JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 2, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i2.9395

AUDIT KEAMANAN SISTEM INFORMASI DALAM MENDUKUNG AKTIVITAS TRANSAKSI PADA PLATFORM DEFI JUPITER SWAP MENGGUNAKAN FRAMEWORK COBIT 2019

Faisal Hidayat Sukma [1*], Nina Sulistio[2], Apriade Voutama[3]

[1,2,3]Universitas Singaperbangsa Karawang; Jl. HS. Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41361; 0267641177

Keywords:
Decentralized Finance;
Jupiter Swap;
COBIT 2019;
Keamanan Sistem Informasi.

Corespondent Email:
2310631250053@student.unsika.ac.id

Abstrak. Perkembangan decentralized finance (DeFi) mendorong perubahan signifikan dalam layanan keuangan berbasis blockchain, termasuk pada platform Jupiter Swap di jaringan Solana. Meskipun menawarkan efisiensi dan transparansi, sistem DeFi memiliki risiko keamanan yang tinggi akibat sifatnya yang terdesentralisasi dan kompleks. Oleh karena itu, penelitian ini bertujuan untuk menganalisis keamanan dan tata kelola sistem informasi pada Jupiter Swap menggunakan framework COBIT 2019. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif melalui observasi sistem, studi literatur, serta analisis menggunakan COBIT 2019 Design Toolkit yang mencakup enterprise strategy, enterprise goals, dan IT risk profile. Hasil penelitian menunjukkan bahwa sistem memiliki orientasi kuat pada inovasi dan transformasi digital, dengan dominasi domain BAI dan APO dalam tata kelola. Namun, profil risiko menunjukkan tingkat eksposur yang tinggi terhadap serangan siber, kesalahan pengguna, dan ketergantungan pada pihak ketiga. Selain itu, terdapat kesenjangan antara kondisi saat ini dan target capability level, terutama pada aspek keamanan dan pengelolaan perubahan sistem. Penelitian ini menunjukkan bahwa penerapan COBIT 2019 dapat membantu mengevaluasi dan meningkatkan tata kelola sistem DeFi secara lebih terstruktur dan adaptif.

Abstract. *The development of decentralized finance (DeFi) has significantly transformed blockchain-based financial services, including the Jupiter Swap platform on the Solana network. Despite offering efficiency and transparency, DeFi systems present high security risks due to their decentralized and complex nature. Therefore, this study aims to analyze the security and information system governance of Jupiter Swap using the COBIT 2019 framework. The research employs a descriptive qualitative approach through system observation, literature review, and analysis using the COBIT 2019 Design Toolkit, including enterprise strategy, enterprise goals, and IT risk profile. The results indicate that the system strongly emphasizes innovation and digital transformation, with governance dominated by the BAI and APO domains. However, the risk profile reveals high exposure to cyber attacks, user errors, and third-party dependencies. Additionally, a gap exists between the current condition and the target capability level, particularly in security and system change management. This study demonstrates that COBIT 2019 can be effectively applied to evaluate and improve governance in DeFi systems in a structured and adaptive manner.*

1. PENDAHULUAN

Perkembangan teknologi informasi dalam beberapa dekade terakhir telah membawa perubahan yang signifikan pada berbagai sektor industri maupun pribadi, termasuk sektor keuangan [1]. Transformasi digital yang terjadi mendorong munculnya berbagai layanan keuangan berbasis teknologi atau yang dikenal sebagai *financial technology* (*fintech*) [1]. Layanan ini memungkinkan proses transaksi keuangan dilakukan secara lebih cepat, efisien, dan mudah diakses oleh masyarakat luas melalui perangkat digital seperti komputer maupun smartphone [1]. Dengan adanya teknologi ini, layanan keuangan tidak hanya mengubah cara transaksi dilakukan, tetapi juga mengubah model bisnis menjadi lebih praktis dan optimal.

Perkembangan teknologi blockchain turut melahirkan inovasi baru dalam sektor layanan keuangan yang dikenal dengan istilah *decentralized finance* (*DeFi*) [2],[3]. DeFi merupakan sistem keuangan yang beroperasi di atas jaringan blockchain yang dimana pengguna bisa melakukan berbagai transaksi tanpa harus melalui perantara terpusat, seperti bank konvensional maupun institusi keuangan tradisional [2],[3]. Sistem ini memanfaatkan teknologi *smart contract*, yaitu protokol atau program komputer yang tersimpan di atas blockchain, yang secara otomatis mengeksekusi perjanjian tanpa perantara ketika kondisi yang telah ditentukan terpenuhi [4]. Melalui mekanisme tersebut, transaksi dapat berlangsung secara langsung antar pengguna secara transparan serta tanpa campur tangan pihak ketiga sebagai pengelola dana.

Salah satu jaringan blockchain yang banyak diminati oleh pengguna dalam mendukung pengembangan aplikasi DeFi adalah Solana [5]. Jaringan ini dikenal memiliki kemampuan untuk memproses transaksi dengan kecepatan tinggi, dengan menggunakan mekanisme konsensus *Proof of History* (*PoH*) yang dikombinasikan dengan *Proof of Stake* (*PoS*), memungkinkan throughput ribuan transaksi per detik dengan latensi rendah [5]. Keunggulan tersebut membuat Solana banyak dimanfaatkan oleh banyak pengguna sebagai platform untuk melakukan berbagai layanan keuangan terdesentralisasi, seperti pertukaran aset kripto, penyediaan likuiditas, hingga beragam layanan keuangan digital lainnya.

Di dalam ekosistem Solana, terdapat berbagai platform DeFi yang menyediakan layanan pertukaran aset digital melalui mekanisme *decentralized exchange* (*DEX*) [2]. Salah satu platform DeFi yang cukup populer adalah Jupiter, yang berfungsi sebagai agregator DEX. Platform ini menggabungkan berbagai sumber likuiditas dari beberapa protokol pertukaran aset yang tersedia di jaringan Solana untuk memberikan rute transaksi terbaik bagi pengguna saat melakukan pertukaran token. Dengan adanya sistem agregasi tersebut, membuat pengguna memperoleh harga transaksi yang lebih efisien dibandingkan jika menggunakan satu platform pertukaran saja.

Walaupun DeFi menawarkan berbagai keunggulan, seperti transparansi transaksi, kemudahan akses layanan, serta efisiensi biaya operasional, penggunaan teknologi ini tetap memiliki sejumlah risiko yang perlu diperhatikan, terutama yang berkaitan dengan keamanan aplikasi serta integrasi sistem [2],[3]. Risiko tersebut dapat muncul akibat kerentanan pada aplikasi, kesalahan integrasi dengan *smart contract*, maupun potensi gangguan dalam proses eksekusi transaksi [6],[7],[8]. Selain itu, kompleksitas mekanisme transaksi pada platform berbasis blockchain dapat meningkatkan kemungkinan kesalahan penggunaan oleh pengguna. Berbeda dengan sistem keuangan konvensional yang memiliki mekanisme perlindungan konsumen melalui lembaga pengawas atau institusi keuangan, pada sistem DeFi tanggung jawab transaksi sebagian besar berada pada pengguna itu sendiri.

Salah satu aspek yang perlu mendapat perhatian dalam penggunaan platform DeFi adalah keamanan aplikasi yang digunakan sebagai penghubung antara pengguna dan jaringan blockchain [9]. Aplikasi ini menjadi sarana utama bagi pengguna untuk melakukan transaksi, menghubungkan dompet digital (*wallet*), serta mengirimkan instruksi transaksi ke jaringan blockchain. Apabila terdapat celah keamanan pada aplikasi tersebut, maka potensi manipulasi transaksi, kesalahan eksekusi, maupun penyalahgunaan akses dapat terjadi

dan berisiko menimbulkan kerugian bagi pengguna [6]. Oleh karena itu, keamanan aplikasi memegang peranan penting dalam memastikan proses transaksi dapat berjalan dengan aman dan dapat dipercaya [10].

Selain faktor keamanan, penyajian informasi transaksi pada aplikasi juga menjadi hal yang penting untuk diperhatikan. Informasi yang kurang jelas, proses validasi transaksi yang tidak optimal, ataupun tampilan antarmuka yang kurang informatif dapat meningkatkan kemungkinan terjadinya kesalahan transaksi oleh pengguna. Dalam ekosistem DeFi, transaksi yang telah diproses umumnya tidak dapat dibatalkan karena seluruh data transaksi tersimpan secara permanen pada jaringan blockchain [3]. Kondisi ini menyebabkan setiap kesalahan transaksi berpotensi menimbulkan kerugian yang tidak dapat diperbaiki.

Dalam konteks tersebut, audit sistem informasi dapat digunakan untuk mengevaluasi tingkat keamanan serta tata kelola teknologi informasi yang mendukung operasional platform DeFi [11]. Salah satu kerangka kerja yang umum digunakan dalam audit tata kelola teknologi informasi adalah COBIT, yang menyediakan pedoman untuk menilai efektivitas pengendalian, manajemen risiko, serta keselarasan antara teknologi informasi dan tujuan organisasi [12]. Audit sistem informasi bertujuan untuk menilai efektivitas pengendalian sistem, mengidentifikasi potensi kerentanan keamanan, serta memberikan rekomendasi perbaikan guna meningkatkan kualitas sistem teknologi informasi yang digunakan.

Penelitian ini difokuskan pada analisis keamanan dan tata kelola sistem informasi pada platform Jupiter yang beroperasi di jaringan Solana dengan menggunakan pendekatan audit COBIT 2019. Proses evaluasi dilakukan melalui studi literatur serta analisis sistem berdasarkan dokumentasi platform dan observasi terhadap mekanisme transaksi yang tersedia bagi pengguna. Melalui pendekatan tersebut, penelitian ini berupaya mengidentifikasi potensi risiko keamanan sekaligus memberikan rekomendasi perbaikan guna meningkatkan perlindungan aplikasi dalam mendukung aktivitas transaksi pada layanan keuangan terdesentralisasi.

Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam memperluas pemahaman mengenai penerapan audit sistem informasi pada platform DeFi, khususnya terkait aspek keamanan aplikasi. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi bagi pengguna maupun pengembang layanan keuangan digital dalam meningkatkan kualitas keamanan sistem, sehingga perkembangan ekosistem keuangan digital dapat berlangsung dengan lebih aman dan terpercaya di masa mendatang.

2. TINJAUAN PUSTAKA

2.1 Decentralized Finance (DeFi)

Decentralized finance (DeFi) merupakan sistem layanan keuangan yang dibangun di atas teknologi blockchain dan memungkinkan pengguna melakukan transaksi tanpa perantara terpusat seperti bank atau lembaga keuangan tradisional [2],[3]. Sistem ini memanfaatkan smart contract untuk mengeksekusi transaksi secara otomatis berdasarkan kondisi yang telah ditentukan. Dengan karakteristik yang terbuka, transparan, dan non-custodial, DeFi memberikan fleksibilitas tinggi bagi pengguna dalam mengelola aset digital. Namun demikian, sifat sistem yang terdesentralisasi juga menyebabkan tanggung jawab keamanan berada pada pengguna, sehingga meningkatkan potensi risiko dalam proses transaksi.

2.2 Keamanan Sistem pada Platform DeFi

Keamanan merupakan aspek krusial dalam sistem DeFi, terutama karena transaksi yang telah dieksekusi pada blockchain bersifat permanen dan tidak dapat dibatalkan [6]. Beberapa risiko yang umum terjadi meliputi serangan phishing, eksploitasi smart contract, kesalahan dalam proses persetujuan transaksi, serta interaksi dengan aset digital yang tidak valid [4],[7]. Selain itu, kompleksitas mekanisme transaksi dan integrasi dengan berbagai protokol juga dapat meningkatkan kemungkinan kesalahan penggunaan oleh pengguna. Oleh karena itu, diperlukan mekanisme pengamanan yang mampu memastikan transparansi informasi serta validasi transaksi sebelum proses eksekusi dilakukan.

2.3 Audit Sistem Informasi

Audit sistem informasi merupakan proses evaluasi terhadap sistem teknologi informasi untuk menilai efektivitas pengendalian, keamanan, serta kesesuaian sistem dengan tujuan organisasi [11]. Dalam konteks sistem berbasis blockchain, audit tidak hanya berfokus pada infrastruktur teknis, tetapi juga pada bagaimana sistem digunakan oleh pengguna serta bagaimana mekanisme kontrol diterapkan dalam proses transaksi. Audit sistem informasi bertujuan untuk mengidentifikasi potensi risiko, mengevaluasi kelemahan sistem, serta memberikan rekomendasi perbaikan guna meningkatkan kualitas dan keandalan sistem [13].

2.4 Framework COBIT 2019

COBIT 2019 merupakan framework tata kelola teknologi informasi yang dikembangkan oleh ISACA untuk membantu organisasi dalam mengelola dan mengendalikan sistem teknologi informasi secara efektif [12]. Framework ini menyediakan pendekatan yang sistematis dalam menghubungkan tujuan bisnis dengan pengelolaan teknologi informasi melalui berbagai domain tata kelola [14].

2.5 Penilaian Risiko (Risk Assessment)

Penilaian risiko merupakan metode yang digunakan untuk mengidentifikasi dan mengukur tingkat risiko yang terdapat dalam suatu sistem [11]. Dalam penelitian ini, tingkat risiko dihitung menggunakan pendekatan probabilitas dan dampak dengan persamaan:

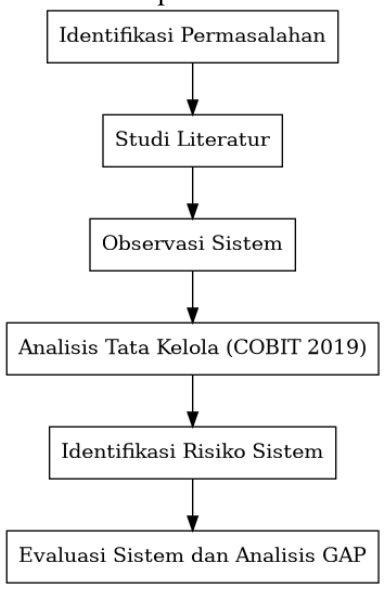
$$R = P \times L$$

di mana R merupakan tingkat risiko, P adalah probabilitas terjadinya risiko, dan I adalah dampak yang ditimbulkan [15]. Hasil penilaian risiko digunakan sebagai dasar dalam menyusun IT risk profile pada framework COBIT 2019, sehingga dapat mendukung proses evaluasi tata kelola teknologi informasi secara lebih terstruktur.

3. METODE PENELITIAN

3.1. Jenis dan Tahapan Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode analisis sistem informasi. Pendekatan ini dipilih karena penelitian bertujuan untuk memahami serta mengevaluasi aspek keamanan dan tata kelola sistem informasi pada platform decentralized finance (DeFi), khususnya pada fitur Jupiter Swap yang terdapat pada platform Jupiter Aggregator yang beroperasi di jaringan blockchain Solana. Pendekatan kualitatif deskriptif digunakan untuk menggambarkan kondisi sistem, mekanisme transaksi, serta potensi risiko keamanan yang terdapat pada platform tersebut. Penelitian tidak melakukan pengujian langsung terhadap infrastruktur internal platform, melainkan melakukan analisis berdasarkan mekanisme sistem yang dapat diamati dari sisi pengguna serta informasi yang tersedia secara publik



Gambar 3.1 Flowchart Tahapan Penelitian

Dalam penelitian ini, proses penelitian dilakukan melalui beberapa tahapan sebagai berikut:

1. Identifikasi Permasalahan**:** Tahap awal penelitian dilakukan dengan mengidentifikasi permasalahan yang berkaitan dengan keamanan dan tata kelola sistem informasi pada platform DeFi. Pada tahap ini peneliti mengkaji berbagai fenomena yang berkaitan dengan penggunaan layanan keuangan terdesentralisasi, seperti potensi kerentanan keamanan aplikasi, risiko kesalahan transaksi oleh pengguna, serta kompleksitas mekanisme transaksi yang terdapat pada sistem berbasis blockchain.
2. Studi Literatur**:** Setelah permasalahan penelitian ditentukan, tahap selanjutnya adalah melakukan studi literatur untuk

memperoleh landasan teoritis yang relevan dengan topik penelitian. Studi literatur dilakukan dengan mengkaji berbagai sumber referensi seperti jurnal ilmiah, buku akademik, artikel penelitian, serta dokumentasi resmi yang berkaitan dengan teknologi blockchain, *decentralized finance* (DeFi), keamanan sistem informasi, dan audit teknologi informasi menggunakan framework COBIT 2019.

3. Observasi Sistem**:** Tahap berikutnya adalah melakukan observasi terhadap sistem yang menjadi objek penelitian. Observasi dilakukan dengan mengamati secara langsung mekanisme penggunaan fitur Jupiter Swap pada platform Jupiter Aggregator dari perspektif pengguna. Proses observasi meliputi aktivitas seperti mengakses antarmuka aplikasi, menghubungkan dompet digital (*wallet*), serta mengamati alur proses pertukaran token (*token swap*) yang terjadi pada platform.
4. Analisis Sistem Menggunakan Design Factor COBIT 2019**:** Setelah proses observasi dilakukan, tahap selanjutnya adalah melakukan analisis sistem menggunakan kerangka kerja COBIT 2019. Analisis ini bertujuan untuk mengevaluasi aspek keamanan serta tata kelola teknologi informasi yang mendukung operasional platform. Proses analisis dilakukan dengan mengaitkan mekanisme sistem yang diamati dengan *design factor* yang terdapat dalam framework COBIT.
5. Identifikasi Risiko Sistem**:** Pada tahap ini dilakukan identifikasi berbagai potensi risiko yang dapat muncul dalam penggunaan platform DeFi, khususnya pada fitur Jupiter Swap. Risiko yang dianalisis meliputi potensi serangan keamanan, kesalahan dalam proses persetujuan transaksi, serta kompleksitas mekanisme sistem yang dapat mempengaruhi keamanan pengguna.
6. Evaluasi Sistem dan Analisis GAP: Tahap ini dilakukan dengan mengevaluasi hasil analisis tata kelola sistem informasi dengan membandingkan kondisi saat ini terhadap target capability level yang telah ditetapkan berdasarkan framework COBIT 2019. Proses ini bertujuan untuk mengidentifikasi kesenjangan (gap) pada aspek perubahan sistem, konfigurasi, keamanan, dan kontrol operasional, sehingga dapat diketahui area tata kelola yang masih perlu ditingkatkan.

3.2. Teknik Analisis Data

Teknik analisis data dalam penelitian ini dilakukan secara deskriptif dengan menginterpretasikan data yang diperoleh dari hasil studi literatur serta observasi terhadap mekanisme sistem pada fitur Jupiter Swap pada platform Jupiter Aggregator. Data tersebut dianalisis menggunakan pendekatan COBIT 2019 Design Toolkit untuk mengevaluasi kebutuhan tata kelola teknologi informasi pada sistem yang diteliti.

Proses analisis dilakukan melalui identifikasi design factor yang meliputi enterprise strategy, enterprise goals, dan IT risk profile. Ketiga faktor tersebut digunakan untuk menggambarkan karakteristik sistem DeFi yang dianalisis, termasuk orientasi strategis layanan, tujuan utama sistem, serta profil risiko teknologi informasi yang dihadapi. Khusus pada IT risk profile, penilaian dilakukan dengan pendekatan risk assessment menggunakan perhitungan probabilitas dan dampak risiko.

Hasil analisis design factor selanjutnya digunakan untuk menentukan governance objectives priority, menetapkan target capability level, serta melakukan analisis gap antara kondisi saat ini dan kondisi yang diharapkan. Dengan pendekatan tersebut, analisis tidak hanya menghasilkan gambaran mengenai tingkat risiko dan kebutuhan tata kelola, tetapi juga menunjukkan area pengelolaan sistem yang perlu diperkuat agar keamanan dan tata kelola teknologi informasi pada platform Jupiter Swap dapat berjalan lebih efektif.

3.3. Objek Penelitian

Objek penelitian dalam studi ini adalah fitur Jupiter Swap yang terdapat pada platform Jupiter Aggregator yang beroperasi di jaringan blockchain Solana. Jupiter Swap merupakan layanan pertukaran aset kripto (*token swap*)

yang memungkinkan pengguna menukar satu aset digital dengan aset lainnya melalui mekanisme agregasi likuiditas dari berbagai *decentralized exchange* (DEX) yang terhubung dalam ekosistem Solana.

Fitur Jupiter Swap bekerja dengan cara menganalisis berbagai sumber likuiditas yang tersedia pada beberapa protokol pertukaran aset digital untuk menentukan rute transaksi (*routing*) yang paling optimal bagi pengguna. Melalui mekanisme tersebut, sistem secara otomatis memilih jalur transaksi yang memberikan harga pertukaran terbaik dengan mempertimbangkan faktor seperti likuiditas pasar, biaya transaksi, serta efisiensi rute perdagangan.

Dalam penelitian ini, fokus analisis diarahkan pada mekanisme keamanan serta tata kelola sistem informasi yang mendukung aktivitas transaksi pada fitur Jupiter Swap. Beberapa aspek yang diamati meliputi proses koneksi dompet digital (*wallet*), mekanisme pemilihan pasangan token, penyajian informasi transaksi sebelum persetujuan (*transaction preview*), serta proses otorisasi transaksi melalui tanda tangan digital pada dompet pengguna. Analisis terhadap aspek-aspek tersebut dilakukan untuk mengevaluasi potensi risiko keamanan serta efektivitas mekanisme pengendalian sistem dalam mendukung aktivitas transaksi pada platform DeFi.

3.4. Kerangka Kerja Audit

Penelitian ini menggunakan framework COBIT 2019 sebagai kerangka kerja dalam melakukan analisis keamanan dan tata kelola sistem informasi pada fitur Jupiter Swap yang terdapat pada platform Jupiter Aggregator di jaringan blockchain Solana. COBIT 2019 merupakan kerangka kerja tata kelola dan manajemen teknologi informasi yang dikembangkan oleh ISACA dan digunakan secara luas untuk mengevaluasi efektivitas pengelolaan teknologi informasi serta pengendalian sistem dalam suatu organisasi.

Framework COBIT menyediakan seperangkat praktik terbaik yang dapat digunakan untuk menilai bagaimana sistem teknologi informasi dikelola, dipantau, serta dikendalikan agar dapat mendukung tujuan organisasi secara efektif. Dalam konteks penelitian ini, COBIT digunakan untuk mengevaluasi mekanisme keamanan aplikasi yang mendukung aktivitas transaksi pada platform DeFi, khususnya pada proses pertukaran aset digital (token swap).

Dalam penelitian ini, pendekatan yang digunakan adalah COBIT 2019 Design Toolkit, yang berfokus pada analisis design factor untuk menentukan prioritas tata kelola sistem. Design factor yang digunakan meliputi enterprise strategy, enterprise goals, dan IT risk profile.

Hasil dari analisis design factor digunakan untuk menentukan governance objectives yang relevan, serta menetapkan target capability level dan melakukan analisis kesenjangan (gap) antara kondisi saat ini dan kondisi yang diharapkan.

3.5. Model Penilaian Risiko

Dalam penelitian ini, proses evaluasi keamanan sistem dilakukan dengan menggunakan pendekatan penilaian risiko (risk assessment). Penilaian risiko digunakan untuk mengidentifikasi serta mengukur tingkat risiko yang dapat muncul pada aktivitas transaksi pengguna pada fitur Jupiter Swap. Pendekatan ini mempertimbangkan dua komponen utama yaitu probabilitas terjadinya risiko dan dampak yang ditimbulkan oleh risiko tersebut terhadap pengguna.

Tingkat risiko dihitung menggunakan persamaan berikut:

$$R = P \times I$$

Keterangan:

Simbol	Keterangan
R	Tingkat risiko
P	Probabilitas risiko
I	Dampak risiko

Tabel 1 *Risk Formula*

3.6 Analisis Design Factor COBIT 2019

Analisis tata kelola dalam penelitian ini menggunakan pendekatan COBIT 2019 Design Factors untuk menentukan prioritas tata kelola sistem.

Design Factor	Deskripsi
Enterprise Strategy	Strategi utama sistem dalam menyediakan layanan DeFi
Enterprise Goals	Tujuan organisasi dalam pengembangan layanan

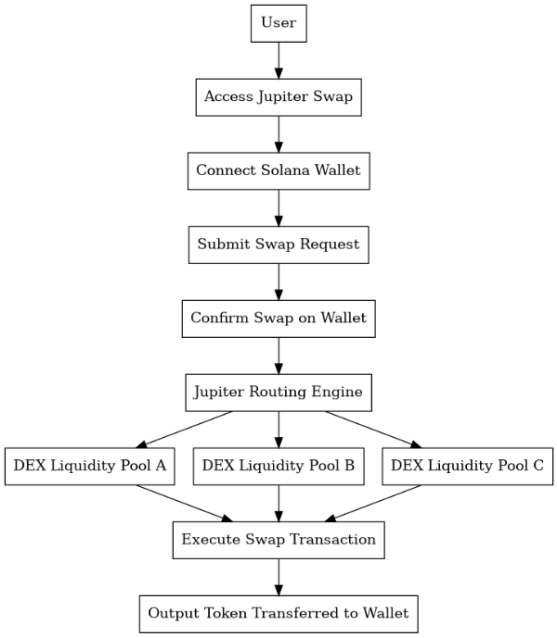
Design Factor	Deskripsi
IT Risk Profile	Profil risiko teknologi informasi yang dihadapi sistem

Tabel 2 *Design Factor*

4. HASIL DAN PEMBAHASAN

4.1. Gambaran Sistem Jupiter Swap

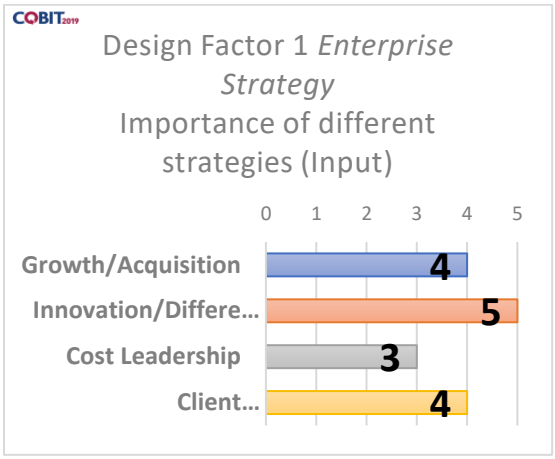
Jupiter Swap merupakan layanan pertukaran aset digital yang beroperasi pada jaringan blockchain Solana dan berfungsi sebagai agregator likuiditas dari berbagai protokol decentralized exchange. Sistem ini memungkinkan pengguna melakukan transaksi pertukaran token dengan memanfaatkan jalur likuiditas yang paling efisien.



Gambar 4.1 Diagram Alur Cara Kerja Jupiter Swap

4.2 Analisis Design Factor

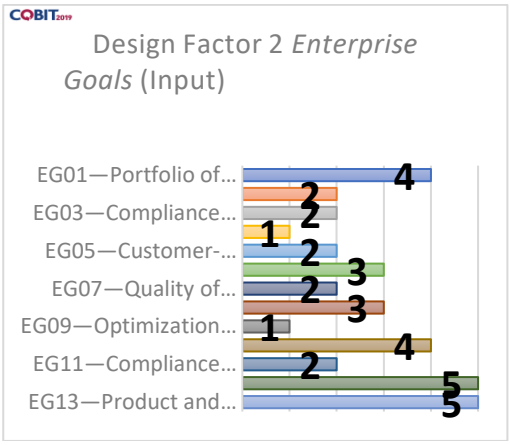
4.2.1. Enterprise Strategy



Gambar 4.2.1 Hasil Penilaian *Enterprise Strategy*

Hasil analisis menunjukkan bahwa strategi Jupiter Swap didominasi oleh inovasi dan diferensiasi layanan, terutama melalui penggunaan agregasi likuiditas dan *routing engine* untuk mendapatkan harga transaksi terbaik. Selain itu, aspek pertumbuhan pengguna dan kualitas layanan juga cukup diperhatikan untuk menjaga pengalaman pengguna dalam ekosistem DeFi. Sementara itu, efisiensi biaya tidak menjadi fokus utama karena biaya transaksi lebih banyak dipengaruhi oleh kondisi jaringan dan likuiditas pasar, sehingga strategi sistem secara keseluruhan lebih berorientasi pada pengembangan teknologi dan peningkatan kualitas layanan.

4.2.2. Enterprise Goals



Gambar 4.2.2 *Design Factor* COBIT

Berdasarkan hasil penilaian, tujuan utama sistem berfokus pada transformasi digital dan inovasi produk, yang mencerminkan karakter platform DeFi yang dinamis dan berbasis

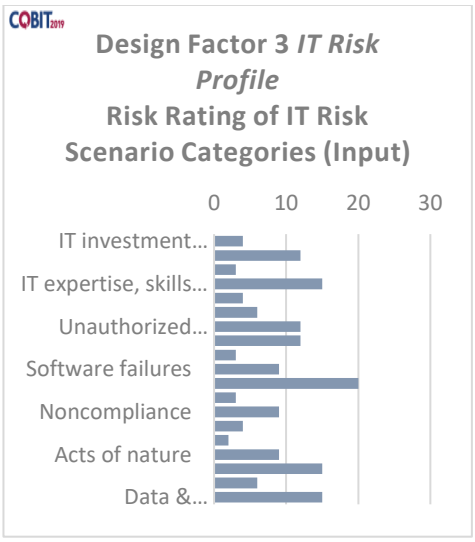
teknologi. Selain itu, tujuan seperti penyediaan layanan yang kompetitif dan efisiensi proses transaksi juga cukup menonjol, menunjukkan bahwa sistem dirancang untuk memberikan pengalaman transaksi yang optimal. Di sisi lain, tujuan seperti kualitas informasi keuangan dan optimalisasi biaya operasional memiliki prioritas lebih rendah karena sistem tidak beroperasi sebagai lembaga keuangan tradisional, melainkan sebagai platform teknologi berbasis *blockchain.*

4.2.3. IT Risk Profile

Risiko	P	I	R	Kategori
Phishing domain (website palsu)	2	3	6	Tinggi
Kesalahan approval transaksi	2	3	6	Tinggi
Interaksi dengan token scam	1	3	3	Sedang
Kesalahan parameter slippage	2	2	4	Sedang
Kompleksitas routing transaksi	1	2	2	Rendah

Tabel 3 Hasil Perhitungan Risiko Sistem

Hasil perhitungan risiko ini digunakan sebagai dasar dalam menentukan nilai pada kategori IT Risk Profile menggunakan pendekatan COBIT 2019. Nilai risiko yang diperoleh selanjutnya dikonversi ke dalam skala penilaian COBIT (0–20) dengan mempertimbangkan tingkat eksposur dan relevansi masing-masing kategori risiko terhadap sistem DeFi.



Gambar 4.2.3 Hasil *IT Risk Profile*

Profil risiko menunjukkan bahwa ancaman terbesar berada pada *logical attacks*, seperti peretasan, eksploitasi *smart contract*, dan *phishing*, yang umum terjadi pada sistem DeFi. Selain itu, risiko juga muncul dari kompleksitas penggunaan sistem, termasuk potensi kesalahan pengguna dalam memahami mekanisme transaksi. Faktor lain yang cukup signifikan adalah ketergantungan terhadap pihak ketiga, seperti *wallet* dan protokol likuiditas, yang dapat menambah potensi kerentanan. Secara keseluruhan, risiko pada sistem tidak hanya berasal dari aspek teknis, tetapi juga dari interaksi pengguna serta karakter ekosistem DeFi yang terbuka.

4.3 Governance Objectives Priority

Berdasarkan hasil pemetaan design factor yang meliputi enterprise strategy, enterprise goals, dan IT risk profile, diperoleh sejumlah governance objectives yang memiliki tingkat prioritas tinggi dalam mendukung tata kelola sistem pada Jupiter Swap[16][17].

Adapun governance objectives yang menjadi prioritas utama adalah sebagai berikut:

Code	Governance Objective
BAI06	Managed IT Changes
BAI10	Managed Configuration
APO03	Managed Enterprise Architecture
APO04	Managed Innovation
DSS06	Managed Business Process Controls
APO13	Managed Security
DSS02	Managed Service Requests and Incidents

Tabel 4 Prioritas *Governance Objectives* COBIT 2019

Secara khusus, domain APO menjadi dominan dalam hasil analisis, yang menunjukkan bahwa kebutuhan utama sistem Jupiter Swap berfokus pada aspek perencanaan, arsitektur, inovasi, dan keamanan teknologi informasi. Hal ini sejalan dengan karakteristik platform DeFi yang berbasis inovasi dan pengembangan teknologi, di mana pengelolaan arsitektur sistem (APO03), inovasi layanan (APO04), serta keamanan informasi (APO13) menjadi faktor kunci dalam menjaga keberlangsungan sistem.

Sementara itu, domain BAI tetap memiliki peran penting dalam mendukung implementasi teknis, khususnya dalam pengelolaan perubahan (BAI06) dan konfigurasi sistem (BAI10), yang berkaitan langsung dengan stabilitas operasional dan integrasi protokol likuiditas pada platform.

4.4 Target Capability Level

Berdasarkan prioritas governance objectives yang telah diidentifikasi, tahap selanjutnya adalah menentukan target capability level yang diharapkan untuk masing-masing objective.

Code	Governance Objective	Target Level
BAI06	Managed IT Changes	4
BAI10	Managed Configuration	4
APO03	Managed Enterprise Architecture	4
APO04	Managed Innovation	4
DSS06	Managed Business Process Controls	3
APO13	Managed Security	4
DSS02	Managed Service Requests and Incidents	3

Tabel 5 *Target Capability Level*

Penetapan target capability level menunjukkan bahwa sebagian besar objective berada pada level 4 (predictable process). Hal ini mengindikasikan bahwa sistem diharapkan memiliki proses yang terstandarisasi, terdokumentasi, serta dapat diprediksi dalam mendukung aktivitas transaksi.

Objective seperti BAI06 dan BAI10 ditetapkan pada level tinggi karena perubahan sistem dan konfigurasi memiliki dampak langsung terhadap keamanan serta keandalan transaksi pada platform DeFi. Selain itu, APO03 dan APO04 juga memiliki target tinggi karena arsitektur sistem dan inovasi teknologi merupakan komponen utama dalam pengembangan layanan Jupiter Swap.

Sementara itu, objective seperti DSS06 dan DSS02 berada pada level 3 (defined process), yang menunjukkan bahwa proses operasional sudah terdokumentasi dengan baik, namun belum sepenuhnya terukur secara kuantitatif.

4.5 GAP Governance Analysis

Code	Current	Target	GAP
BAI06	2	4	2
BAI10	2	4	2
APO03	3	4	1
APO04	3	4	1
DSS06	2	3	1
APO13	2	4	2
DSS02	2	3	1

Tabel 6 Hasil Analisis GAP Tata Kelola

Hasil analisis menunjukkan adanya kesenjangan pada beberapa objective utama, terutama pada **BAI06**, **BAI10**, dan **APO13** yang memiliki GAP sebesar 2. Hal ini menunjukkan bahwa pengelolaan perubahan sistem, konfigurasi, serta keamanan masih perlu ditingkatkan agar mencapai tingkat tata kelola yang lebih optimal.

Sementara itu, objective lain seperti **APO03**, **APO04**, dan **DSS06** memiliki GAP yang lebih kecil, yang menunjukkan bahwa sistem telah memiliki dasar pengelolaan yang cukup baik, namun masih memerlukan penyempurnaan dalam aspek standardisasi dan pengukuran kinerja.

5. KESIMPULAN

Berdasarkan analisis menggunakan *framework* COBIT 2019, tata kelola teknologi informasi pada Jupiter Swap menunjukkan orientasi kuat pada inovasi dan transformasi digital, dengan dominasi oleh *governance objectives* pada domain BAI dan APO yang menekankan pengelolaan perubahan sistem, konfigurasi, dan arsitektur teknologi, serta dukungan DSS dalam kontrol operasional transaksi. Di sisi lain, profil risiko menunjukkan eksposur tinggi terhadap *logical attacks*, kompleksitas penggunaan, dan ketergantungan pada pihak ketiga, yang menegaskan bahwa tantangan utama tidak hanya bersifat teknis tetapi juga berasal dari interaksi pengguna dan karakter ekosistem DeFi. Hasil *gap analysis* juga menunjukkan masih adanya kesenjangan pada aspek perubahan sistem, keamanan, dan konfigurasi, sehingga diperlukan penguatan kontrol dan tata kelola yang lebih terstruktur. Secara keseluruhan, COBIT 2019 dapat diterapkan untuk mengevaluasi tata kelola sistem berbasis *blockchain*, dengan

penyesuaian terhadap sifatnya yang terdesentralisasi dan dinamis.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Apriade Voutama dan Ibu Nina Sulistiyowati selaku dosen pengampu yang telah memberikan bimbingan, arahan, serta dukungan dalam proses penyusunan penelitian ini. Ucapan terima kasih juga disampaikan kepada kedua orang tua penulis atas doa, dukungan, dan motivasi yang diberikan sehingga penelitian ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

[1] M. I. Qureshi and N. Khan, "Technological Evolution in Fintech: A Decadal Scientometric and Systematic Review of Developments and Criticisms," *International Journal of Finance and Economics*, 2026, doi: 10.1002/ijfe.70180.

[2] W. Li, J. Bu, X. Li, H. Peng, Y. Niu, and Y. Zhang, "A Survey of DeFi Security: Challenges and Opportunities," Oct. 2022, doi: 10.1016/j.jksuci.2022.10.028.

[3] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," Sep. 2022, [Online]. Available: http://arxiv.org/abs/2101.08778

[4] H. Chu, P. Zhang, H. Dong, Y. Xiao, S. Ji, and W. Li, "A survey on smart contract vulnerabilities: Data sources, detection and repair," Jul. 01, 2023, *Elsevier B.V.* doi: 10.1016/j.infsof.2023.107221.

[5] X. Li, X. Wang, T. Kong, J. Zheng, and M. Luo, "From Bitcoin to Solana-Innovating Blockchain towards Enterprise Applications."

[6] F. Schär, "Decentralized finance: on blockchain-and smart contract-based financial markets," *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021, doi: 10.20955/r.103.153-74.

[7] P. Qian, Z. Liu, Q. He, B. Huang, D. Tian, and X. Wang, "Smart Contract Vulnerability Detection Technique: A Survey," Sep. 2022, doi: 10.13328/j.cnki.jos.006375.

[8] G. Iuliano and D. Di Nucci, "Smart Contract Vulnerabilities, Tools, and Benchmarks: an Updated Systematic Literature Review," Jan. 2026, doi: 10.1016/j.jss.2026.112788.

[9] N. Ivanov, C. Li, Q. Yan, Z. Sun, Z. Cao, and X. Luo, "Security Defense For Smart Contracts: A Comprehensive Survey," May 2023, doi: 10.1145/3593293.

[10] P. Schueffel, "DeFi: Decentralized Finance - An Introduction and Overview," 2021, *Universidade do Porto - Faculdade de Engenharia*. doi: 10.24840/2183-0606_009.003_0001.

[11] A. Rusman, R. Nadlifatin, and A. P. Subriadi, "Information System Audit Using COBIT and ITIL Framework: Literature Review," *SinkrOn*, vol. 7, no. 3, pp. 799–810, Jul. 2022, doi: 10.33395/sinkron.v7i3.11476.

[12] ISACA, "COBIT 2019 Framework: Introduction and Methodology." Accessed: Apr. 02, 2026. [Online]. Available: https://www.isaca.org/resources/cobit

[13] D. Riyanti, P. Purwadi, and D. U. Hidayah, "IT Governance Audit Using COBIT 5: A Case Study of Banyumas Regency Regional Library," *Journal of Information Systems and Informatics*, vol. 8, no. 1, pp. 288–314, Feb. 2026, doi: 10.63158/journalisi.v8i1.1457.

[14] A. Nugroho and H. Ginardi, "Information Technology Governance Analysis to Reduce Information Security Risks Using Cobit 2019: A Case Study of Manufacturing Companies," *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 8, p. 3722, 2024, [Online]. Available: http://jist.publikasiindonesia.id/

[15] S. Salimuddin, M. Ula, and N. Nurdin, "ANALISIS KINERJA TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 PADA UNIVERSITAS JABAL GHAFUR," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 2, Apr. 2025, doi: 10.23960/jitet.v13i2.6130.