkan banyak dampak pada sektor bisnis, termaksuk bisnis Koperasi Simpan Pinjam. Dalam dunia bisnis koperasi simpan pinjam memulai dan mengembangkan serta memperluas jangkauan bisnis mereka melalui kemudahan dalam melakukan transaksi yang sangat cepat dan dinamis. Teknologi informasi menjadi alat yang dipakai untuk berhubungan dengan konsumen baik secara langsung maupunn tidak langsung[2]. Salah satu organisasi yang menfaatkan teknologi informasi adalah Koperasi Simpan Pinjam ABC (KSP ABC) guna meningkatkan kualitas layanan dan operasionalnya.

Koperasi Pimpan Pinjam ABC (KPS ABC) memiliki berbagai tujuan untuk meningkatkan kesejatheraan anggotanya dalam kemajuan lingkungan kerja pada umumnya untuk menciptakan sumber keredit bagi anggota-anggotanya dengan menerapkan bunga yang layak[3]. Pada saat ini, KSP ABC telah mengintergrasikan beberapa sistem teknologi di antara departemennya, termasuk salah satunya yang digunakan untuk menyediakan layanan

dalam bertransaksi kepada nasabah. Aplikasi ini digunakan untuk mempermudahkan anggotanya melakukan transaksi keuangan secara digital diberbagai layanan yang disediakan oleh KSP ABC. CUPK Mobile merupakan suatu sistem berbasis Android yang terhubung langsung dengan sistem rekening online milik nasabah. Aplikasi ini digunakan untuk memasukkan data transaksi yang akan dijalankan. Setelah data dimasukkan ke dalam aplikasi CUPK Mobile, informasi tersebut akan langsung terkirim ke sistem rekening online dan diubah menjadi rekening anggota untuk digunakan sebagai bukti transaksi.

Dalam penggunaan sistem teknologi informasi tidak dapat menjamin bahwa tidak akan muncul risiko atau ancaman yang dapat mengganggu kinerja pada aplikasi. Salah satu kendala yang sering terjadi adalah kegagalan dalam proses transaksi melalui aplikasi CUPK Mobile. Hal ini dapat terjadi karena server mengalam *Errol* atau mengalami gangguan. Jika server mengalami masalah, maka sistem informasi tidak dapat digunakan dan mengalami kegagalam dalam menupdate software dan koneksi jaringan internet yang tidak stabil. Hal ini dapat mempengaruhi efisiensi kerja dan mengganggu pengguna aplikasi tersebut. Oleh karena itu, perlu dilakukan pengawasan dan pemeliharaan terus menerus pada sistem teknologi informasi yang digunakan untuk meminimalisir risiko dan mencegah terjadinnya kendala yang dapat menggangu kinerja pegawai. Risiko-risiko tersebut berkaitan dengan teknologi informasi yang ada pada asset TI termasuk dalam lingkup manajemen bisnis. Pengembangan teknologi informasi juga merupakan bagian penting dari manajemen bisnis. Karena itu, kegagalan atau bencana pada TI dapat menghambat proses bisnis[4].

Analisis risiko teknologi informasi terhadap aplikasi CATTER dengan menggunakan ISO 31000 sudah pernah dilakukan oleh Enik Muryanti dan menghasilkan 26 kemungkinan risiko yang dapat menghambat kinerja pada aplikasi CATTER, yang sudah dikelompokkan berdasarkan level risikonya[5]. Penelitian analisis risiko menggunakan ISO 31000 yang dilakukan oleh Aprillis Rahmawati pada aplikasi iTop dan menghasilkan 21 kemungkinan risiko yang sudah dikelompokkan berdasarkan level risiko untuk meminimalisir kemungkinan risiko pada aplikasi iTop[6]. Selain itu, Penelitian yang berkaitan dengan ISO 31000 juga pernah dilakukan oleh Miftakhatun pada website Ecofo dan menghasilkan 24 kemungkinan risiko yang sudah dikelompokkan berdasarkan level risikonya sehingga dapat digunakan sebagai acuan dalam penanganan risiko, pencegahan terjadinnya risiko dan pemeliharaan terhadap asset IT dari hasil rekomendasi penilaian risiko pada Website Ecofo[7].

Berdasarkan dari penelitan-penelitian terdahulu, dapat disimpulkan bahwa analisis manajemen risiko menggunakan ISO 31000 bertujuan untuk mengidentifikasi kemungkinan-kemungkinan risiko yang dapat terjadi seperti, dampak risiko, level risiko dan tindakan yang dapat diambil untuk mengatasi risiko diperusahaan atau intansi[8]. Namun, terdapat perbedaan konteks dalam penitian ini seperti aplikasi/sistem yang dianalisis, jumlah dan jenis risiko yang diidentifikasi, pengelompokkan risiko berdasarkan level risiko serta rekomendasi dan tindakan pengelolaan risiko. Penelitian yang akan dilakukan adalah analisis kemungkinan risiko yang terjadi pada aplikasi CUPK Mobile, sehingga risiko-risiko sebulumnya teridentifikasi dapat dianalisis secara terperinci. Selain itu, penelitian ini juga menghasilkan penilaian tentang tingkat dampak risiko yang muncul pada aplikasi CUPK Mobile, serta memberikan pemahaman yang lebih baik tentang sejauh mana risiko-risiko tersebut dapat mempengaruhi operasional dan kinerja aplikasi. Penelitian ini memberikan rekomendasi konkret mengenai perlakuan risiko yang dapat dilakukan untuk meminimalisir kemungkinan terjadinya risiko tersebut, dengan rekomendasi didasarkan pada analisis yang mendalam terhadap risiko-risiko yang telah diidentifikasi pada aplikasi CUPK Mobile.

Tujuan dari penelitian ini adalah membantu Koperasi Simpan Pinjam ABC untuk mengidentifikasi tingkat kemungkinan risiko yang mungkin terjadi pada aplikasi CUPK Mobile, sehingga KSP ABC dapat melakukan pencegahan agar kemungkinan-kemungkinan risiko tersebut tidak terjadi dan mengganggu proses binsis di KSP ABC.

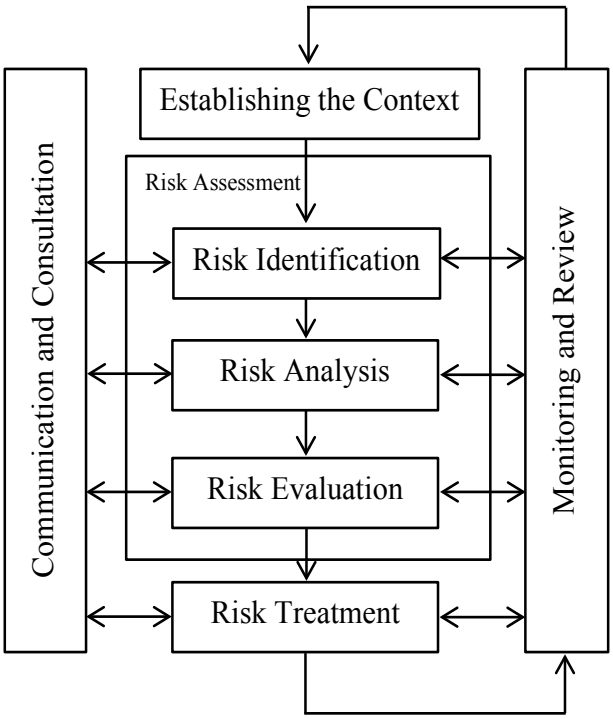
II. METODE PENELITIAN

A. Metode Penelitian

Penelitian ini disajikan dengan menggunakan metode studi kasus (*case study research*) dimana metode ini berhubungan dengan satu tujuan peneliti yang berfokus pada aplikasi CUPK Mobile. Penulis juga melakukan pendekatan kuantitatif dengan melakukan observasi langsung dilapangan untuk mengumpulkan data yang bersifat asli dan sudah terverifikasi.

Metode penelitian dalam kasus manajemen risiko pada aplikasi CUPK Mobile di KSP ABC dilakukan menggunakan metode ISO 31000:2018, dimana suatu standar internasional yang menyediakan prinsip-prinsip dan pendoman dalam manajemen risiko. Dalam manajemen risiko, Langkah-langkah yang dilakukan meliputi identifikasi risiko, analisis risiko, evaluasi risiko, dan rekomendasi pengelolaan risiko[9].

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 16-25



Tahapan pertama yang perlu dilakukan dalam penilaian risiko pada aplikasi CUPK Mobile adalah melakukan penelitian risiko dengan metode yang sistematis untuk menentukan apakah risiko tersebut dapat diterima atau tidak. Tahapan penilaian risiko memiliki beberapa tahapan, yaitu:

1. Tahap Identifikasi Risiko (*Risk Identification*)
   Identifikasi risiko merupakan proses untuk mengidentifikasi dan mengevaluasi risiko-risiko yang kemungkinan terjadi dalam proses operasional binsis diperusahaan[10]. Identifikasi risiko dilakukan untuk semua proses binsis yang terdapat di perusahaan dengan tujuan untuk mengetahui semua factor risiko yang kemungkinan terjadi, termasuk factor manusia, sistem yang diimplementasikan dan infrastruktur.
2. Tahap Analisis Risiko (*Risk Analysis*)
   Analisis risiko ini berupa factor-faktor apa saja yang dapat mempengaruhi penilaian, karaterisasi, manajemen risiko yang berhubungan dengan infrastruktur SI/TI dalam perusahaan[11]. Untuk menganalisis risiko yang terjadi, peneliti menggunakan table Kriteria Kemungkinan (*Likelihood*). Table Kriteria Kemungkinan terdiri dari 5 yaitu : Jarang Sekali (*Rare*), Jarang Terjadi (*Unlikely*), Cukup Sering Terjadi (*Moderate*), Sering Terjadi (*Likely*) dan Selalu Terjadi (*Certain*).

TABEL I
NILAI PADA *LIKELIHOOD*

Nilai	***Likelihood*** **Kriteria**	Deskripsi	Frekuensi Kejadian
1	*Rare*	Risiko sangat jarang sekali terjadi.	>2 tahun
2	*Unlikely*	Risiko jarang sekali terjadi.	1 - 2 tahun
3	*Possible*	Risiko cukup sering sekali terjadi.	7 - 12 bulan
4	*Likely*	Risiko sering sekali terjadi.	4 - 6 bulan
5	*Certain*	Risiko pasti selalu terjadi	1 - 3 bulan

Kemudian dilakukan tahap penilaian terhadap dampak (*Impact*) yang sering terjadi pada objek kasus terkait dengan kemungkinan risiko yang terjadi. Pada kriteria penilaian dampak atau *Impact* ini, dibedakan berdasarkan sejauh mana dampak tersebut akan mempengaruhi kinerja dari aplikasi CUPK Mobile. Table Nilai Kriteria *Impact* terdiri dari 5 kriteria yaitu : Sangat Rendah (*Insignificant*), Rendah (*Minor*), Sedang (*Moderate*), Besar (*Major*) dan Sangat Besar (*Catastrophic*).

TABEL II
NILAI PADA *IMPACT*

Nilai	***Impact*** **kriteria**	Deskripsi
1	*Insignificant*	Risiko tidak mengganggu aktifitas dan proses bisnis pada instasi.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 16-25

2	*Minor*	Aktivitas pada instansi sedikit terhambat, namun tidak mengganggu aktivitas inti pada instansi.
3	*Moderate*	Risiko tersebut mengganggu jalannya proses bisnis pada instansi, sehingga aktivitas bisnis sedikit terhambat.
4	*Major*	Risiko tersebut hampir menghambat seluruh jalannya proses bisnis pada instansi.
5	*Catastrophic*	Risiko hampir mengganggu semua jalannya proses bisnis dan menghentikan aktivitas instansi secara total.

3. Tahap Evaluasi Risiko (*Risk Evaluation*)

Evaluasi risiko merupakan proses penilaian risiko, dimana risiko akan dianalisisi dan dikelompokan berdasarkan tingkat risiko, mulai dari risiko terendah hingga risiko tertinggi[12]. Dalam proses ini, terdapat 3 tingkatan risiko (*Risk Level*), yaitu rendah (*Low*), Sedang (*Madium*), dan Tinggi (*High*). Kemungkinan risiko yang telah ditentukan nilai *Likehood* dan nilai *Impact* pada proses sebelumnya akan dibedakan Kembali dalam sebuat matriks yang ada[13]. Tujuan dari evaluasi risiko adalah untuk mendapatkan proses pengambilan keputusan terkait risiko berdasarkan hasil analisis risiko, sehingga dalam tahapan Perlakuan Risiko (*Risk Treatment*) akan mencantumkan satu atau lebih pilihan Tindakan untuk menanggulangi risiko yang telah diidentifikasi sehingga dapat memungkinkan penerapan penanganan risiko yang lebih efektif[14].

TABEL III
MATRIX EVALUASI RISIKO

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

B. Metode Pengambilan Data

Proses pengambilan data dilakukan dengan wawancara pada Deputi Pengembangan SDM dan Deputi Digital & IT di KSP ABC. Hasil dari wawancara ini bertujuan untuk mengetahui kendala serta masalah apa saja yang terus menerus terjadi pada aplikasi CUPK Mobile di Koperasi Simpan Pinjam ABC. Sehingga, dapat disimpulkan bagaimana *Risk Treatment* yang tepat digunakan untuk meminimalisir risiko pada aplikasi CUPK Mobile. Selain itu, penggaan metode observasi juga bertujuan untuk mengetahui secara langsung apa saja proses yang layak diterpkan dalam rancangan sistem yang akan dikerjakan[15].

III. HASIL DAN PEMBAHASAN

A. Identifikasi Risiko

1) Identifikasi Aset.

Pada tahap ini, dilakukan identifikasi aset-aset yang terkait dengan aplikasi CUPK Mobile yang melibatkan aset data, aset perangkat lunak (*Sotfware*), dan aset perangkat keras (*hardware*) yang terdapat pada aplikasi CUPK Mobile.

TABEL IV
IDENTIFIKASI ASET PADA APLIKASI CUPK MOBILE

Komponen TI/SI	Aset CUPK Mobile
Data	Data Anggota Pengguna
Software	Aplikasi CUPK Mobile
Hardware	Device (PC), Server Database dan Storage

Pada tabel 4 diatas menunjukkan aset-aset TI/SI yang dimiliki oleh KSP ABC yang terdiri dari data, software dan hardware. Dari tabel tersebut dapat dilihat ada berberapa aset penting yang terdapat pada aplikasi CUPK Mobile seperti data anggota pengguna, aplikasi CUPK Mobile dan Device (*PC*), server database dan storage.

2) Identifikasi Kemungkinan Risiko

Setelah dilakukan identifikasi aset pada aplikasi CUPK Mobile di Koperasi Simpan Pinjam ABC (KSP ABC), langkah selanjutnya adalah melakukan identifikasi kemungkinan risiko dengan melakukan pengelompokkan berdasarkan faktor-faktor yang sering muncul seperti pada faktor lingkungan atau alam, faktor SDM, serta faktor pada sistem dan Infrastruktur.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 16-25

TABEL V
IDENTIFIKASI KEMUNGKINAN RISIKO

Faktor	ID	Identifikasi Risiko
Alam dan Lingkungan	R01	Listrik Padam
	R02	Banjir
	R03	Kebakaran
Manusia	R04	Petir
	R05	*Human error*
	R06	Penyalah gunaan hak akses
	R07	*Vandalisme*
	R08	*Cybercrime*
Sistem dan Insfastruktur	R09	Kesalahan teknis
	R10	Overload
	R11	Overhead
	R12	Server Down
	R13	Serangan Virus
	R14	Mengalami Kegagalan pada *software*
	R15	Mengalami Kegagalan pada *Hardware*
	R16	Kegagalan Update
	R17	Memori penuh
	R18	Data corrupt
	R19	Koneksi jaringan tidak stabil
	R20	Web service tiba-tiba mati dan tidak berfungsi.
	R21	*Backup Failure*

Pada tabel 5 diatas menjelaskan faktor-faktor apa saja yang dapat menyebabkan terhambatnya proses bisnis pada aplikasi CUPK Mobile. Dari tabel tersebut telah teridentifikasi risiko yang berpontensi mengancam kelangsungan proses bisnis seperti dalam faktor alam dan lingkungan seperti kebakaran dan banjir yang dapat menyebabkan kerusakan pada insfrastruktur yang mendukung operasional aplikasi. Kemudian terdapat faktor yang disebabkan oleh manusia seperti kesalahan input data oleh pegawai dan serangan siber yang dilakukan anggota internal koperasi. Selanjutnya terdapat faktor sistem dan infrastruktur seperti koneksi jaringan tidak stabil, server *down* dan kerusakan pada perangkat keras yang dapat mengganggu operasional aplikasi.

3) Identifikasi Dampak

Setelah dilakukan tahap identifikasi risiko, maka ditemukan beberapa kemungkinan risiko yang dapat berpotensi untuk mengancam kinerja pada aplikasi CUPK Mobile, seperti faktor lingkungan, alam dan sistem infrastruktur. Oleh karena itu diperlukan analisis dampak yang dihasilkan dari risiko yang telah teridentifikasi.

TABEL VI
IDENTIFIKASI DAMPAK RISIKO

Id	Identifikasi Risiko	Dampak
R01	Listrik Padam	Seluruh Aktifitas di instansi akan terhenti.
R02	Banjir	Terjadinya kerusakan insfastruktur yang akan menghambat kinerja pada KSP ABC.
R03	Kebakaran	Terjadinya kebakaran pada insfatruktur di KSP ABC dapat mengakibatkan proses bisnis terhenti dan lembaga mengalami kerugian dalam segi keuangan.
R04	Petir	Mengalami kerusakan insfatruktur pada instansi dan kerugian dalam finansial.
R05	*Human error*	Proses layanan pada pengkodean tidak berjalan optimal.
R06	Penyalah gunaan hak akses	Mengakibatkan terjadi kebocoran informasi data
R07	*Vandalisme*	Dapat menyebabkan kerusakan pada perangkat keras serta perangkat lainnya
R08	*Cybercrime*	Dapat menyebabkan terjadinya manipulasi data dan pencurian data
R09	Kesalahan teknis	Perkerjaan menjadi terhambat
R10	Overload	Performa Hardware kurang optimal, karena rusaknya hardware di sebabkan oleh penggunaan suhu panas terus menerus
R11	Overhead	Data hilang dan proses loading terhambat yang disebabkan log database dan log temp yang telah mencapai kapasitas maksi-mum.
R12	Server Down	Kegagalan melakukan akses ke server di aplikasi CUPK Mobile
R13	Serangan Virus	Terjadi kehilangan data yang di sebabkan oleh serangan virus malware sehingga proses bisnis terganggu
R14	Mengalami Kegagalan pada *software*	Software tidak dapat beroperasi
R15	Mengalami Kegagalan pada *Hardware*	Hardware mengalami kerusakan serta tidak dapat berfungsi
R16	Kegagalan Update	Kegagalan dalam melakukan update aplikasi setelah dilakukan maintenance
R17	Memori penuh	Data tidak dapat tersimpan dalam komputer

Id	Identifikasi Risiko	Dampak
R18	Sistem crash	Kerusakan pada sistem yang menyebabkan aplikasi CUPK Mobile tidak dapat diakses dalam jangka waktu sementara
R19	Koneksi jaringan tidak stabil	Kegiatan dalam instansi yang memerlukan akses internet akan menjadi sangat lambat
R20	Web servis tiba-tiba mati dan tidak dapat berfungsi	*Customer service* tidak dapat mengakses aplikasi CUPK Mobile dan data tidak dapat di kirim ke rekening online.
R21	*Backup Failure*	Data yang diterima melalui rekening online tidak komprehensif atau tidak lengkap.

Pada tabel 6 dilakukan analisis dampak dari 21 identifikasi risiko yang telah ditemukan pada aplikasi CUPK Mobile, sehingga terdapat beberapa masalah serius yang dapat mengganggu sebagian aktivitas pada instansi, terutama pada KSP ABC. Kerusakan insfastruktur dapat menjadi hambatan kinerja operasional instansi seperti terjadinya kebakaran yang terjadi pada insfastruktur sehingga menyebabkan kerugian pada finansial bagi instansi. Selain masalah fisik terdapat juga ancaman keamanan informasi dan data serta kerusakan pada perangkat keras yang dapat menyebabkan kebocoran data sehingga dapat merugikan reputasi instansi dan membahayakan privasi pelanggan dan pengguna.

B. *Analisis Risiko*

Penilaian kemungkinan risiko berdasarkan pada tabel 1 (*kriteria Likelihood*) dan tabel 2 (*kriteria Impact*) akan dilakukan sebagai acuan dalam memberikan penilaian pada kemungkinan risiko yang telah teridentifikasi. Selanjutnya memberikan penilaian pada kemungkinan risiko berdasarkan dari tabel 1 dan 2.

TABEL VII
PENILAIAN *LIKELIHOOD* DAN *IMPACT*

Id	Identifikasi Risiko	*Likelihood*	*Impact*
R01	Listrik Padam	3	3
R02	Banjir	2	2
R03	Kebakaran	1	5
R04	Petir	3	2
R05	Human *error*	4	3
R06	Penyalah gunaan hak akses	2	2
R07	*Vandalisme*	1	2
R08	*Cybercrime*	2	3
R09	Kesalahan teknis	2	2
R10	Overload	3	2
R11	Overhead	2	4
R12	Server Down	2	4
R13	Serangan Virus	1	4
R14	Mengalami Kegagalan pada *software*	3	3
R15	Mengalami Kegagalan pada *Hardware*	3	2
R16	Kegagalan Update	3	2
R17	Memori penuh	1	2
R18	Sistem Crash	4	4
R19	Koneksi jaringan tidak stabil	4	4
R20	Web service tiba-tiba mati dan tidak berfungsi	4	4
R21	*Backup Failure*	3	4

Pada tabel 7 diatas menjelaskan penilaian *Likelihood* dan *Impact* dari 21 kemungkinan risiko yang telah dikelompokan berdasarkan seberapa berbahayanya risiko yang akan terjadi. Dari penilaian tersebut terdapat kategori angka dari 1-5 sesuai dengan seberapa berbahayanya risiko yang disebabkan sehingga dapat menghambat kinerja pada aplikasi CUPK Mobile. Beberapa risiko memiliki *Likelihood* yang relatif tinggi, seperti *human eror*, kegagalan update, listrik padam, petir dan mengalami kegagalan pada *software*, sehingga hal ini menunjukan bahwa terjadinya risiko yang cukup signifikan. Sedangkan, beberapa risiko pada *Impact* yang relative tinggi, seperti kebakaran, *overhead*, server *down*, serangan virus, sistem *cash*, koneksi jaringan tidak stabil dan web service tiba-tiba mati dan tidak berfungsi, sehingga risiko-risiko ini dapat memiliki dampak terhadap operasional sistem atau layanan yang terkait seperti aplikasi CUPK Mobile.

C. *Evaluasi Risiko*

Tahap terakhir dalam penilaian risiko (*Risk Assesment*) adalah tahap evaluasi risiko. Dalam tahap ini, menggunakan matriks risiko sebagai acuan untuk mengelompokan risiko berdasarkan level risiko atau *Risk Level*, dimulai dari tertinggi hingga terendah. Matriks risiko tersebut biasanya terdiri dari dua kreteria yaitu *Likelihood* dan *Impact*. Setiap ID dari kemungkinan risiko yang telah diidentifikasi akan dimasukan ke dalam matriks evaluasi

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 16-25

risiko sesuai dengan kriteria *Likelihood* dan *Impact* yang telah ditentukan. Dengan demikian, risiko dapat dikelompokkan berdasarkan tingkat keparahannya dan memudahkan untuk menentukan tindakan yang tepat untuk mengelola risiko tersebut. Pada tabel 3 digunakan untuk menjelaskan kriteria dan pengelompokan risiko pada matriks evaluasi risiko.

TABEL VIII
MATRIX EVALUASI RISIKO BERDASARKAN *LIKELIHOOD* DAN *IMPACT*

Likelihood						
	Certain	5				
	Likely	4			R05	R18, R19, R20
	Possible	3		R04, R10, R15, R16	R01, R14	R21
	Unlikely	2		R02, R06, R09	R08	R11, R12, R13
	Rare	1		R07, R17		
			1	2	3	4	5
	Impact		*Insignificant*	*Minor*	*Moderate*	*Major*	*Catastrophic*

Pada tabel 8 dilakukan perhitungan likehood dan impact terhadap 21 kemungkinan risiko. Risiko-risiko tersebut kemudian dikelompokan berdasarkan rasio. Selanjutnya, risiko-risiko tersebut akan dikelompokan dalam tingkat level tinggi (*high*), sedang (*medium*), dan rendah (*low*), sesuai dengan tingkat 21 kemungkinan risiko tersebut.

TABEL IX
PENGELOMPOKAN BERDASARKAN TINGKAT

ID	Identifikasi Risiko	*Likelihood*	*Impact*	*Risk Level*
R18	Sistem Crash	4	4	
R19	Koneksi jaringan tidak stabil	4	4	
R20	Web service tiba-tiba mati dan tidak berfungsi	4	4	
R05	Human *error*	4	3	
R21	*Backup Failure*	3	4	
R01	Listrik Padam	3	3	
R14	Mengalami Kegagalan pada *software*	3	3	
R04	Petir	3	2	
R10	Overload	3	2	
R15	Mengalami Kegagalan pada *Hardware*	3	2	
R16	Kegagalan Update	3	2	
R11	Overhead	2	4	
R12	Server Down	2	4	
R08	*Cybercrime*	2	3	
R02	Banjir	2	2	
R06	Penyalah gunaan hak akses	2	2	
R09	Kesalahan teknis	2	2	
R03	Kebakaran	1	5	
R13	Serangan Virus	1	4	
R07	*Vandalisme*	1	2	
R17	Memori penuh	1	2	

Hasil dari proses evaluasi risiko, ditemukan 21 kemungkinan risiko yang dikelompokkan berdasar besarnya risiko yang dapat menyebabkan terhambatnya proses bisnis pada aplikasi CUPK Mobile yaitu 4 risiko pada *level of risk* tingkat *high* seperti sistem *crash,* koneksi jaringan tidak stabil, web servis tiba-tiba mati dan tidak dapat berfungsi dan human *error*. Risiko dengan tingkat tinggi memerlukan tindakan pencegahan yang kuat dan pengawasan yang ketat. Kemudian 7 risiko pada *level of risk tingkat medium* seperti *backup failure*, listrik padam, mengalami kegagalan pada *software*, petir, *overload*, mengalami kegagalan pada *hardware* dan kegagalan update. Risiko dengan tingkat menengah memerlukan pemantauan dan penanganan yang tepat agar dampaknya dapat dikurangi. Serta 10 risiko pada *level of risk* tingkat *low* seperti *overhead*, server *down*, *cybercrime*, banjir, penyalah gunaan hak akses, kesalahan teknis, kebakaran, serangan virus, *vandalism*, dan memori penuh. Sehingga risiko dengan tingkat rendah tetap perlu diperhatikan dan dapat ditangani dengan langkah-langkah yang sesuai untuk mencegah terjadinya kerusakan pada sistem maupun pada insfastruktur di KSP ABC.

D. Perlakuan Risiko

Setelah dilakukan analisis risiko, maka langkah selanjutnya dilakukan tahap perlakuan risiko atau *Risk Treatment*. Pada tahapan ini, dilakukan pemberian rekomendasi mengenai perlakuan risiko yang telah dikelompokan pada kemungkinan risiko berdasarkan *risk level* yang sudah teridentifikasi dalam Aplikasi CUPK

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 16-25

Mobile. Tujuannya adalah untuk mengurangi risiko dan mencegah terjadinya kemungkinan risiko tersebut di masa depan.

TABEL X
USULAN PERLAKUAN RISIKO

ID	Identifikasi Risiko	*Risk Level*	Tindakan Risiko
R18	Sistem *Crash*		Mengelola tugas di *task manager* dengan cara menonaktifkan aplikasi yang tidak tidak terlalu penting dalam proses latar belakang (*Backgroud proses*).
R19	Koneksi jaringan tidak stabil		Ketika terjadi gangguan pada koneksi jaringan, segera laporkan ke departemen jaringan. Selain itu, lakukan pemeliharaan jaringan secara berkala diperusahaan.
R20	Web service tiba-tiba mati dan tidak berfungsi		Ketika layanan web mati, segera lakukan perbaikan. Selain itu, berikan pengumuman kepada pelanggan mengenai situasi yang sedang terjadi.
R05	*Human error*		Perlu dilakukan pelatihan dan pembinaan (*training, guidance, dan mentoring*) kepada karyawan baru. Membuat sistem manajemen pengetahuan (*Knowledge manajement system*) sebagai dokumentasi acuan bagi karyawan baru sehingga dapat menghindari kesalahan yang sama di masa depan
R21	*Backup Failure*		Memperhatikan penggunaan memori pada database agar tidak mencapai kapasitas maksimum. Membuat rencana pemeliharaan (*Maintenance plan*) yang tepat untuk memastikan kinerja database tetap optimal. Melakukan *backup* data secara berkala untuk mengindari kehilangan data akibat kegagalam sistem.
R01	Listrik Padam		Dalam mengantisipasi listrik padam, menyediakan generator set listrik yang sesuai dengan kebutuhan perusahan. Mempersiapkan *Ininterruptible Power Supply* (UPS) sebagai cadangan sementara sebelum generator set aktif.
R14	Mengalami Kegagalan pada *software*		Melakukan pemeriksaan terhadap driver, IRQ, atau sumber daya lainnya terlebih dahulu. Jika diperlukan, lakukan peninstalan ulang pada sistem operasi.
R04	Petir		Memindahkan server cadangan ke tempat yang berbeda. Menjalankan prosedur mirroring database untuk memastikan bahwa data tersedia di server cadangan. Memasang penangkal petir di area server untuk melindungi dari keusakan akibat sambaran petir.
R10	*Overload*		Lakukan refresh pada penggunaan log, temp, dan RAM yang digunakan oleh aplikasi CUPK Mobile secara berkala. Serta melakukan pemeriksaan pada database.
R15	Mengalami Kegagalan pada *Hardware*		Memberikan perawatan yang sesuai terhadap aset-aset hardware yang dimiliki oleh instansi. Serta membersihkan hardware secara rutin agar tidak terlalu banyak terakumulasi debu dan kotoran.
R16	Kegagalan Update		Setelah kesalahan ditemukan, segera melakukan perbaikan pada sistem.
R11	*Overhead*		Menjaga suhu ruangan tetap stabil, diperlukan ruangan yang cukup luas dan dilengkapi dengan mesin pendingin, serta melakukan servis pada AC secara rutin.
R12	Server *Down*		Melakukan pencadangan data secara rutin pada database utama instansi setiap harinya. Selain itu, perlu juga dilakukan pengurangan load server agar kinerja pada aplikasi CUPK Mobile tetap optimal.
R08	*Cybercrime*		Untuk melindungi data agar tetap aman, perlu dilakukan privasi data dengan menggunakan software keamanan yang selalu update. Menginstall sofware antivirus dan menggunakan fitur keamanan seperti layanan SLP/HTTPs pada website untuk memastikan kemanan saat bertransaksi online. Serta mengganti password secara berkala dan memasang CCTV di gedung perusahaan.
R02	Banjir		Mempersiapkan tempat yang lebih tinggi untuk menempatkan perangkat-perangkat yang digunakan oleh KSP ABC. Serta menerapkan teknik *miroring* database pada sistem database yang digunakan oleh aplikasi CUPK Mobile.
R06	Penyalah gunaan hak akses		Melakukan pemasangan CCTV di gedung perusahaan. Serta melakukan reset pada password secara berkala dan melakukan audit keamanan secara rutin.
R09	Kesalahan teknis		Membuat dan menjalankan SOP (*Standar Operating Procedur*) guna meningkatkan efisiensi dan efektivitas di tempat kerja.
R03	Kebakaran		Menyediakan alat pemadam kebakaran yang mudah ditemukan dan dijangkau di sekitar bangunan. Serta perusahaan harus merencanakan penyediaan infrastruktur cadangan, termasuk perangkat keras dan jaringan.
R13	Serangan Virus		Melakukan pemindaian antivirus pada perangkat portabel dan selalu mengaktifkan firewall serta keamanan internet.
R07	*Vandalisme*		Memasang CCTV di setiap sudut gedung perusahaan dan mengawasi setiap saat untuk meningkatkan keamanan.
R17	Memori penuh		Menambahkan kapasitas memori untuk meningkatkan daya tampung secara optimal dan melakukan pemeriksaan pada memori secara berkala.

Pada tabel 10 diatas memberikan rekomendasi perlakuan risiko yang dapat mengganggu jalannya proses bisnis, dengan memberikan rekomendasi pada risiko-risiko yang telah teridentifikasi di aplikasi CUPK Mobile. Tindakan-tindakan tersebut dapat dikategorikan menjadi beberapa aspek yang berhubungan dengan pengelolaan dan

pemeliharaan infrastruktur teknologi informasi. Pertama, terdapat langkah-langkah untuk memastikan ketersediaan dan keandalan jaringan dan layanan, seperti melaporkan gangguan koneksi, melakukan perbaikan saat layanan web mati, dan memperhatikan penggunaan memori database. Kedua, ada upaya dalam menjaga keberlanjutan operasional, seperti menyediakan sumber listrik cadangan, memastikan perawatan *hardware* yang baik, serta melakukan perbaikan setelah kesalahan ditemukan. Selanjutnya, terdapat langkah-langkah keamanan dan proteksi data, termasuk melindungi data dari serangan *cyber*, memasang CCTV untuk mencegah penyalahgunaan hak akses dan *vandalisme*, serta melindungi perangkat dari serangan virus. Terakhir, terdapat tindakan-tindakan untuk meningkatkan efisiensi dan pengoptimalan sistem, seperti meningkatkan kapasitas memori saat memori penuh. Penelitian ini memberikan konstribusi terhadap pemahaman dan praktek pengelolaan serta memberikan pemiliharaan infrastruktur teknologi informasi. Beberapa aspek yang dibahas, seperti langkah-langkah untuk memastikan ketersediaan dan keandalan jaringan dan layanan, menjaga keberlanjutan operasional, keamanan dan proteksi data, serta meningkatkan efisiensi dan pengoptimalan sistem, telah dikaji sebelumnya dalam penelitian terdahulu. Namun, hasil dari penelitian ini penekanan pengembangan solusi baru atau pendekatan yang lebih efektif dalam mengatasi risiko-risiko yang telah teridentifikasi. Meskipun beberapa langkah tersebut telah ditemukan dalam penelitian sebelumnya, penelitian ini memberikan wawasan tambahan dan mengikuti perkembangan teknologi terbaru untuk mencapai pengelolaan infrastruktur teknologi informasi yang lebih baik.

IV. KESIMPULAN

Tahap analisis manajemen risiko pada aplikasi CUPK Mobile di Koperasi Simpan Pinjam ABC yang berpedoman pada *International Organization for Standardization* (ISO 31000:2018) telah dilakukan. Proses analisis risiko yang dilakukan melalui 3 langkah dalam tahapan evaluasi risiko, yaitu *risk identification*, *risk analysis*, dan *risk evaluation*. Selanjutnya, dilakukan tahapan risk treatment untuk memberikan saran-saran tindakan yang perlu dilakukan untuk mengatasi kemungkinan risiko yang pada aplikasi CUPK Mobile. Hasil dari penelitian Analisis Manajemen Risiko menggunakan ISO 31000 yang telah dilakukan pada aplikasi CUPK Mobile di KSP ABC, yang terlah teridentifikasi ada 21 kemungkinan risiko yang dapat menghambat proses bisnis pada aplikasi CUPK Mobile di KSP ABC. Terdapat 4 kemungkinan risiko yang masuk ke dalam kategori risiko tinggi (*level of risk* tingkat *high*) pada aplikasi CUPK Mobile, yaitu sistem *crash*, koneksi jaringan tidak stabil, web service tiba-tiba mati dan tidak berfungsi, dan *human error*. Selanjutnya, terdapat 7 kemungkinan risiko yang masuk ke dalam kategori risiko sedang (*level of risk* tingkat *medium*), yaitu *backup failure*, listrik padam, kegagalam software, petir, *overload*, kegagalam hardware, dan kegagalan update. Terahkir, terdapat 10 kemungkinan risiko yang masuk ke dalam kategori risiko rendah (*level of risk* tingkat *low*), yaitu *overhead*, server *down*, *cybercrime*, banjir, penyalah gunaan hak akses, kesalahan teknis, kebakaran, serangan virus, *vandalisme*,dan memori penuh. Hasil penelitian ini diharapkan dapat memberikan panduan bagi KSP ABC dalam mengurangi kemungkinan risiko yang dapat terjadi akibat faktor-faktor yang telah teridentifikasi pada tabel 5. Dengan menerapkan rekomendasi perlakuan risiko yang diajukan, diharapkan organisasi dapat mengatasi risiko-risiko tersebut.

DAFTAR PUSTAKA

[1] M. Adhisyanda Aditya, R. Dicky Mulyana, A. Mulyawan, S. LIKMI Bandung, and S. Mardira Indonesia, "Perbandingan Cobit 2019 Dan Itil V4 Sebagai Panduan Tata Kelola Dan Management It," *J. Comput. Bisnis*, vol. 13, no. 2, pp. 100–105, 2019.

[2] 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.

[3] 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.

[4] Y. Erlika, M. I. Herdiansyah, and A. H. Mirza, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," *J. Ilm. Inform. Glob.*, vol. 11, no. 1, 2020, doi: 10.36982/jig.v11i1.1073.

[5] E. Muryanti and K. D. Hartomo, "Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, pp. 1265–1277, 2021, doi: 10.35957/jatisi.v8i3.948.

[6] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP," *J. SITECH Sist. Inf. dan Teknol.*, vol. 2, no. 1, pp. 13–20, 2019, doi: 10.24176/sitech.v2i1.3122.

[7] 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.

[8] G. G. Moleong and A. R. Tanaamah, "Analisis Risiko Teknologi Informasi Menggunakan Iso 31000 Pada Aplikasi Inlislite Di Dinas Kearsipan Dan Perpustakaan Provinsi Nusa Tenggara Timur," *JATI(Jurnal Mhs. Tek. Inform.*, vol. 6, no. 2, pp. 501–506, 2022, [Online]. Available: https://ejournal.itn.ac.id/index.php/jati/article/view/4840

[9] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.

[10] 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/sebatik.v23i1.441.

[11] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar

Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 2, pp. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[12] Fabiana Meijon Fadul, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *JUISI (Jurnal Inform. dan Sist. Informasi)*, vol. Vol. 02, N, 2019.

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

[14] W. Harefa, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 407–420, 2022, doi: 10.35957/jatisi.v9i1.1478.

[15] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 3, pp. 546–558, 2020, doi: 10.35957/jatisi.v7i3.525.