Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), email: puslit.stmikbjb@gmail.com
eISSN: 26850893
pISSN: 20893787

Pemanfaatan *COBIT 2019 Information* Security Dalam Merancang Manajemen Keamanan Informasi Pada Transformasi BankCo

Aini Rahmadana[1*], Rahmat Mulyana[2], Ari Fajar Santoso[3]
[1,3]Sistem Informasi, Telkom University, Bandung, Indonesia
[2]Computer and Systems Sciences, Stockholm University, Kista, Sweden
*e-mail *Corresponding Author*: ainirahmadana@student.telkomuniversity.ac.id

Abstract

Consumer behavior changes, the rapid digital innovation pace among competitors, and regulatory directives have compelled incumbent companies to accelerate digital transformation (DT) efforts. Previous research has successfully identified the influence of information technology governance (ITG) on organizational performance (OP), fully mediated by DT. However, a deeper understanding of the design of information security management mechanisms to guide the DT journey is still necessary. This study employs the Design Science Research (DSR) approach, based on the latest ISACA framework, COBIT 2019 Information Security Focus Area. A case study is conducted at BankCo, with data collection through interviews and document triangulation. Solution design and implementation roadmaps are based on gaps identified from the assessment of the three BankCo priorities: DSS05 Managed Security Services, APO13 Managed Security, and BAI06 Managed IT Changes. This research contributes to the knowledge base of information security management in DT and is particularly practical for guiding BankCo's DT journey, as well as benefiting the broader industry.

Keywords: *Digital Transformation; IT Governance and Management; COBIT 2019 Information Security; Design Science Research; Bank*.

Abstrak

Perubahan perilaku konsumen, kecepatan inovasi digital kompetitor, dan arahan regulasi telah memaksa perusahaan *incumbent* untuk percepatan transformasi digital (TD). Penelitian sebelumnya berhasil mengidentifikasi pengaruh tata kelola TI (TKTI) terhadap kinerja organisasi (KO), dimediasi penuh oleh TD. Namun masih diperlukan pendalaman mengenai rancangan mekanisme pengelolaan keamanan informasi untuk mengawal perjalanan TD. Penelitian ini menggunakan pendekatan *Design Science Research* (DSR) berbasis kerangka kerja terkini dari ISACA yaitu COBIT 2019 *Information Security Focus Area*. Studi kasus dilakukan di BankCo, dengan pengumpulan data melalui wawancara dan triangulasi dokumen. Perancangan solusi dan *roadmap* implementasi dilakukan berdasarkan kesenjangan yang didapatkan dari hasil penilaian tujuh komponen pada ketiga prioritas BankCo yaitu DSS05 *Managed Security Services*, APO13 *Managed Security*, dan BAI06 *Managed IT Changes*. Penelitian ini berkontribusi terhadap basis pengetahuan mengenai pengelolaan keamanan informasi pada DT, serta secara praktis khususnya bermanfaat bagi BankCo untuk mengawal perjalanan TD-nya, dan umumnya bagi industri terkait.

Kata Kunci: Transformasi Digital; Tata Kelola dan Manajemen TI; COBIT 2019 *Information Security*; *Design Science Research*; Bank

1. Pendahuluan

Kemunculan teknologi digital, kecepatan inovasi digital pesaing, dan perubahan perilaku konsumen telah mengganggu banyak perusahaan *incumbent* dan membuat mereka kehilangan pangsa pasar dengan cepat [1]. Hal ini menyebabkan perubahan pada *customer behavior, stakeholder behavior*, serta COVID 19 membuat perusahaan-perusahaan harus melakukan transformasi digital (TD). Transformasi Digital (TD) pada studi ini adalah "*proses perubahan mendasar, yang dimungkinkan oleh penggunaan teknologi digital yang inovatif disertai dengan pengaruh strategis sumber daya dan kemampuan utama, yang bertujuan untuk meningkatkan*

entitas (seperti, organisasi, jaringan bisnis, industri, atau masyarakat) secara radikal dan mendefinisikan kembali proposisi nilainya bagi para pemangku kepentingannya" [2, p. 13].

Mulyana dkk. [3] menyatakan bahwa pendekatan *agile*/adaptif dapat membantu organisasi dalam melakukan transformasi digital dengan menyediakan solusi dengan cepat melalui inovasi digital meskipun menghadapi risiko dan ketidakpastian yang lebih tinggi. Mulyana dkk. [3] juga menyatakan ditemukan juga bahwa tidak semua inisiatif TI dan digital cocok untuk diwujudkan dengan pendekatan *agile*/adaptif, pendekatan seperti ini lebih cocok untuk solusi cepat, lebih mengandalkan fitur yang menarik, waktu pemasaran yang lebih cepat, dan persyaratan yang belum dirinci. Kemudian pada penelitian studi Delphi sebelumnya yang dilakukan oleh Mulyana dkk. [3] telah teridentifikasi 46 mekanisme TKTI *hybrid* yang berpengaruh terhadap TD pada enam (6) dimensi TD. Penelitian ini mengambil definisi "*TKTI adalah bagian integral dari tata kelola perusahaan yang dilaksanakan oleh dewan dan membahas definisi dan implementasi proses, struktur, dan mekanisme dalam organisasi yang memungkinkan bisnis dan TI untuk melaksanakan tanggung jawab mereka dalam mendukung penyelarasan bisnis/TI dan penciptaan nilai bisnis dari investasi bisnis yang didukung TI*" [4, p. 11].

Terdapat regulasi terkait TKTI menurut Peraturan Otoritas Jasa Keuangan (OJK) No. 55/POJK.03/2016 tentang penerapan tata kelola bagi bank umum mengharuskan adanya penerapan tata kelola untuk bank umum semakin kompleksnya risiko yang dihadapi bank maka semakin meningkat pula kebutuhan praktik tata kelola yang baik oleh perbankan [5]. Dan Otoritas Jasa Keuangan [5]juga mencantumkan pada Peraturan OJK No. 55 /POJK.03/2016 tentang penerapan tata kelola bagi bank umum bahwa dalam rangka meningkatkan kinerja bank, melindungi kepentingan para pemangku kepentingan, dan meningkatkan kepatuhan terhadap peraturan perundang-undangan serta nilai-nilai etika yang berlaku umum pada industri perbankan, diperlukan pelaksanaan tata kelola yang baik.

Selain itu, pada Master Plan Sektor Jasa Keuangan 20212025 terdapat satu fokus area mengenai akselerasi Transformasi Digital [6]. Selanjutnya, pada peraturan Otoritas Jasa Keuangan Nomor 11 /POJK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum pada pasal 16 ayat (1) bahwa Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dan efisien [7]. Pada Penelitian ini juga mempertimbangkan Indonesia karena memiliki perkembangan ekonomi digital yang paling substansial diprediksi di negara-negara ASEAN dan memiliki pangsa pasar yang prospektif dalam pelayanan digital terutama pada sektor perbankan dan asuransi [8].

Dalam rangka pemenuhan kepatuhan terhadap regulasi, BankCo sebagai salah satu bank umum di bawah naungan BUMN, telah mengikuti kebijakan yang berlaku di Indonesia serta menerapkan TKTI dan pengamanan informasi. Penggunaan TI di BankCo diatur dalam kebijakan, standar, dan prosedur yang diterapkan secara konsisten dan berkesinambungan sesuai ketentuan regulasi Peraturan OJK No. 11/POJK.03/2022 perihal Penyelenggaraan Teknologi Informasi oleh Bank Umum yang meliputi aspek: TKTI Bank, Arsitektur TI Bank, Manajemen Risiko TI, Ketahanan dan Keamanan Siber, Penggunaan Pihak Penyedia Jasa TI, Penempatan Sistem Elektronik, Pengelolaan Data dan Perlindungan Data Pribadi, Penyedia Jasa TI Oleh Bank, Pengendalian Intern dan Audit Intern, Pelaporan, dan Penilaian Tingkat Maturitas Digital Bank.

Selain itu, BankCo juga harus mematuhi Peraturan Menteri BUMN Nomor PER02MBU032023 bahwa BUMN harus menjaga prinsip keamanan informasi sesuai dengan prinsip kerahasiaan, keutuhan, dan ketersediaan. Selain itu, regulasi tersebut juga menekankan untuk melakukan tata kelola perusahaan yang baik dengan menerapkan prinsip keterbukaan, akuntabilitas, tanggung jawab, kemandirian, dan keadilan [9].Sehingga berdasarkan Peraturan OJK No. 11/POJK.03/2022 dan PER02MBU032023, BankCo harus melakukan penerapan TKTI perusahaan yang baik dengan prinsip keamanan informasi, keterbukaan, akuntabilitas, tanggung jawab, kemandirian, dan keadilan. Untuk mematuhi regulasi tersebut, BankCo perlu menyusun TKTI dan manajemen keamanan informasi yang dapat membantu BankCo melakukan TD [10]. Kerangka kerja yang digunakan adalah COBIT 2019 dengan fokus area *information security* dengan menerapkan penilaian terhadap tujuh komponen.

Oleh karena itu, penelitian ini telah merumuskan beberapa pertanyaan penelitian (RQs) untuk merancang TKTI pada BankCo dengan menggunakan kerangka kerja COBIT 2019 *Information Security* yang dapat membantu BankCo menjalani upaya transformasi digital. Pertanyaan penelitian utama (RQ1) dari penelitian ini adalah: "Apa tujuan tata kelola dan manajemen teknologi informasi (TKMTI) keamanan informasi yang dibutuhkan oleh BankCo?" Pertanyaan penelitian kedua (RQ2) adalah: "Bagaimana menyusun rekomendasi optimalisasi

tujuan TKMTI pada BankCo berdasarkan hasil analisis kesenjangan tujuh komponen kemampuan yang dimiliki saat ini dan target?" Dan pertanyaan penelitian terakhir (RQ3) adalah: "Bagaimana merancang optimalisasi yang esensial pada tujuan TKMTI berdasarkan hasil penyusunan rekomendasi?"

2. Tinjauan Pustaka

Transformasi Digital (TD) adalah proses perubahan mendasar, yang dimungkinkan oleh penggunaan teknologi digital yang inovatif disertai dengan pengaruh strategis sumber daya dan kemampuan utama, yang bertujuan untuk meningkatkan entitas (seperti, organisasi, jaringan bisnis, industri, atau masyarakat) secara radikal dan mendefinisikan kembali proposisi nilainya bagi para pemangku kepentingannya [2, p. 12].

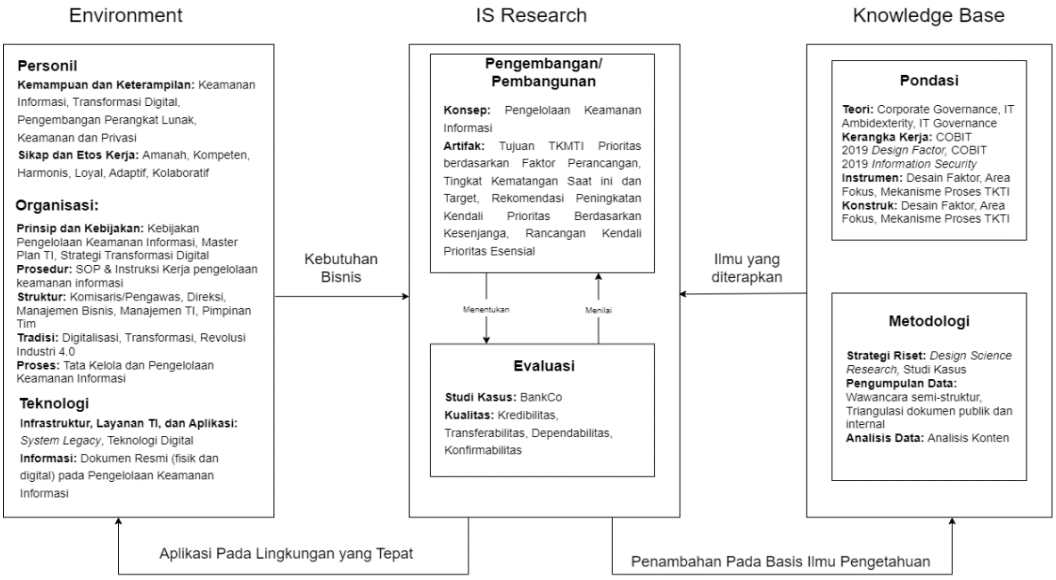
Transformasi digital juga mengandung orientasi budaya yang mengakui pentingnya pengambilan keputusan yang cepat dan fleksibel untuk bersaing dalam konteks yang tidak pasti (Warner & Wäger, 2019). Dalam dekade terakhir, teknologi digital yang disruptif, perilaku konsumen yang tidak terduga, dan persaingan yang mengganggu telah mempercepat tingkat perubahan yang belum pernah terjadi sebelumnya bagi *incumbent* [11].

Untuk mendukung TD, Tata Kelola TI tradisional saat ini diragukan keefektifannya. Tata Kelola TI tradisional ini membuat perusahaan menggunakan pendekatan yang lebih klasik untuk pengembangan perangkat lunak (waterfall) dan memisahkan pengembangan perangkat lunak dari operasi [12]. TKTI saat ini membutuhkan pendekatan agile yang dapat merespon dinamika yang berubah. Akibatnya, perusahaan sangat bergantung pada strategi agile untuk mengamankan kinerja perusahaan yang lebih baik. Dengan mengadopsi prinsip-prinsip agile, nilainilai, dan praktik terbaik dalam konteks TKTI dapat menyebabkan peningkatan kecepatan pengambilan keputusan, peningkatan proses bisnis,organisasi daya saing, dan aspek lainnya [13].

Dalam merancang TKTI untuk mendukung TD, telah dilakukan penelitian oleh Afifah, Nurafifah, dan Luthfia yang menguji bagaimana pengaruh TKTI terhadap TD dan kinerja organisasi pada industri perbankan [14]–[16]. Pada penelitian ini, dilakukan pembaharuan dari penelitian sebelumnya yang befokus dalam merancang tata kelola dan manajemen teknologi informasi (TKMTI), khususnya dalam manajemen keamanan informasi. Di mana, dalam manajemen keamanan informasi, terdapat perancangan manajemen keamanan informasi menggunakan ISO27001 [17], namun dalam penelitian ini, perancangan manajemen keamanan informasi di industri perbankan dilakukan dengan menerapkan pendekatan yang berbeda, yakni menggunakan *framework* COBIT 2019 *Information Security* dengan analisis terhadap tujuh komponen TKMTI [18], [19].

3. Metodologi

Penelitian ini mengimplementasikan kerangka *Design Science Research* (DSR) untuk merancang manajemen keamanan informasi serta membantu upaya transformasi digital BankCo.



Gambar 1 Model Konseptual [20]

Gambar 1 menampilkan DSR yang terbagi menjadi tiga (3) bagian, yaitu *environment* yang menjelaskan mengenai lingkup dari penelitian, *knowledge base* yang menjelaskan mengenai dasar ilmu yang digunakan *,* dan *information system research* yang menjelaskan hasil dari penelitian.

Gambar 2 Sistematika Penyelesaian Masalah [21]

Gambar 2 menampilkan lima (5) tahapan sistematika penyelesaian masalah, yaitu *problem explication, requirement specification, design and development, demonstration,* dan *evaluation*. *Problem explication* merupakan tahap dalam menyelidiki dan menganalisis masalah yang kemudian dirumuskan dengan tepat. *Requirement specification* merupakan tahap dalam merancang solusi yang dimulai dari menyusun daftar pertanyaan wawancara, menentukan prioritas tujuan TKMTI, analisis kesenjangan dari tujuh komponen, dan penyusunan rekomendasi. *Design and development* merupakan tahap dalam melakukan analisis rekomendasi perbaikan menggunakan analisis *risk, resourc*e, dan *value* serta menyusun rekomendasi perbaikan berdasarkan aspek *people*, *process*, dan *technology*. *Demonstration* merupakan tahapan penyusunan *roadmap* implementasi serta menganalisis pengaruh implementasi rancangan terhadap BankCo. *Evaluation* merupakan tahapan yang dilakukan untuk melakukan evaluasi hasil berdasarkan uji *credibility, transferability, dependability*, dan *confirmability* [22].

4. Hasil dan Pembahasan

4.1. Hasil Analisis Prioritas Tujuan TKMTI

Dalam menentukan prioritas tujuan TKMTI yang menjadi fokus pada penelitian ini, hasil dari *design factor* COBIT 2019 [12] dikalikan dengan nilai area fokus COBIT 2019 *Information Security* [18] dan prioritas mekanisme TKMTI [1], [23] menampilkan hasil analisis prioritas tujuan TKMTI.

Tabel 1 Hasil Prioritas Tujuan TKMTI

Tujuan TKMTI	Penilaian Desain Faktor	Penilaian Fokus Area	Penilaian Mekanisme	Penilaian Akhir
DSS05 *Managed Security Services*	95	2	5	950
APO13 *Managed Security*	80	2	5	800
BAI06 *Managed* IT *Changes*	100	1	4	400

Berdasarkan perhitungan yang telah dilakukan pada **Error! Reference source not f ound.**, didapatkan tiga (3) prioritas tujuan TKMTI tertinggi, yaitu DSS05 *Managed Security Services* dengan nilai prioritas akhir sebesar 950, APO13 *Managed Security* dengan nilai prioritas akhir 800, dan BAI06 *Managed IT Changes* dengan nilai prioritas akhir 400.

4.2. Hasil Analisis Penilaian dan Kesenjangan

4.2.1 Komponen Proses

Tabel 2 menampilkan bahwa BankCo hanya memiliki satu (1) kesenjangan pada praktik manajemen APO13. Adapun rata-rata skor tingkat kemampuan pada masing-masing tujuan TKMTI adalah 3,3 pada APO13, 3,4 pada DSS05, dan 3,5 untuk BAI06

Tabel 2 Hasil Penilaian dan Analisis Kesenjangan Komponen Proses

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
APO13 *Managed Security*		
APO13.01	100% F (*Fully*)	2
APO13.02	67% L (*Largely*)	3
	100% F (*Fully*)	4
APO13.03	100% F (*Fully*)	4
	100% F (*Fully*)	5
Rata-Rata Skor Tingkat Kemampuan		3,3
DSS05 *Managed Security Services*		
DSS05.01	100% F (*Fully*)	2
	100% F (*Fully*)	3
	100% F (*Fully*)	4
DSS05.02	100% F (*Fully*)	2
	100% F (*Fully*)	3
	100% F (*Fully*)	4
DSS05.03	100% F (*Fully*)	2
	100% F (*Fully*)	3
DSS05.04	100% F (*Fully*)	2
	100% F (*Fully*)	3
	100% F (*Fully*)	4
DSS05.05	100% F (*Fully*)	2
	100% F (*Fully*)	3
DSS05.06	100% F (*Fully*)	2
	100% F (*Fully*)	3
DSS05.07	100% F (*Fully*)	2
	100% F (*Fully*)	3
Rata-Rata Skor Tingkat Kemampuan		3,4
BAI06 *Managed IT Changes*		
BAI06.01	100% F (*Fully*)	2
	75% L (*Largely*)	3
BAI06.02	100% F (*Fully*)	2
	100% F (*Fully*)	3
	100% F (*Fully*)	4
BAI06.03	100% F (*Fully*)	4
BAI06.04	100% F (*Fully*)	2
	100% F (*Fully*)	3
Rata-Rata Skor Tingkat Kemampuan		3,5

4.2.2 Komponen Struktur Organisasi

Tabel 3 menampilkan bahwa BankCo hanya memiliki satu (1) kesenjangan pada komponen struktur organisasi, di mana BankCo belum memiliki peran terkait Program Manager.

Tabel 3 Hasil Penilaian dan Analisis Kesenjangan Komponen Struktur Organisasi

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
Chief Information Officer	APO13, DSS05, dan BAI06	Direktur IT & *Operations*
Chief Technology Officer	APO13	
Chief Information Security Officer	APO13 dan DSS05	
Enterprise Risk Committee	APO13	Komite Pemantauan Risiko
Business Process Owners	APO13, DSS05, dan BAI06	*Business Owners*

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
Program Manager	BAI06	BankCo belum memiliki *Program Manager*
Project Manager	BAI06	*Project Manager*
Project Management Office	APO13	*Project Management Office*
Head Architect	APO13	*Head* IT *Strategy & Architecture*
Head Development	APO13, DSS05, dan BAI06	*Head* IT *Developmen*t
Head Human Resources	DSS05	*Head Human Capital Service*
Head IT *Operations*	APO13, DSS05, dan BAI06	*Head IT Operations*
Head IT *Administration*	APO13	
Business Continuity Manager	BAI06	*Business Continuity Manager*
Service Manager	APO13 dan BAI06	Unit Kualitas Layanan
Information Security Manager	APO13, DSS05, dan BAI06	*Head Information Security*
Privacy Officer	APO13, DSS05 dan BAI06	Direktur *Human Capital & Compliance*

4.2.3 Komponen Informasi

Tabel 4 menampilkan bahwa BankCo memiliki satu (1) kesenjangan pada komponen informasi, di mana sudah memiliki *service catalog*, namun hanya mencakup sebagian layanan TI.

Tabel 4 Hasil Penilaian dan Analisis Kesenjangan Komponen Informasi

Praktik Manajemen	*Information Output*	Kondisi Saat Ini
DSS05 *Managed Security Services*		
DSS05.01 Melindungi dari perangkat lunak berbahaya.	*Information Security Management Reports*	Laporan Audit TI
	Information Security Service Catalog	Sudah ada *service catalog* namun belum mencakup seluruh layanan TI, hanya sebagian dari divisi operasional TI
DSS05.02 Mengelola keamanan jaringan dan konektivitas.	*Connectivity Security Policy*	Standar Keamanan Interkoneksi Internet dan Jaringan
	Results Of Penetration Tests	BankCo telah melakukan *penetration testing*, namun tidak akses melihat laporan terkait *penetration testing*
DSS05.03 Kelola keamanan titik akhir.	*Security Policies for Endpoint Devices*	Prosedur Pengamanan Perangkat *End Point*
DSS05.04 Kelola identitas pengguna dan akses logis.	*Results of Reviews of User Accounts and Privileges*	Dokumen pengelolaan akses sistem, dokumen pembuatan dan penghapusan hak akses karyawan, hasil pengelolaan *user ID* dan *password* melalui aplikasi *identity management*, Kebijakan Pembatasan Akses Terhadap Sistem dan Informasi.
	Approved User Access Rights	Kebijakan pengelolaan akses *user*.
DSS05.05 Mengelola akses fisik ke aset I&T.	*Access Logs*	Dokumen pengamanan perangkat keras dan peralatan lainnya, berisi prosedur pengelolaan *log*.
	Approved Access Requests	Prosedur pengendalian hak akses karyawan.
DSS05.06 Kelola dokumen sensitif dan perangkat keluaran.	*Access Privileges*	Dokumen pengamanan informasi, berisi prosedur pengelolaan *user privileged*.
	Inventory of Sensitive Documents and Devices	Inventaris aset maupun dokumen yang bersifat sensitif atau *confidential*.
DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian terkait keamanan.	*Security Incident Tickets*	Kebijakan pendeteksian dan penanganan insiden keamanan informasi.

Praktik Manajemen	*Information Output*	Kondisi Saat Ini
	Security Incident Characteristics	Petunjuk teknis pendeteksian dan penanganan insiden keamanan informasi
	Security Event Logs	*Procedure disaster recovery plan*,
APO13 *Managed Security*		
APO13.01 Menetapkan dan memelihara sistem manajemen keamanan informasi (ISMS).	ISMS *Scope Statement*	Dokumen ISMS unit keamanan informasi
	IS *Policy*	Dokumen kebijakan pengamanan informasi
APO13.02 Menetapkan dan mengelola rencana penanganan risiko keamanan dan privasi informasi.	IS *Risk Treatment Plan*	Dokumen BankCo ITSP
	IS *Business Case*	Laporan akhir audit IT
APO13.03 Pantau dan tinjau sistem manajemen keamanan informasi (ISMS).	IS Review Report	Dokumen audit IT internal dan eksternal
BAI06 *Managed IT Changes*		
BAI06.01 Mengevaluasi, mengutamakan, dan mengotorisasi permintaan perubahan.	*Impact Assessments*	Dokumen prosedur *Change Advisory Forum* (CAF) dan *Change Control Committee* (CCC)
BAI06.03 Melacak dan melaporkan status perubahan.	*Updated Change Request Status Reports*	Dokumen prosedur *Change Control Committee* (CCC)
BAI06.04 Menutup dan mendokumentasikan perubahan.	*Change Documentation*	Dokumen prosedur *Change Advisory Forum* (CAF)

4.2.4 Komponen Orang, Keterampilan, dan Kompetensi

Tabel 5 menampilkan bahwa BankCo memiliki satu (1) kesenjangan pada komponen orang, keterampilan, dan kompetensi. Di mana, BankCo belum memiliki perancangan dan pengembangan strategi keamanan informasi yang terintegrasi..

Tabel 5 Hasil Penilaian dan Analisis Kesenjangan Komponen Orang, Keterampilan, dan Kompetensi

Kemampuan	Kondisi Saat Ini
DSS05 *Managed Security Services*	
Information Security	Staf IT BankCo telah melakukan pelatihan keamanan informasi telah sertifikasi CISSP (*Certified Information Systems* Security) dan sertifikasi ISO 27001.
Information Security Management	Staf IT BankCo telah melakukan pelatihan keamanan informasi telah sertifikasi ISO 27001 *Lead Implementer*.
Penetration Testing	Telah mengikuti dan tersertifikasi *Certified Ethical Hacker* (CEH)
Security Administration	Meninjau kontrol keamanan yang diterapkan termasuk pembaharuannya serta mengelola hak akses untuk melihat, mengubah dan mengajukan permintaan hapus data. Staf IT telah *Certified Ethical Hacker* (CEH) *Certified Information Security Manager* (CISM).
DSS05 *Managed Security Services*	
Information Security	BankCo telah melakukan pemasangan antimalware dan antivirus, membatasi hak akses, dan melakukan pelatihan keamanan informasi serta staf TI telah sertifikasi ISO 27001.
Information Security Strategy Development	Belum terdapat perancangan dan pengembangan strategi keamanan informasi yang terintegrasi.
BAI06 *Managed IT Changes*	
Change Management	Staf TI BankCo telah mengikuti dan memiliki sertifikasi *Project Management Professional* (PMP).
Change Support	Staf TI BankCo telah mengikuti dan memiliki sertifikasi *Project Management Professional* (PMP)

4.2.5 Komponen Kebijakan dan Prosedur

Tabel 6 menampilkan bahwa BankCo tidak memiliki kesenjangan pada komponen kebijakan dan prosedur.

Tabel 6 Hasil Penilaian dan Analisis Kesenjangan Komponen Kebijakan dan Prosedur

Kebijakan	Kondisi Saat Ini
DSS05 *Managed Security Services*	
Kebijakan keamanan informasi	Kebijakan tata kelola dan pengelolaan TI, kebijakan pembatasan akses terhadap sistem dan informasi, Kebijakan penggunaan standarisasi ISO 27001 Kebijakan pembatasan akses terhadap sistem dan informasi, Kebijakan pengamanan password, Kebijakan dan prosedur pengelolaan userID dan password, Kebijakan pengamanan informasi bagi pengguna, Kebijakan pelatihan dan sosialisasi keamanan informasi secara rutin untuk pegawai, Kebijakan pendeteksian dan penanganan insiden keamanan informasi, Prosedur pengamanan perangkat end point, Prosedur clear desk dan clear screen, Prosedur pengelolaan perangkat internet security, Prosedur pengamanan PC dan perangkat kerja, Prosedur antisipasi pengamanan terhadap serangan virus.
APO13 *Managed Security*	
Keamanan informasi dan kebijakan privasi	Perlindungan aset, privasi, data, dan ISO 27001, Pengamanan Perangkat Keras dan Peralatan Lainnya (Kebijakan C*lear Screen*), Kebijakan Antisipasi Pengamanan Terhadap Serangan Virus, Kebijakan Pengamanan *Password*, dan Pengelolaan Kebijakan Akses Sistem.
BAI06 *Managed IT Changes*	
Kebijakan manajemen perubahan TI – Minimalkan risiko dan dampak perubahan pada TI perusahaan. Meliputi aset yang relevan dan proses manajemen perubahan standar.	Kebijakan pengelolaan prosedur *change control*, Prosedur *Architecture Review Forum*, Prosedur *Change Adviosry Forum*, Prosedur *Change Oversight Forum* (COF), dan Prosedur *Emergency Change Advisory Forum* (ECAF).

4.2.6 Komponen Budaya, Etika, dan Perilaku

Tabel 7 menampilkan bahwa BankCo tidak memiliki kesenjangan pada komponen budaya, etika, dan perilaku.

Tabel 7 Hasil Penilaian dan Analisis Kesenjangan Komponen Budaya, Etika, dan Perilaku

Elemen Kunci Budaya	Kondisi Saat Ini
DSS05 *Managed Security Services*	
Membentuk budaya kesadaran pengguna dalam menjaga praktik keamanan dan privasi.	Memberikan pelatihan dan sosialisai pemahaman tata kelola, keamanan informasi, privasi, dan keamanan data serta mendapatkan sertifikasi ISO 27001.
APO13 *Managed Security*	
Membentuk budaya kesadaran akan keamanan dan privasi untuk mendorong perilaku yang diinginkan dan implementasi kebijakan keamanan dan privasi dalam praktik seharihari.	Pelatihan dan Sosialisasi Kepada Pegawai dengan membuat Kebijakan Pelatihan dan Sosialisasi Keamanan Informasi Secara Rutin Untuk Pegawai.
BAI06 *Managed IT Changes*	
Pemimpin harus mendorong budaya peningkatan berkelanjutan dalam solusi dan layanan TI, dengan mempertimbangkan dampak perubahan teknologi pada perusahaan, mengelola risiko dan biaya, serta mengevaluasi manfaat dan kesesuaian dengan strategi TI dan tujuan perusahaan.	Di dalam kebijakan BankCo, BankCo memberikan pelatihan dan sosialisasi pemahaman tata kelola dan keamanan informasi, privasi, dan keamanan data serta mendapatkan sertifikasi ISO 27001 untuk karyawannya.

4.2.7 Komponen Layanan, Infrastruktur, dan Aplikasi

Tabel 8 menampilkan bahwa BankCo memiliki satu (1) kesenjangan pada komponen layanan, infrastruktur, dan aplikasi. Di mana, BankCo belum memiliki *tools* terkait *Security Information and Event Management* (SIEM).

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

Kemampuan	Kondisi Saat Ini
DSS05 *Managed Security Services*	
Directory Services	*Single SignOn* (SSO).
Email Filtering Systems	Layanan pengamanan menggunakan *email*
Identity and Access Management System	Layanan autentikasi dan otorisasi akses, *Single SignOn* (SSO), dan Biometrik
Security Awareness Services	Program pengembangan kompetensi sumber daya manusia atau pelatihan terkait keamanan, serta layanan edukasi pengamanan transaksi dan data pribadi melalui situs web BankCo.
Security Information and Event Management (SIEM) *Tools*	BankCo belum memiliki tools SIEM
Security Operations Center (SOC) *Services*	Layanan *Security Operations Center* (SOC) BankCo berupa pemantauan *cybersecurity*
ThirdParty Security Assessment Services	*Penetration testing* dan simulasi *phising*
URL Filtering Systems	Standar keamanan interkoneksi internet dan jaringan
APO13 *Managed Security*	
Configuration Management Tools	Jenkins, GitHub
Security and Privacy Awareness Services	Pelatihan kesadaran keamanan dan privasi
Thirdparty Security Assessment Services	*Assessment* ISO 27001
BAI06 *Managed IT Changes*	
IT *Changes Management Tools*	Remedy
Configuration management tools	Jenkins, GitHub

4.3 Perbaikan Potensial

Perbaikan potensial memiliki tujuan untuk menentukan perbaikan yang dapat dilakukan guna mengatasi kesenjangan yang telah teridentifikasi pada BankCo. Perbaikan potensial terbagi menjadi tiga (3) aspek, yaitu aspek *people*, *process*, dan *technology*. Tabel 9 menampilkan perbaikan potensial pada aspek *people, process,* dan *technology*.

Tabel 9 Perbaikan Potensial Aspek *People, Process*, dan *Technology*

Komponen	Type	Perbaikan Potensial
Aspek *People*		
APO13 Managed Security		
Orang, Keterampilan, dan Kompetensi	*Skills & Awareness*	Meningkatkan pengetahuan, pengalaman, dan kemampuan dalam memahami tentang standar kerangka kerja keamanan informasi untuk mengembangkan strategi keamanan informasi yang efektif.
BAI06 *Managed IT Changes*		
Struktur Organisasi	*Roles*	Menambahkan tanggung jawab Program Manager ke dalam struktur organisasi BankCo yang bertanggung jawab dalam mengawasi dan mengevaluasi keseluruhan jalannya program untuk memastikan keberhasilannya, termasuk merencanakan dan mengelola seluruh rangkaian proyek dalam membentuk suatu program.
Aspek *Process*		
DSS05 Managed Security Services		
Informasi	*Record*	Menambahkan service catalog untuk seluruh layanan dan divisi TI
APO13 Managed Security		

Komponen	Type	Perbaikan Potensial
Proses	*Record*	Menyusun pedoman penyusunan proposal untuk mengimplementasikan rencana penanganan risiko keamanan informasi
BAI06		
Proses	*Policy*	*Menyusun template Kebijakan manajemen perubahan terhadap keamanan informasi*
Aspek *Technology*		
DSS05		
Layanan, Infrastruktur, dan Aplikasi	*Tools*	*Menambahkan tools Security Information and Event Management (SIEM) yang berfungsi dalam mengelola keamanan informasi serta peristiwaperistiwa (security events) yang terjadi dalam lingkungan TI suatu organisasi.*

4.4 Prioritas *Roadmap* Implementasi Berdasarkan Analisis Resource, Risk, dan Value

Tabel 10 menampilkan prioritas implementasi berdasarkan analisis *resources, risk, value* (RRV).

Tabel 10 Prioritas *Roadmap* Implementasi Berdasarkan Anaisis *Resource*, *Risk*, dan *Value*

Perbaikan Potensial	Skor	Prioritas
Aspek *People*		
Menambahkan tanggung jawab Program Manager ke dalam struktur organisasi BankCo dalam membimbing program dan mengelola risiko serta dampaknya terhadap bisnis.	*12*	*2*
Meningkatkan pengetahuan, pengalaman, dan kemampuan dalam perancangan dan pengembangan strategi keamanan informasi yang terintegrasi melalui pelatihan dan sertifikasi.	*12*	*1*
Aspek *Process*		
Menambahkan service catalog yang mencakup mencakup seluruh layanan TI	8	5
Menyusun pedoman penyusunan proposal untuk mengimplementasikan rencana penanganan risiko keamanan informasi.	12	3
Menyusun Kebijakan manajemen perubahan terhadap keamanan informasi	12	4
Aspek *Technology*		
Menambahkan tools *Security Information and Event Management* (SIEM) yang berfungsi dalam mengelola keamanan informasi serta peristiwaperistiwa (security events) yang terjadi dalam lingkungan TI suatu organisasi.	*9*	*6*

4.5 Rancangan Rekomendasi

Perancangan rekomendasi pada aspek *people* menghasilkan dua (2) rekomendasi, yaitu penambahan tanggung jawab terkait program *manager*, yakni pengawasan serta evaluasi keseluruhan jalannya program pada peran *IT Strategy* and *Architecture*. Selain itu, terdapat rekomendasi untuk melakukan pelatihan terkait keamanan informasi guna meningkatkan kemampuan mencakup pelatihan terkait standar dalam keamanan informasi untuk melindungi aset perusahaan dari kerentanan.

4.5.1 Rekomendasi Aspek *People*

Perancangan rekomendasi pada aspek *people* menghasilkan dua (2) rekomendasi, yaitu penambahan tanggung jawab terkait program manager, yakni pengawasan serta evaluasi keseluruhan jalannya program pada peran IT *Strategy* and *Architecture*. Selain itu, terdapat rekomendasi untuk melakukan pelatihan terkait keamanan informasi guna meningkatkan kemampuan mencakup pelatihan terkait standar dalam keamanan informasi untuk melindungi aset perusahaan dari kerentanan.

4.5.2 Rekomendasi Aspek *Process*

Perancangan rekomendasi pada aspek *process* menghasilkan tiga (3) rekomendasi, yakni penyusunan pedoman pembuatan proposal rencana penanganan risiko, pedoman penyusunan service catalog, serta penyusunan kebijakan terkait manajemen perubahan.

4.5.3 Rekomendasi Aspek *Technology*

Perancangan rekomendasi pada aspek *technology* menghasilkan satu (1) rekomendasi, yaitu mengimplementasikan aplikasi Splunk Enterprise sebagai *tools* dalam *security information and event management* (SIEM) [24].

4.6 *Roadmap* Implementasi

Tabel 11 menampilkan *roadmap* implementasi yang dapat dijadikan pedoman oleh BankCo dalam mengimplementasikan rancangan rekomendasi yang telah dibuat.

Tabel 11 *Roadmap* Implementasi

Rekomendasi	Prioritas	*Roadmap Timeline (Quarter)* 2023 1	2	3	4	2024 1	2	3	4
Aspek *People*									
Meningkatkan pengetahuan, pengalaman, dan kemampuan dalam perancangan dan pengembangan strategi keamanan informasi yang terintegrasi melalui pelatihan dan sertifikasi.	1								
Menambahkan tanggung jawab *Program Manager* ke dalam struktur organisasi BankCo dalam membimbing program dan mengelola risiko serta dampaknya terhadap bisnis.	2								
Aspek *Process*									
Menyusun pedoman penyusunan proposal untuk mengimplementasikan rencana penanganan risiko keamanan informasi.	3								
Menyusun pedoman penyusunan laporan penilaian dampak potensial dari perubahan terhadap keamanan informasi	4								
Menambahkan s*ervice catalog* yang mencakup mencakup seluruh layanan TI	5								
Aspek *Technology*									
Mengimplementasikan *tools Security Information and Event Management* (SIEM) yang berfungsi dalam mengelola keamanan informasi serta peristiwaperistiwa (*security events*) yang terjadi dalam lingkungan TI suatu organisasi.	6								

4.7 Pengaruh Rancangan

Setelah melakukan perancangan rekomendasi berdasarkan aspek *people*, *process*, dan *technology*, dilakukan komparasi untuk melihat kondisi BankCo sebelum dan sesuah dilakukannya penerapan rancangan rekomendasi tersebut. Tabel 12 menampilkan estimasi pengaruh perancangan rekomendasi pada komponen proses.

Tabel 12 Estimasi Pengaruh Perancangan Rekomendasi pada Komponen Proses

Tujuan TKMTI	Skor Tingkat Kemampuan Sebelum Perbaikan	Skor Tingkat Kemampuan Sesudah Perbaikan
DSS05 *Managed Security Services*	3,4	3,4
APO13 Managed Security	3,3	3,6
BAI06 Managed IT Changes	3,5	3,5

Tabel 13 menampilkan estimasi pengaruh perancangan rekomendasi pada komponen struktur organisasi, informasi, orang, keterampilan, dan kompetensi serta layanan, infrastruktur, dan aplikasi.

Tabel 13 Estimasi Pengaruh Perancangan Rekomendasi

Sebelum Perbaikan	Setelah Perbaikan

Komponen Struktur Organisasi	
BankCo belum memiliki tanggung jawab terkait *Program Manager*.	Penambahan tanggung jawab terkait *Program Manager* pada divisi IT *Strategy & Architecture*
Komponen Informasi	
BankCo belum memiliki *service catalog*	Dokumen *Service Catalog*
Komponen Orang, Keterampilan dan Kompetensi	
BankCo belum memiliki keterampilan untuk dapat mengembangkan strategi keamanan informasi yang efektif.	Pelatihan terkait pengembangan strategi keamanan informasi yang efektif, seperti pelatihan CISA, CISSP, CISM, dan CIS
Komponen Layanan, Infrastruktur, dan Aplikasi	
BankCo belum memiliki *tools* terkait *Security Information and Event Management* (SIEM)	Splunk Enterprise

4.8 Pembahasan Hasil Studi

Penelitian sebelumnya menyatakan bahwa mekanisme struktur, proses, dan relasional TKTI berpengaruh terhadap TD dan kinerja organisasi [14]–[16]. Ditemukan bahwa pendekatan *agile*/adaptif dapat membantu organisasi dalam melaksanakan TD, namun tidak semua inisiatif digital cocok untuk direalisasikan dengan pendekatan *agile*/adaptif [3]. Pendekatan ini lebih cocok untuk model bisnis baru yang membutuhkan solusi cepat. Sedangkan untuk proses bisnis kritis seperti aplikasi perbankan inti dan asuransi, para ahli tidak merekomendasikan penggunaan pendekatan *agile*/adaptif. Di sisi lain, industri perbankan dan asuransi yang telah ada di Indonesia terikat oleh regulasi yang relatif kaku yang memerlukan dokumentasi pekerjaan yang formal, dibandingkan dengan pendekatan *agile* yang cenderung memiliki dokumentasi yang lebih informal. Sehingga, perusahaan *incumbent* membutuhkan TKTI *hybrid* berupa perpaduan antara pendekatan tradisional dan adaptif untuk mengawal keberhasilan TD untuk meningkatkan pencapaian kinerja pada organisasi [23]. Oleh karena itu, Pada penelitian ini, ditemukan bahwa BankCo membutuhkan dukungan TKMTI dengan memadukan pendekatan tradisional dan adaptif, sehingga diperlukan pengawalan manajemen keamanan informasi. Oleh karena itu, pendekatan *Design Science Research* (DSR) berbasis *framework* COBIT 2019 *Information Security* dapat menjadi solusi alternatif dalam memenuhi kebutuhan manajemen keamanan informasi dalam mengawal perusahaan *incumbent*, khususnya pada sektor perbankan dalam melakukan TD.

5. Simpulan

Berdasarkan hasil analisis penelitian, dalam melakukan proses prioritas tujuan TKMTI, dapat dilakukan dengan tiga tahapan yaitu berdasarkan faktor desain, area fokus keamanan informasi, dan mekanisme TKMTI. Dari ketiga pertimbangan tersebut didapatkan tiga prioritas tujuan TKMTI keamanan informasi BankCo yaitu, DSS05 *Managed Security Services*, APO13 *Managed Security*, dan BAI06 *Managed IT Changes*. Setelah dilakukan analisis kesenjangan terhadap tujuh (7) komponen, terdapat total enam (6) perbaikan potensial yang terbagi menjadi tiga (3) aspek, yakni aspek *people*, *process*, dan *technology*. Perancangan rekomendasi didasari oleh perbaikan potensial yang telah teridentifikasi berdasarkan aspek *people*, *process*, dan *technology*. Pada aspek *people*, terdapat penambahan tanggung jawab terkait program manager, yakni pengawasan serta evaluasi keseluruhan jalannya program pada peran *IT Strategy* and *Architecture*. Selain itu, terdapat rekomendasi untuk melakukan pelatihan terkait keamanan informasi guna meningkatkan kemampuan mencakup pelatihan terkait standar dalam keamanan informasi untuk melindungi aset perusahaan dari kerentanan. Pada aspek process, terdapat penyusunan pedoman pembuatan proposal rencana penanganan risiko, pedoman penyusunan *service catalog*, serta penyusunan kebijakan terkait manajemen perubahan. Dan terakhir pada aspek *technology*, terdapat komparasi *tools* yang dapat dijadikan referensi oleh BankCo untuk mengimplementasikan aplikasi yang tepat terkait *security information and event management* (SIEM). Seluruh perancangan rekomendasi tersebut dapat mendukung BankCo dalam melakukan transformasi digital. Penelitian ini berkontribusi dalam memperluas pengetahuan mengenai konsep prioritas pengelolaan keamanan informasi dalam mendukung transformasi digital organisasi, dan sangat berguna bagi BankCo dalam mengawal keberhasilan program strategisnya, serta bagi industri perbankan secara umum di Indonesia.

Daftar Referensi

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

[2] C. Gong and V. Ribiere, "Developing a unified definition of digital transformation," *Technovation*, vol. 102, p. 102217, Apr. 2021, doi: 10.1016/j.technovation.2020.102217.

[3] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry," *Pacific Asia Conference on Information Systems (PACIS), AI-IS-ASIA (Artificial Intelligence, Information Systems, in Pacific Asia), Virtual Conference, July 5-9, 2022. Association for Information Systems (AIS),* 2022.

[4] S. De Haes, L. Caluwe, T. Huygh, and A. Joshi, *Governing Digital Transformation: Guidance for Corporate Board Members*. in Management for Professionals. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-30267-2.

[5] Otoritas Jasa Keuangan Republik Indonesia, "Peraturan Otoritas Jasa Keuangan Republik Indonesianomor 11 /POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum." 2016.

[6] Otoritas Jasa Keuangan, "The Indonesian Financial Services Sector Master Plan." 2020.

[7] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11 /POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum." 2022.

[8] Google, Temasek, and Bain, "E-Conomy Sea 2020: At Full Velocity - Resilient and Racing Ahead." Syria Studies., 2020.

[9] Menteri BUMN, "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." 2023.

[10] P. M. Dewi, R. Fauzi, and R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework COBIT 2019 Domain Build, Acquire And Implement: Studi Kasus Bank XYZ.," *eProceedings of Engineering, vol. 8, no. 5, pp. 9672-9683,* 2019.

[11] K. S. R. Warner and M. Wäger, "Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal," *Long Range Planning*, vol. 52, no. 3, pp. 326–349, Jun. 2019, doi: 10.1016/j.lrp.2018.12.001.

[12] ISACA, *COBIT® 2019 Framework: introduction and methodology*. Schaumburg, Illinois: ISACA, 2018.

[13] S. Vejseli and A. Rossmann, "The Impact of IT Governance on Firm Performance A Literature Review," 2017.

[14] N. Afifah, R. Mulyana, and L. Abdurrahman, "Survei Pengaruh Tata Kelola TI terhadap Transformasi Digital dan Kinerja Organisasi Bank," *Jurnal Sistem Informasi*, vol. 11, no. 2, pp. 1-13, 2022.

[15] T. Z. Nurafifah, R. Mulyana, and L. Abdurrahman, "Pengujian Model Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Bank A," *josh*, vol. 4, no. 1, pp. 73–82, Oct. 2022, doi: 10.47065/josh.v4i1.2257.

[16] F. Luthfia, R. Mulyana, and L. Ramadani, "Analisis Pengaruh Tata Kelola Ti Terhadap Transformasi Digital Dan Kinerja Bank B," *ZONAsi: Jurnal Sistem Informasi*, vol. 4, no. 2, pp. 100–116, 2022.

[17] B. Panjaitan, L. Abdurrahman, and R. Mulyana, "Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001:2013 Menggunakan Kontrol Annex : Studi Kasus Data Center PT. XYZ," *eProceedings of Engineering, vol. 8, no. 2, pp.* pp. 2813-2825, 2021.

[18] ISACA, *COBIT Focus Area: Information Security Using COBIT 2019*. ISACA, 2020.

[19] D. A. Permana, R. Fauzi, and R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework Cobit 2019 Domain Align, Plan, And Organise : Studi Kasus Di Bank XYZ," *e-Proceeding of Engineering*, vol. 8, no. 5, pp. 9672-9683, 2021.

[20] Hevner, March, Park, and Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, p. 75, 2004, doi: 10.2307/25148625.

[21] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[22] A. K. Shenton, “Strategies for ensuring trustworthiness in qualitative research projects,” *EFI*, vol. 22, no. 2, pp. 63–75, Jul. 2004, doi: 10.3233/EFI-2004-22201.
[23] R. Mulyana, L. Rusu, and E. Perjons, “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.*, 2023.
[24] Gartner, “Gartner Magic Quadrant & Critical Capabilities.” [Online]. Available: https://www.gartner.com/en/research/magic-quadrant