Volume 6 Issue 2 (2023) Pages 388 - 406
SEIKO : Journal of Management & Business
ISSN : 2598-831X (Print) and ISSN : 2598-8301 (Online)

Pengendalian Digitalisasi FintechCo Melalui Perancangan Pengelolaan Keamanan Informasi Berbasis COBIT 2019 *Information Security Focus Area*

Reynaldy Aditya Prayudi[1], Rahmat Mulyana[2], Rokhman Fauzi[3]
[1]Prodi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University
[2]Department of Computer and Systems Sciences, Stockholm University
[3]Prodi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University

Abstrak

Dengan semakin meningkatnya implementasi TI, hampir semua sektor, termasuk sektor keuangan, dipengaruhi untuk melakukan digitalisasi. Digitalisasi telah memunculkan inovasi *Financial Technology* (Fintech) dalam industri keuangan. Namun, Fintech menghadapi risiko keamanan informasi, yang juga berlaku untuk FintechCo. Sebagai perusahaan di bawah naungan Badan Usaha Milik Negara (BUMN) dan diatur oleh Otoritas Jasa Keuangan (OJK), FintechCo diharuskan untuk mematuhi regulasi yang mewajibkan pengawasan independen dan mengadopsi prinsip tata kelola TI yang mendorong keterbukaan, akuntabilitas, tanggung jawab, kemandirian, dan keadilan. Studi ini mengikuti pendekatan *Design Science Research* (DSR), yang terdiri dari lima tahap: *problem explication, requirement specification, design and development, demonstration,* dan *evaluation*. Pengumpulan data dilakukan melalui wawancara semi-terstruktur dan triangulasi dokumen internal dan eksternal. Data yang dikumpulkan kemudian dianalisis menggunakan kerangka kerja COBIT 2019 *Information Security*. Penelitian ini berfokus pada faktor-faktor desain yang menghasilkan tujuan tata kelola dan manajemen TI (TKMTI), yaitu APO13 *Managed Security*, DSS05 *Managed Security Services*, dan APO12 *Managed Risk*. Kesenjangan yang diidentifikasi kemudian ditangani dengan rekomendasi berdasarkan aspek *people, process,* dan *technology* yang dapat memitigasi risiko keamanan informasi FintechCo. Penelitian ini berkontribusi terhadap basis pengetahuan mengenai analisis prioritas manajemen keamanan informasi dalam konteks digitalisasi organisasi. Studi ini juga memberikan wawasan implikasi praktis yang relevan untuk FintechCo secara khususnya, dan industri Fintech pada umumnya.

Kata Kunci: *Digitalisasi, Tata Kelola dan Manajemen Teknologi Informasi (TKMTI), Manajemen Keamanan Informasi, COBIT 2019 Information Security, Design Science Research.*

Abstract

With the escalating implementation of Information Technology (IT), almost all sectors, including the financial sector, are influenced to embark on digitalization. This digitalization has given rise to Financial Technology (Fintech) innovations in the financial industry. However, Fintech encounters information security risks, which also applies to FintechCo. As a company under the auspices of State-Owned Enterprises (SOEs) and regulated by the Financial Services Authority (OJK), FintechCo is required to comply with regulations that require independent supervision and the adoption of IT governance principles that promote transparency, accountability, responsibility, independence, and fairness. This study adheres to the Design Science Research (DSR) approach, which consists of five stages: problem explication, requirement specification, design and development, demonstration, and evaluation. Data collection is conducted through semi-structured interviews and internal and external document

triangulation. The gathered data is subsequently analyzed using the COBIT 2019 Information Security framework. The research concentrates on design factors that produce Information Technology Governance and Management (ITGM) objectives, namely APO13 Managed Security, DSS05 Managed Security Services, and APO12 Managed Risk. The identified gaps are addressed with recommendations based on people, process, and technology aspects that can mitigate FintechCo's information security risks. This research contributes to the knowledge base concerning prioritizing information security management in the context of organizational digitalization. This study also provides relevant practical implication insights specifically for FintechCo, and the Fintech industry in general.

Keywords: *Digitalization, IT Governance and Management, Information Security Management, COBIT 2019 Information Security, Design Science Research*

[1]Reynaldy Aditya Prayudi, [2]Rahmat Mulyana, [3]Rokhman Fauzi
[1]aldyprayudi@student.telkomuniversity.ac.id, [2]rahmat@dsv.su.se,
[3]rokhmanfauzi@telkomuniversity.ac.id

PENDAHULUAN

Teknologi Informasi (TI) merupakan teknologi yang digunakan untuk mengolah data dengan memproses, mendapatkan, menyusun, menyimpan, serta memanipulasi data untuk menghasilkan informasi yang berkualitas (Suryana, 2012). Awalnya, TI hanya digunakan untuk pengolahan data, namun dengan semakin berkembangnya TI, hampir seluruh aktivitas yang ada telah mengimplementasikan TI, termasuk industri keuangan (Maharsi, 2000). Di industri keuangan, kemajuan TI telah mengganggu banyak perusahaan keuangan *incumbent* dan mendorong mereka untuk menerapkan Transformasi Digital (TD) (Mulyana et al., 2022). TD dalam industri keuangan merujuk pada "*pemanfaatan teknologi digital baru seperti media sosial, teknologi mobile, analitik data, perangkat tersemat, dan lainnya, untuk mendorong peningkatan bisnis yang substansial. Peningkatan ini termasuk meningkatkan pengalaman pelanggan, menyempurnakan efisiensi operasional, dan memperkenalkan model bisnis inovatif* (Fitzgerald et al., 2013, p. 2)". Transformasi ini bertujuan untuk meningkatkan efisiensi, layanan pelanggan, dan penawaran produk keuangan inovatif, mendefinisikan kembali bagaimana pemangku kepentingan memandang dan berinteraksi dengan institusi keuangan tradisional (Mulyana et al., 2023).

Namun, kemajuan TI juga mendorong digitalisasi di perusahaan keuangan *disruptive* yang dikenal sebagai *Financial Technology* (Fintech). Menurut Peraturan Bank Indonesia (PBI) Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial, "*Fintech adalah penggunaan teknologi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi dan/atau model bisnis baru dan dapat berdampak pada stabilitas moneter, stabilitas sistem keuangan dan/atau efisiensi, kelancaran, keamanan dan keandalan sistem pembayaran* (Bank Indonesia, 2017)".

Digitalisasi di Fintech merujuk pada proses transformasi yang mencakup perubahan dalam struktur organisasi, proses, kompetensi individu, dan budaya keseluruhan perusahaan Fintech. Meskipun perusahaan Fintech biasanya lahir di era digital, mereka masih menjalani upaya digitalisasi berkelanjutan yang memanfaatkan teknologi digital seperti internet, *cloud computing, big data*, dan kecerdasan buatan untuk meningkatkan efisiensi bisnis dan menciptakan pengalaman pelanggan yang superior. Transformasi ini memungkinkan perusahaan Fintech untuk menyediakan layanan keuangan yang lebih mudah diakses, lebih cepat, dan lebih nyaman daripada

institusi keuangan tradisional (Alt, 2018; Bloomberg, 2018; El Sawy et al., 2020; Frenzel et al., 2021; Giglio, 2021).

Perbedaan utama antara TD dan digitalisasi dalam industri keuangan terletak pada titik awal dan inisiatif fokus. DT dalam industri keuangan terutama ditujukan untuk institusi keuangan tradisional untuk mengadopsi teknologi digital (Pramanik et al., 2019). Sementara itu, digitalisasi dalam Fintech berfokus pada pemanfaatan teknologi digital untuk menyediakan layanan keuangan yang lebih mudah diakses, lebih cepat, dan nyaman (Bank Indonesia, 2017, p. 3; Pant, 2020).

Namun demikian, digitalisasi di Fintech membawa risiko inheren: keamanan informasi (Utami et al., 2021). Untuk memitigasi risiko ini, Otoritas Jasa Keuangan (OJK) merilis regulasi yang ditetapkan dalam Pasal 18 Ayat 1 Bagian A dari Peraturan Otoritas Jasa Keuangan (POJK) Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan yang menyatakan bahwa "*operator diharuskan untuk menerapkan prinsip tata kelola teknologi informasi dan komunikasi* (Otoritas Jasa Keuangan Republik Indonesia, 2018, p. 10)". Oleh karena itu, semua operator layanan Fintech di Indonesia wajib mengikuti regulasi ini, termasuk FintechCo.

FintechCo adalah perusahaan Fintech di Indonesia di bawah naungan Badan Usaha Milik Negara (BUMN). Oleh karena itu, FintechCo harus mematuhi Peraturan Menteri BUMN Nomor PER-02-MBU-03-2023, yang menekankan bahwa "*tata kelola perusahaan yang baik adalah pengelolaan perusahaan yang menerapkan prinsip keterbukaan, akuntabilitas, tanggung jawab, kemandirian, dan keadilan* (Menteri BUMN, 2023)".

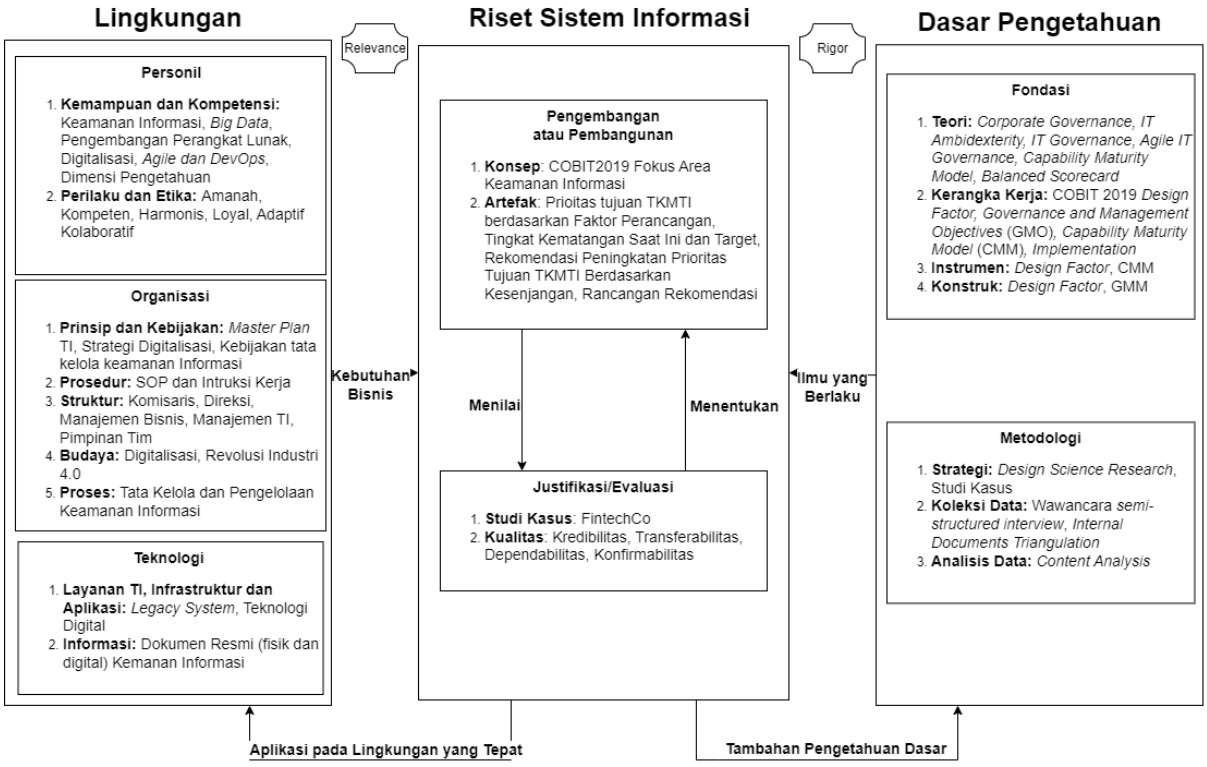
Berdasarkan POJK Nomor 13/POJK.02/2018 dan PER-02-MBU-03-2023, FintechCo diharuskan untuk menerapkan prinsip tata kelola teknologi informasi (TKTI) dan komunikasi yang menerapkan prinsip keterbukaan, akuntabilitas, tanggung jawab, kemandirian, dan keadilan. Tata Kelola TI (TKTI) adalah bagian dari tata kelola perusahaan yang berfokus pada pengawasan aset TI, berdampak pada nilai bisnis, dan memitigasi risiko terkait TI (De Haes et al., 2020). TKTI juga memiliki posisi yang sangat penting dalam mendorong usaha digital dalam organisasi (Mulyana et al., 2021). Dikarenakan FintechCo harus menghadapi risiko keamanan informasi yang inheren, diperlukan TKTI yang berfokus pada keamanan informasi. Keamanan informasi berfokus pada penanganan berbagai jenis informasi, meliputi dokumen fisik, kekayaan digital dan intelektual, dan komunikasi verbal atau visual (ISACA, 2020).

Untuk memitigasi risiko keamanan informasi dari digitalisasi Fintech, FintechCo perlu merancang tata kelola dan manajemen keamanan informasi. Penelitian ini mengembangkan pendekatan standar lebih lanjut pada industri keuangan menggunakan kerangka kerja COBIT 2019 terbaru, yakni COBIT 2019 *Information Security Focus Area* (ISACA, 2020) dengan menggunakan penilaian tujuh komponen, bukan hanya pada komponen proses seperti penelitian sebelumnya pada industri keuangan (Dewi et al., 2019). Oleh karena itu, penelitian ini telah merumuskan beberapa pertanyaan penelitian (RQs) untuk mengidentifikasi cara memitigasi risiko keamanan informasi yang dapat membantu FintechCo menjalani upaya digitalisasi berkelanjutan. Pertanyaan penelitian utama (RQ1) dari penelitian ini adalah: "Apa tujuan tata kelola dan manajemen teknologi informasi (TKMTI) keamanan informasi yang dibutuhkan oleh FintechCo untuk menjalani upaya digitalisasi berkelanjutan?" Pertanyaan penelitian kedua (RQ2) adalah: "Apa peningkatan potensial berdasarkan kesenjangan yang diidentifikasi dari tujuh komponen TKMTI untuk membantu FintechCo menjalani upaya digitalisasi

berkelanjutan, khususnya di area fokus manajemen keamanan informasi?" Dan pertanyaan penelitian terakhir (RQ3) adalah: "Bagaimana merancang rekomendasi berdasarkan peningkatan potensial yang diidentifikasi untuk mendukung FintechCo menjalani upaya digitalisasi berkelanjutan?"

METODOLOGI

Penelitian ini mengimplementasikan kerangka *Design Science Research* (DSR) untuk merancang manajemen keamanan informasi guna mendukung digitalisasi FintechCo serta memitigasi risiko keamanan informasi.



Gambar 1. Model Konseptual
(Diadaptasi dari Hevner DSR (Hevner et al., 2004))

Gambar 1 menampilkan bahwa DSR terbagi menjadi tiga (3) bagian, yaitu lingkungan, dasar pengetahuan, dan riset sistem informasi (SI) untuk mendefinisikan masalah, menentukan faktor yang relevan, dan menyediakan koneksi untuk memfasilitasi pemetaan inti masalah.

Gambar 2. Sistematika Penyelesaian Masalah
(Diadaptasi dari *Design Science Research Methodology* Hevner (Hevner & Chatterjee, 2010))

Gambar 2 menampilkan lima (5) tahapan sistematika penyelesaian masalah, yaitu *problem explication, requirement specification, design and development, demonstration,* dan *evaluation. Problem explication* merujuk pada tahap identifikasi masalah melalui tinjauan literatur untuk menentukan pernyataan masalah, tujuan penelitian, dan batasan penelitian. *Requirement specification* adalah fase untuk mengidentifikasi solusi, yang dimulai dengan menyusun daftar pertanyaan, menentukan prioritas tujuan tata kelola IT, melakukan analisis kesenjangan dari tujuh komponen kapabilitas, dan menyarankan rekomendasi perbaikan berdasarkan aspek *people, process,* dan *technology*. *Design and development* adalah fase untuk menganalisis rekomendasi perbaikan berdasarkan *resource, risk*, dan *value* serta merumuskan rekomendasi berdasarkan aspek *people, process,* dan *technology*. *Demonstration*, melibatkan penyusunan *roadmap* implementasi dan penentuan dampak dari rekomendasi yang diajukan terhadap perusahaan. *Evaluation* adalah tahap akhir untuk menguji temuan penelitian berdasarkan uji *credibility, transferability, dependability,* dan *confirmability* (Shenton, 2004).

HASIL DAN PEMBAHASAN

1. Hasil Prioritas Tujuan TKMTI

Dalam menentukan prioritas tujuan TKMTI yang menjadi fokus pada penelitian ini, hasil dari *design factor* COBIT 2019 (ISACA, 2018) dikalikan dengan nilai area fokus COBIT 2019 *Information Security* (ISACA, 2020). Tabel 1 menampilkan hasil analisis prioritas tujuan TKMTI.

Tabel 1. Hasil Prioritas Tujuan TKMTI

Tujuan TKMTI	Skor *Design Factor*	Skor Area Fokus	Skor Akhir
DSS05 *Managed Security Services*	80	2	160
APO13: *Managed Security*	55	2	110
APO12: *Managed Risk*	100	1	100

Area fokus keamanan informasi memiliki skor dua (2) pada dua (2) domain, yaitu APO13 *Managed Security* dan DSS05 *Managed Security Services.* Selain dua (2) domain tersebut, domain lainnya memiliki skor satu (1). Kemudian berdasarkan hasil perkalian tersebut, tiga (3) domain dengan nilai tertinggi dijadikan fokus pada penelitian ini.

2. Hasil Penilaian dan Analisis Kesenjangan

A. Komponen Proses

Tabel 2 menampilkan bahwa terdapat total delapan (8) kesenjangan pada komponen proses yang terbagi menjadi: satu (1) kesenjangan pada APO13, dua (2) kesenjangan pada DSS05, dan lima (5) kesenjangan pada APO12. Adapun skor tingkat kemampuan pada masing-masing tujuan TKMTI adalah 2.7 untuk APO13, 3 untuk DSS05, dan 1.7 untuk APO12.

Tabel 2. Hasil Penilaian dan Analisis Kesenjangan Komponen Proses

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
APO13 *Managed Security*		
APO13.01	36% *Partially*	2
APO13.02	92% *Fully*	3
	100% *Fully*	4
APO13.03	63% *Largely*	4
	0% N.A	5
Total Tingkat Kemampuan yang Tercapai		**8**
Rata-rata Skor Tingkat Kemampuan (Skala 0-5)		**2,7**
DSS05 *Managed Security Services*		
DSS05.01	100% (*Fully*)	2
	100% (*Fully*)	3
	100% (*Fully*)	4
DSS05.02	100% (*Fully*)	2
	100% (*Fully*)	3
	75% (*Largely*)	4
DSS05.03	89% (*Fully*)	2
	100% (*Fully*)	3
DSS05.04	100% (*Fully*)	2
	90% (*Fully*)	3
	100% (*Fully*)	4
DSS05.05	88% (*Fully*)	2
	67% (*Largely*)	3
DSS05.06	75% (*Largely*)	2
	83% (*Largely*)	3
DSS05.07	88% (*Fully*)	2
	100% (*Fully*)	3
Total Tingkat Kemampuan yang Tercapai		**21**
Rata-rata Skor Tingkat Kemampuan (Skala 0-5)		**3,0**
APO12 *Managed Risk*		
APO12.01	50% (*Partially*)	2
	50% (*Partially*)	3
	0% (None)	4
APO12.02	8% (*Partially*)	3
	0% (None)	4
	0% (None)	5
APO12.03	67% (*Largely*)	2
	50%(*Partially*)	3
	50%(*Partially*)	4

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
APO12.04	0% (None)	3
	50% (*Partially*)	4
APO12.05	50% (*Partially*)	2
	50% (*Partially*)	3
APO12.06	100% (*Fully*)	3
	83% (*Largely*)	4
	0% (None)	5
Total Tingkat Kemampuan yang Tercapai		**10**
Rata-rata Skor Tingkat Kemampuan (Skala 0-5)		**1,7**

B. Komponen Struktur Organisasi

Tabel 3 menunjukkan bahwa terdapat total tiga (3) kesenjangan pada komponen struktur organisasi, dimana FintechCo belum memiliki peran *Enterprise Risk Committee, Business Continuity Manager*, dan *Project Management Office*.

Tabel 3. Hasil Penilaian dan Analisis Kesenjangan Komponen Struktur Organisasi

Struktur Organisasi COBIT	Tujuan TKMTI	Struktur Organisasi FintechCo
Chief Technology Officer	APO13, APO12	*Chief Technology Officer*
Chief Information Officer	APO13, DSS05, APO12	
Chief Information Security Officer	APO13, DSS05, APO12	
Chief Digital Officer	APO12	
Chief Risk Officer	APO12	*Chief Risk Officer*
I & T Governance Board	APO13, DSS05, APO12	*IT Steering Committee*
Enterprise Risk Committee	APO13, APO12	FintechCo belum memiliki *role* maupun *responsibility* terkait Enterprise Risk Committee.
Business Process Owners	APO13, DSS05, APO12	B2B Services Group, IT Big Data & Analytic Group, Core Engineering Group, DevOps Group, dan B2B and Core Services
Business Continuity Manager	APO13, APO12	FintechCo belum memiliki *role* maupun *responsibility* terkait Business Continuity Manager.
Project Management Office	APO13, APO12	FintechCo belum memiliki *role* maupun *responsibility* terkait Project Management Office.
Service Manager	APO13, APO12	*Service Management Unit*
Information Security Manager	APO13, DSS05, APO12	*IT Security Policy and Control Unit, IT Compliance and Control Unit*
Head Architect	APO13, APO12	*IT Architecture Unit*
Head Development	APO13, DSS05, APO12	*Development Center*
Head IT Operations	APO13, DSS05, APO12	*IT Infrastructure Unit*
Head IT Administration	APO13, APO12	

Struktur Organisasi COBIT	Tujuan TKMTI	Struktur Organisasi FintechCo
Head Human Resources	DSS05	*Human Resources*
Data Management Function	APO12	*Data Engineering Unit*
Privacy Officer	APO13, DSS05, APO12	*IT Security Policy and Control Unit dan IT Compliance and Control Unit*

C. Komponen Kebijakan dan Prosedur

Tabel 4 menampilkan bahwa tidak ditemukan kesenjangan pada komponen kebijakan dan prosedur.

Tabel 4. Hasil Penilaian dan Analisis Kesenjangan Komponen Kebijakan dan Prosedur

Kebijakan	Kondisi Saat Ini
APO13 *Managed Security*	
Keamanan informasi dan kebijakan privasi	Kebijakan Pengelolaan Keamanan Informasi
DSS05 *Managed Security Services*	
Kebijakan Keamanan Informasi	Kebijakan Pengelolaan Keamanan Informasi
APO12 *Managed Risk*	
Kebijakan risiko perusahaan	Keputusan Direksi tentang Manajemen Risiko
Kebijakan risiko penipuan	Panduan dalam memantau serta mendeteksi risiko penipuan

D. Komponen Informasi

Tabel 5 menampilkan bahwa terdapat total lima (5) kesenjangan pada komponen informasi. Ditemukan bahwa FintechCo belum memiliki dokumen ruang lingkup SMKI, hasil laporan terkait *penetration test* dan tinjauan akses pengguna, proposal proyek untuk memitigasi risiko keamanan informasi, dan praktik mitigasi risiko keamanan informasi.

Tabel 5. Hasil Penilaian dan Analisis Kesenjangan Komponen Informasi

Praktik Manajemen	*Information Output*	Kondisi Saat Ini
APO13 *Managed Security*		
APO13.01 Membangun dan menjaga sistem manajemen keamanan informasi (ISMS).	*ISMS Scope Statement*	FintechCo belum memiliki pernyataan ruang lingkup ISMS
	IS Policy	Kebijakan Pengelolaan Keamanan Informasi
APO13.02 Mendefinisikan dan mengelola rencana perlakuan risiko keamanan informasi	*IS Risk Treatment Plan*	Kebijakan Pengelolaan Keamanan Informasi, Dokumen Kebijakan Manajemen Risiko Perseroan
	IS Business Case	Laporan akhir IT Audit FintechCo
APO13.03 Memantau dan meninjau sistem pengelolaan keamanan informasi (ISMS)	*IS Review Reports*	Laporan akhir IT Audit FintechCo
DSS05 *Managed Security Risk*		

Praktik Manajemen	*Information Output*	Kondisi Saat Ini
DSS05.01 Melindungi dari perangkat lunak berbahaya	*Information Security Management Reports*	Laporan akhir IT Audit FintechCo
	Information Security Service Catalog	Katalog layanan keamanan informasi
DSS05.02 Mengelola keamanan jaringan dan konektivitas	*Connectivity Security Policy*	Kebijakan Pengelolaan Keamanan Informasi
	Results Of Penetration Tests	FintechCo belum memiliki hasil laporan terkait *penetration tests.*
DSS05.03 Mengelola keamanan pada *endpoint.*	*Security Policies for Endpoint Devices*	Kebijakan Pengelolaan Keamanan Informasi
DSS05.04 Mengelola identitas pengguna dan akses logis	*Results of Reviews of User Accounts*	FintechCo belum memiliki laporan terkait tinjauan akses pengguna
	Approved User Access Rights	Prosedur Pengendalian Akses
DSS05.05 Mengelola akses fisik ke aset TI	*Access Logs*	Prosedur Pengendalian Akses
	Approved Access Requests	Prosedur Pengendalian Akses
DSS05.06 Mengelola dokumen sensitif dan perangkat *output.*	*Access Privileges*	Kebijakan terkait Pengaturan Akses
	Inventory Of Sensitive Documents and Devices	Kebijakan Pengelolaan Keamanan Informasi
DSS05.07 Mengelola kerentanan dan memantau infrastruktur untuk kejadian terkait keamanan	*Security Incident Tickets*	Service Desk
	Security Incident Characteristics	Service Desk
	Security Event Logs	Service Desk
APO12 ***Managed Risk***		
APO12.01 Mengumpulkan data.	*Data On Information Security Risk*	Penilaian Risiko Keamanan Informasi, Laporan Akhir IT Audit FintechCo
APO12.02 Menganalisis risiko.	*Information Security Risk Analysis Results*	Laporan Akhir IT Audit FintechCo
	Information Security Risk Scenarios	Kebijakan Pengelolaan Keamanan Informasi
APO12.03 Menjaga profil risiko	*Information Security Risk Profile*	Penilaian Risiko Keamanan Informasi
APO12.04 Mengartikulasikan risiko	*Information Security Risk Response Strategies*	Kebijakan Pengelolaan Keamanan Informasi
APO12.05 Mendefinisikan portofolio tindakan pengelolaan risiko.	*Project Proposals for Reducing Information Security Risk*	FintechCo belum memiliki proposal proyek untuk memitigasi risiko keamanan informasi
APO12.06 Menanggapi risiko.	*Information Security Risk Mitigation Practices*	FintechCo belum memiliki praktik mitigasi risiko keamanan informasi

E. Komponen Budaya, Etika, dan Perilaku

Tabel 6 menampilkan bahwa tidak ditemukan kesenjangan pada komponen budaya, etika, dan perilaku.

Tabel 6. Hasil Penilaian dan Analisis Kesenjangan Komponen Budaya, Etika, dan Perilaku

Elemen Kunci Budaya	Kondisi Saat Ini
APO13 ***Managed Security***	
Membentuk budaya kesadaran akan keamanan dan privasi untuk mendorong perilaku yang diinginkan dan implementasi kebijakan keamanan dan privasi dalam praktik sehari-hari.	Kebijakan Manajemen Keamanan Informasi dan pelaksanaan *awareness* terhadap keamanan informasi
DSS05 ***Managed Security Services***	
Membentuk budaya kesadaran pengguna dalam menjaga praktik keamanan dan privasi.	Kebijakan Manajemen Keamanan Informasi dan pelaksanaan *awareness* terhadap keamanan informasi
APO12 ***Managed Risk***	
Mendukung budaya risiko yang transparan dan keikutsertaan, di mana manajemen senior harus menetapkan arah dan menunjukkan dukungan yang jelas untuk pengintegrasian praktik risiko di perusahaan. Manajemen mendorong komunikasi terbuka dan kepemilikan bisnis terkait risiko bisnis I&T.	FintechCo telah memiliki Keputusan Direksi tentang Manajemen Risiko yang dapat dijadikan pedoman dalam manajemen risiko

F. Komponen Individu, Keterampilan dan Kompetensi

Tabel 7 menampilkan bahwa tidak ditemukan kesenjangan pada komponen individu, keterampilan, dan kompetensi.

Tabel 7. Hasil Penilaian dan Analisis Kesenjangan Komponen Individu, Keterampilan dan Kompetensi

Kemampuan	Kondisi Saat Ini
APO13 ***Managed Security***	
Information Security	FintechCo telah mengimplementasikan pemasangan antivirus, pengaturan hak *akses*, serta pelatihan *awareness* terkait keamanan informasi
Information Security Strategy Development	FintechCo telah mengatur pengembangan strategi terkait keamanan informasi pada Kebijakan Pengelolaan Keamanan Informasi.
DSS05 ***Managed Security Services***	
Information Security	FintechCo telah mengimplementasikan pemasangan antivirus, pengaturan hak akses, serta pelatihan *awareness* terkait keamanan informasi
Information Security Management	FintechCo telah mengimplementasikan manajemen dalam pemasangan antivirus, manajemen pembatasan hak akses, serta manajemen *awareness* dengan cara melakukan pelatihan *awareness* terkait keamanan informasi.

Kemampuan	Kondisi Saat Ini
Penetration Testing	FintechCo telah melakukan *penetration testing* terkait keamanan informasi dan juga keamanan sistem.
Security Administration	Administrasi terkait keamanan pada FintechCo telah diatur dalam Kebijakan Pengelolaan Keamanan Informasi FintechCo.
APO12 *Managed Risk*	
Business Risk Management	Keputusan Direksi Perseroan No. 01/FKN-01/KD/VIII/2019 tentang Kebijakan Rencana Keberlangsungan Usaha (*Business Continuity Plan Policy*)
Information Assurance	Kebijakan Pengelolaan Keamanan Informasi
Risk management	Keputusan Direksi Manajemen Risiko menggunakan COSO dan ERM

G. Komponen Layanan, Infrastruktrur, dan Aplikasi

Tabel 8 menampilkan bahwa terdapat total tiga (3) kesenjangan pada komponen layanan, infrastruktur, dan aplikasi. Ditemukan bahwa FintechCo belum memiliki *tools* terkait *security information and event management* (SIEM), *services operations center* (SOC), dan manajemen krisis.

Tabel 8. Hasil Penilaian dan Analisis Kesenjangan Komponen Layanan, Infrastruktur, dan Aplikasi

Layanan, Infrastruktur, dan Aplikasi	Kondisi Saat Ini
APO13 *Managed Security*	
Configuration Management Tools	Aplikasi Ansible, GitLab
Security and Privacy Awareness Services	Telah dilakukan pelatihan kesadaran keamanan dan privasi
Third-party Security Assessment Services	Laporan Akhir IT Audit FintechCo
DSS05 *Managed Security* Risk	
Directory Services	*Microsoft Single Sign On (SSO)*
Email Filtering Systems	Telah terdapat kebijakan terkait pengelolaan email, termasuk *filtering* email
Identity and Access Management System	*Microsoft Single Sign On (SSO)*
Security Awareness Services	Telah dilakukan pelatihan kesadaran keamanan
Security Information and Event Management (SIEM) Tools	Tidak ditemukan *tools* terkait SIEM
Security Operations Center (SOC) Services	Tidak ditemukan layanan SOC
Third-Party Security Assessment Services	Laporan Akhir IT Audit FintechCo
URL Filtering Systems	Telah terdapat kebijakan terkait pengelolaan URL, termasuk *filtering* URL
APO12 *Managed Risk*	
Crisis Management Services	Tidak ditemukan layanan terkait manajemen krisis
Governance, Risk and Compliance (GRC) Tools	APU-PPT, *Intelligent Fraud Management System, Biometric, CPN,* Ansible
Risk Analysis Tools	*Big data and Analytics, Intelligent Fraud Management System,* CPN

Layanan, Infrastruktur, dan Aplikasi	Kondisi Saat Ini
Risk Intelligence Services	*Big data and analytics, Intelligent Fraud Management System*

3. Perbaikan Potensial

Perbaikan potensial bertujuan untuk menentukan perbaikan yang diperlukan untuk mengatasi hasil kesenjangan yang telah teridentifikasi. Perbaikan potensial terbagi menjadi tiga (3) aspek, yaitu *people, process* dan *technology*. Tabel 9 menampilkan perbaikan potensial pada aspek *people.*

Tabel 9. Perbaikan Potensial Aspek *People*

Komponen	*Type*	Perbaikan Potensial
APO13 *Managed Security*		
Struktur Organisasi	*Roles and Responsibility*	Menambahkan peran dan tanggung jawab terkait *Enterprise Risk Comittee*
	Roles and Responsibility	Menambahkan peran dan tanggung jawab terkait *Business Continuity Manager*.
	Roles and Responsibility	Menambahkan peran dan tanggung jawab terkait *Project Management Office*.
APO12 *Managed Risk*		
Struktur Organisasi	*Roles and Responsibility*	Menambahkan peran dan tanggung jawab terkait *Enterprise Risk Comittee*
	Roles and Responsibility	Menambahkan peran dan tanggung jawab terkait *Business Continuity Manager*.
	Roles and Responsibility	Menambahkan peran dan tanggung jawab terkait *Project Management Office*.

Tabel 10 menampilkan perbaikan potensial pada aspek *process*.

Tabel 10. Perbaikan Potensial Aspek *Process*

Komponen	*Type*	Perbaikan Potensial
APO13 *Managed Security*		
Proses	*Policy*	Menambahkan BAB baru pada Kebijakan Pengelolaan Keamanan Informasi yang mengatur tentang Sistem Manajemen Keamanan Informasi (SMKI)
DSS05 *Managed Security Services*		
Proses	*Policy*	Menambahkan kebijakan terkait pelatihan kesadaran keamanan informasi fisik secara teratur
	Procedure	Menyusun prosedur penghancuran dokumen sensitive
Informasi	*Record*	Menyusun pedoman penyusunan laporan hasil *penetration testing*.
	Record	Menyusun pedoman penyusunan laporan hasil tinjauan akses pengguna
APO12 *Managed Risk*		
Proses	*Procedures*	Menyusun prosedur manajemen risiko
	Policy	Menambahkan kebijakan terkait komunikasi risiko kepada pemangku kepentingan
Informasi	*Record*	Menyusun pedoman penyusunan proposal proyek untuk memitigasi risiko keamanan informasi

Komponen	*Type*	Perbaikan Potensial
	Policy	Menambahkan kebijakan terkait praktik mitigasi risiko keamanan informasi

Tabel 11 menampilkan perbaikan potensial pada aspek *technology*.

Tabel 11. Perbaikan Potensial Aspek *Technology*

Komponen	*Type*	Perbaikan Potensial
DSS05 *Managed Security Services*		
Layanan, Infrastruktur, dan Aplikasi	*Tools*	Menentukan *tools* yang tepat untuk *Security Information and Event Management* (SIEM)
	Tools	Menentukan *tools* yang tepat untuk *Security Operation Center (*SOC)
APO12 *Managed Risk*		
Layanan, Infrastruktur, dan Aplikasi	*Tools*	Menentukan *tools* yang tepat untuk manajemen krisis

4. Prioritas *Roadmap* Implementasi Berdasarkan Analisis *Resource, Risk,* dan *Value* (RRV).

Setelah menganalisis perbaikan potensial, ditentukan prioritas *roadmap* implementasi berdasarkan hasil analisis *resource, risk,* dan *value* (RRV). Analisis RRV memiliki hasil akhir yang terbagi menjadi tiga (3) skor. Pertama, diberikan skor tiga (3) jika sumber daya yang dibutuhkan berasal dari internal saja, risiko kegagalan hanya mempengaruhi satu unit perusahaan, dan nilai dari implementasi yang berhasil mempengaruhi semua unit perusahaan. Kedua, diberikan skor dua (2) jika sumber daya yang dibutuhkan berasal dari internal dan eksternal, risiko kegagalan mempengaruhi beberapa unit perusahaan, dan nilai dari implementasi yang berhasil mempengaruhi beberapa unit perusahaan. Ketiga, diberikan skor satu (1) jika sumber daya yang dibutuhkan berasal dari eksternal, risiko kegagalan mempengaruhi semua unit perusahaan, dan nilai dari implementasi yang berhasil hanya mempengaruhi satu unit perusahaan. Tabel 12 menampilkan hasil analisis RRV untuk menentukan prioritas *roadmap* implementasi.

Tabel 12. Prioritas Roadmap Implementasi Berdasarkan Analisis *Resource, Risk*, dan *Value* (RRV).

Perbaikan Potensial	Skor	Prioritas
Aspek *People*		
Menambahkan peran dan tanggung jawab terkait *Business Continuity Manager.*	12	1
Menambahkan peran dan tanggung jawab terkait *Project Management Office.*	12	2
Menambahkan peran dan tanggung jawab terkait *Enterprise Risk Comittee*	6	3
Aspek *Process*		
Menyusun pedoman penyusunan laporan hasil penetration testing.	27	1
Menyusun pedoman penyusunan laporan hasil tinjauan akses pengguna.	27	2
Menyusun pedoman penyusunan proposal proyek untuk memitigasi risiko keamanan informasi	27	3

Perbaikan Potensial	Skor	Prioritas
Menambahkan BAB baru pada Kebijakan Pengelolaan Keamanan Informasi yang mengatur tentang Sistem Manajemen Keamanan Informasi (SMKI)	18	4
Menambahkan kebijakan terkait pelatihan kesadaran keamanan informasi fisik secara teratur	18	5
Menambahkan kebijakan terkait praktik mitigasi risiko keamanan informasi	18	6
Menambahkan kebijakan terkait komunikasi risiko kepada pemangku kepentingan	18	7
Menyusun prosedur penghancuran dokumen sensitive	9	8
Menyusun prosedur manajemen risiko	9	9
Aspek *Technology*		
Menentukan *tools* yang tepat untuk *Security Information and Event Management* (SIEM)	6	1
Menentukan *tools* yang tepat untuk *Security Operation Center (*SOC)	6	2
Menentukan *tools* yang tepat untuk manajemen krisis	6	3

5. Perancangan Rekomendasi Berdasarkan Perbaikan Potensial

A. Rekomendasi Aspek *People*

Perancangan pada aspek *people* menghasilkan tiga (3) rekomendasi, yaitu menambahkan peran dan tanggung jawab terkait *Enterprise Risk Committee, Business Continuity Manager,* and *Project Management Office.*

B. Rekomendasi Aspek *Process*

Perancangan pada aspek *process* menghasilkan sembilan (9) rekomendasi, yaitu mengembangkan panduan untuk hasil pengujian penetrasi, merumuskan panduan untuk laporan tinjauan akses, membuat prosedur untuk pembuangan dokumen sensitif, mengintegrasikan bab baru ke dalam kebijakan manajemen keamanan informasi yang mengatur sistem manajemen keamanan informasi (ISMS), menetapkan kebijakan yang berhubungan dengan pelatihan kesadaran keamanan informasi fisik secara rutin, membuat kebijakan mengenai praktik mitigasi risiko keamanan informasi, menetapkan kebijakan untuk komunikasi risiko kepada pemangku kepentingan, merumuskan panduan untuk proposal proyek mitigasi risiko, dan mengembangkan prosedur manajemen risiko.

C. Rekomendasi Aspek *Technology*

Perancangan pada aspek *technology* menghasilkkan tiga (3) rekomendasi, yaitu mengimplementasikan aplikasi Splunk Enterprise untuk *Security Information and Event Management* (SIEM) dan *Service Operation Center* (SOC) serta mengimplementasikan aplikasi OnSolve untuk manajemen krisis.

6. *Roadmap* Implementasi

Tabel 13 menampilkan *roadmap* implementasi yang dirancang sebagai pedoman bagi organisasi untuk mengimplementasikan rekomendasi.

Tabel 13. *Roadmap* Implementasi

Rekomendasi	Prioritas	*Roadmap Timeline (Quarter)*							
		2024				2025			
		1	2	3	4	1	2	3	4
Aspek *People*									

Rekomendasi	Prioritas	*Roadmap Timeline (Quarter)*							
		2024				2025			
		1	2	3	4	1	2	3	4
Mengimplementasikan penambahan peran dan tanggung jawab terkait *Business Continuity Manager.*	1			■					
Mengimplementasikan penambahan peran dan tanggung jawab terkait *Project Management Office.*	2				■				
Mengimplementasikan penambahan peran dan tanggung jawab terkait *Enterprise Risk Comittee*	3					■			
Aspek *Process*									
Mengimplementasikan pedoman penyusunan laporan hasil penetration testing.	1	■							
Mengimplementasikan pedoman penyusunan laporan hasil tinjauan akses pengguna.	2	■							
Mengimplementasikan pedoman penyusunan proposal proyek untuk memitigasi risiko keamanan informasi	3		■						
Mengimplementasikan penambahan BAB baru pada Kebijakan Pengelolaan Keamanan Informasi yang mengatur tentang Sistem Manajemen Keamanan Informasi (SMKI)	4			■					
Mengimplementasikan penambahan kebijakan terkait pelatihan kesadaran keamanan informasi fisik secara teratur	5				■				
Mengimplementasikan penambahan kebijakan terkait praktik mitigasi risiko keamanan informasi	6					■			
Mengimplementasikan penambahan kebijakan terkait komunikasi risiko kepada pemangku kepentingan	7						■		
Mengimplementasikan prosedur penghancuran dokumen sensitif	8							■	
Mengimplementasikan prosedur manajemen risiko	9								■
Aspek *Technology*									
Mengimplementasikan Splunk Enterprisie untuk *Security Information and Event Management* (SIEM) dan *Security Operation Center* (SOC)	1						■		
Mengimplementasikan *OnSolve* untuk manajemen krisis	2							■	

7. Estimasi Pengaruh Implementasi Rekomendasi terhadap FintechCo

Setelah merancang rekomendasi berdasarkan aspek *people, process,* dan *technology,* dilakukan perbandingan untuk membandingkan keadaan perusahaan sebelum dan sesudah menerapkan rekomendasi tersebut. Tabel 14 menampilkan estimasi pengaruh perancangan rekomendasi pada komponen proses.

Tabel 14. Estimasi Pengaruh Perancangan Rekomendasi Pada Komponen Proses

Tujuan TKMTI	Skor Tingkat Kemampuan Sebelum Perbaikan	Skor Tingkat Kemampuan Sesudah Perbaikan
APO13 *Managed Security*	2,7	3,0
DSS05 *Managed Security Services*	3,0	3,3
APO12 *Managed Risk*	1,7	3,0

Tabel 15 menampilkan estimasi pengaruh implementasi rekomendasi pada komponen struktur organisasi

Tabel 15. Estimasi Pengaruh Implementasi Rekomendasi Pada Komponen Struktur Organisasi

Sebelum Perbaikan	Setelah Perbaikan
APO13 *Managed Security* and APO12 *Managed Risk*	
FintechCo belum memiliki peran terkait *Enterprise Risk Committee*	Peran dan tanggung jawab terkait *Enterprise Risk Committee*
FintechCo belum memiliki peran terkait *Business Continuity Manager*	Peran dan tanggung jawab terkait *Business Continuity Manager*
FintechCo belum memiliki peran terkait *Project Management Office*	Peran dan tanggung jawab terkait *Project Management Office*

Tabel 16 menampilkan estimasi pengaruh implementasi rancangan pada komponen informasi

Tabel 16. Estimasi Pengaruh Implementasi Rekomendasi Pada Komponen Informasi

Sebelum Perbaikan	Setelah Perbaikan
APO13 *Managed Security*	
FintechCo belum memiliki kebijakan yang mengatur SMKI	Kebijakan yang mengatur SMKI
DSS05 *Managed Security Services*	
FintechCo belum memiliki laporan hasil *penetration testing*	Pedoman penyusunan laporan hasil *penetration testing*
FintechCo belum memiliki laporan hasil tinjauan akses pengguna	Pedoman penyusunan laporan hasil tinjauan akses pengguna
APO12 *Managed Risk*	
FintechCo belum memiliki proposal proyek untuk mitigasi risiko keamanan informasi	Pedoman penyusunan proposal proyek untuk mitigasi risiko keamanan informasi
FintechCo belum memiliki dokumen terkait praktik mitigasi risiko keamanan informasi	Kebijakan yang mengatur praktik mitigasi risiko keamanan informasi

Tabel 17 menampilkan estimasi pengaruh rancangan pada komponen layanan, infrastruktur, dan aplikasi.

Tabel 17. Estimasi Pengaruh Perancangan Rekomendasi Pada Komponen Layanan, Infrastruktur, dan Aplikasi

Sebelum Perbaikan	Setelah Perbaikan
DSS05 *Managed Security Services*	
Tidak terdapat *tools* terkait *security information and event management* (SIEM)	Splunk Enterprise (Gartner, 2023)
Tidak terdapat *tools* terkait *Security Operation Center* (SOC)	
APO12 *Managed Risk*	

Tidak terdapat layanan manajemen krisis	OnSolve (Gartner, 2023)

Penelitian terdahulu terkait mekanisme TKTI yang mempengaruhi TD di industri finansial pada sektor perbankan dan asuransi (Mulyana et al., 2023) menemukan bahwa untuk perusahaan *incumbent* diperlukan TKTI hibrida berupa kombinasi antara pendekatan tradisional dan *agile*-adaptif untuk mengawal kesuksesan TD menuju pencapaian target kinerja organisasi. Hal ini terjadi karena lembaga keuangan tradisional di Indonesia sudah memiliki aset yang besar dengan risiko inheren yang tinggi, serta terikat oleh regulasi yang relatif ketat dan memerlukan dokumentasi pekerjaan yang formal. Namun, perusahaan *incumbent* tersebut perlu lebih lincah dan beradaptasi dengan cepat untuk tetap kompetitif dengan meningkatkan solusi *customer experience* mereka agar tetap *survive* di era digital, sehingga membutuhkan TKTI yang *agile*-adaptif.

Pada studi ini ditemukan bahwa perusahaan pada industri keuangan sektor Fintech seperti FintechCo biasanya merupakan perusahaan *startup* yang terlahir di era digital dengan aset awal yang tidak terlalu besar dan memiliki risiko yang cenderung lebih rendah. Sehingga regulator pun memberikan ruang bergerak yang lebih luas melalui pendekatan *Regulatory Sandbox* yang membutuhkan dukungan TKTI yang lebih *agile* dan adaptif yang tentunya memerlukan pengawalan Manajemen Keamanan Informasi yang memadai untuk pengendalian digitalisasi yang berkelanjutan. Oleh karena itu, pendekatan Design Science Research berbasis kerangka kerja terbaru dari ISACA yaitu COBIT 2019 Information Security Focus Area yang telah ditunjukkan pada studi ini merupakan satu alternatif solusi untuk pemenuhan kebutuhan industri keuangan *disruptive* seperti sektor Fintech ini.

SIMPULAN

Penelitian ini mungkin mengalami bias seleksi karena mengandalkan studi kasus tunggal. Karakteristik unik dan konteks perusahaan yang dipilih mungkin tidak mewakili semua organisasi, yang membatasi generalisasi temuan. Meski memiliki keterbatasan, penelitian ini menemukan bahwa berdasarkan hasil faktor desain yang telah dilakukan menggunakan kerangka kerja COBIT 2019 dan teknik prioritas dalam area fokus keamanan informasi, ada tiga (3) tujuan TKMTI tertinggi untuk keamanan informasi yang dibutuhkan oleh FintechCo untuk menjalankan upaya digitalisasi berkelanjutan, yaitu APO13: *Managed Security*, DSS05: *Managed Security* Services, dan APO12: *Managed Risk*. Kemudian, terdapat lima belas (15) perbaikan potensial yang dibagi menjadi aspek *people, process,* dan *technology* berdasarkan kesenjangan yang teridentifikasi dari tujuh komponen TKMTI untuk membantu FintechCo menjalankan upaya digitalisasi berkelanjutan, khususnya di area fokus manajemen keamanan informasi.

Perancangan rekomendasi berdasarkan perbaikan potensial yang teridentifikasi juga terbagi menjadi tiga (3) aspek. Pada aspek *people*, terdapat penambahan peran dan tanggung jawab. Pada aspek *Process,* terdapat penambahan kebijakan, prosedur, serta dokumen informasi. Dan yang terakhir, pada aspek *technology* terdapat penambahan *tools*. Pada aspek *people*, terdapat perancangan dalam penambahan *roles* dan *responsibility* terkait *Enterprise Risk Committee*, *Business Continuity Manager*, dan *Project Management Office.* Pada aspek *process,* terdapat perancangan dokumen SOP yang berisi langkah-langkah yang terperinci dan terstruktur yang harus diikuti dalam

menjalankan tugas, dokumen pedoman penyusunan laporan yang digunakan sebagai kerangka dasar dalam membuat laporan, dan penambahan kebijakan sebagai petunjuk tertulis yang ditetapkan oleh perusahaan untuk memberikan arah, panduan, dan aturan dalam mengatur perilaku, pengambilan keputusan dan tindakan dalam lingkup tertentu. Dan terakhir, dalam aspek *technology* terdapat perbandingan *tools* yang dapat digunakan sebagai referensi dalam menerapkan aplikasi yang tepat untuk meningkatkan kinerja FintechCo.

Semua rekomendasi tersebut mendukung FintechCo dalam menjalankan upaya digitalisasi berkelanjutan. Peneliti berharap penelitian ini dapat berkontribusi terhadap basis pengetahuan mengenai analisis prioritas manajemen keamanan informasi dalam konteks digitalisasi organisasi. Studi ini juga memberikan wawasan implikasi yang relevan untuk FintechCo secara khusus, dan industri Fintech pada umumnya.

Referensi:

Alt, R. (2018). Electronic Markets on digitalization. *Electronic Markets*, *28*(4), 397–402. https://doi.org/10.1007/s12525-018-0320-7

Bank Indonesia. (2017). *Peraturan Bank Indonesia (PBI) No. 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial*.

Bloomberg, J. (2018). *Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril*.

De Haes, S., Caluwe, L., Huygh, T., & Joshi, A. (2020). *Governing Digital Transformation: Guidance for Corporate Board Members*. Springer International Publishing. https://doi.org/10.1007/978-3-030-30267-2

Dewi, P. M., Fauzi, R., & Mulyana, R. (2019). *Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework COBIT 2019 Domain Build, Acquire And Implement: Studi Kasus Bank XYZ*.

El Sawy, O. A., Kræmmergaard, P., Amsinck, H., & Vinther, A. L. (2020). How LEGO Built the Foundations and Enterprise Capabilities for Digital Leadership. In R. D. Galliers, D. E. Leidner, & B. Simeonova (Eds.), *Strategic Information Management* (5th ed., pp. 174–201). Routledge. https://doi.org/10.4324/9780429286797-8

Frenzel, A., Bruckner, M. T., Muench, J. C., & Veit, D. J. (2021). *Digitization or Digitalization? – Toward an Understanding of Definitions, Use and Application in IS Research*.

Gartner. (2023). *Gartner Magic Quadrant & Critical Capabilities*. https://www.gartner.com/en/research/magic-quadrant

Giglio, F. (2021). Fintech: A Literature Review. *International Business Research*, *15*(1), 80. https://doi.org/10.5539/ibr.v15n1p80

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice* (Vol. 22). Springer US. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

ISACA. (2018). *COBIT® 2019 Implementation guide: Implementing and optimizing an information and technology governance solution*. ISACA.

ISACA. (2020). *COBIT Focus Area: Information Security Using COBIT 2019*. ISACA.

Maharsi, S. (2000). PENGARUH PERKEMBANGAN TEKNOLOGI INFORMASI TERHADAP BIDANG AKUNTANSI MANAJEMEN. *Jurnal Akuntansi*, *2*(2).

Menteri BUMN. (2023). *Peraturan Menteri Badan Usaha Milik Negara (BUMN) Republik Indonesia Nomor Per-2/MBU/03/2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara*.

Mulyana, R., Rusu, L., & Perjons, E. (2021). IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review. *Americas' Conference on Information Systems (AMCIS), Virtual, 2021, Pp. 1-10.*

Mulyana, R., Rusu, L., & Perjons, E. (2022). *IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry.*

Mulyana, R., Rusu, L., & Perjons, E. (2023). How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry of Indonesia. *Information Systems Development (ISD) Conference, Lisbon, 2023, Pp. 1-12.*

Otoritas Jasa Keuangan Republik Indonesia. (2018). *Peraturan Otoritas Jasa Keuangan (POJK) Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan*.

Pant, S. K. (2020). *Fintech: Emerging Trends. 13*(1).

Pramanik, H. S., Kirtania, M., & Pani, A. K. (2019). Essence of digital transformation—Manifestations at large financial institutions from North America. *Future Generation Computer Systems*, *95*, 323–343. https://doi.org/10.1016/j.future.2018.12.003

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Suryana, D., (Ed). (2012). *Mengenal Teknologi: Teknologi Informasi.* CreateSpace Independent Publishing Platform.

Utami, A. F., Ekaputra, I. A., & Japutra, A. (2021). Adoption of FinTech Products: A Systematic Literature Review. *Journal of Creative Communications*, *16*(3), 233–248. https://doi.org/10.1177/09732586211032092