

## MANAJEMEN KEAMANAN INFORMASI UNTUK TRANSFORMASI DIGITAL INSURCO BERBASIS COBIT 2019 FOCUS AREA INFORMATION SECURITY

Muhammad Anugerah Andyas<sup>1</sup>, Rahmat Mulyana<sup>2</sup>, Widyatasya Agustika Nurtrisha<sup>3</sup>

<sup>1,2,3</sup> Pogram Studi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

Jl. Telekomunikasi Terusan Buah Batu, 40257, Bandung, Indonesia

e-mail: <sup>1</sup>anugerahandyas@student.telkomuniversity.ac.id, <sup>2</sup>rahmatmoelyana@telkomuniversity.ac.id,

<sup>3</sup>widyatasya@telkomuniversity.ac.id

### Abstrak

Penelitian sebelumnya telah menunjukkan kontribusi tata kelola TI untuk transformasi digital. Namun masih diperlukan pendalaman terkait peranan manajemen keamanan informasi dalam mengawal perubahan tersebut melalui studi kasus asuransi InsurCo. Hal ini dibutuhkan seiring dengan arahan terbaru PER-2/MBU/03/2023 tentang pedoman tata kelola korporasi serta Master Plan Sektor Jasa Keuangan Indonesia 2021–2025 mengenai akselerasi transformasi digital. Metode penelitian ini menggunakan Design Science Research berbasis data wawancara. Terpilih DSS05 Managed Security Service, APO13 Managed Security, dan APO12 Managed Risk sebagai prioritas implementasi COBIT 2019 Information Security Focus Area. Asesmen kapabilitas, analisis kesenjangan, penyusunan rekomendasi, perancangan solusi serta roadmap telah dilaksanakan pada tujuh komponen tata kelola terkait. Terestimasi peningkatan rata-rata kematangan sebesar 0,8 (29,6%) pada ketiga proses tersebut. Studi ini berkontribusi menambah basis pengetahuan pada konsep prioritasasi manajemen keamanan informasi dalam mendukung transformasi digital organisasi, serta secara praktis khususnya bermanfaat bagi InsurCo untuk mengawal kesuksesan program strategisnya, serta umumnya untuk industri asuransi.

**Kata kunci:** Transformasi digital, COBIT 2019, Manajemen Keamanan Informasi, Asuransi, Design Science Research.

### Abstract

Previous research has shown the contribution of IT governance to digital transformation. However, further exploration is needed regarding the role of information security management in overseeing such changes through a case study of InsurCo insurance company. This is necessary in line with the latest guidance provided by PER-2/MBU/03/2023 on corporate governance and the Indonesian Financial Services Sector Master Plan 2021–2025 regarding the acceleration of digital transformation. This research method utilizes Design Science Research based on interview data. DSS05 Managed Security Service, APO13 Managed Security, and APO12 Managed Risk were selected as the priority implementation areas of the COBIT 2019 Information Security Focus Area. Capability assessments, gap analysis, recommendation development, solution design, and roadmap have been conducted on the seven related governance components. An estimated average maturity improvement of 0,8 (29,6%) was observed in these three processes. This study contributes to the knowledge base on the concept of prioritizing information security management to support organizational digital transformation, and it is particularly beneficial for InsurCo in ensuring the success of its strategic programs, as well as for the insurance industry in general.

**Keywords:** Digital transformation, COBIT 2019, Information security management, Insurance, Design Science Research.

## 1. PENDAHULUAN

Saat ini, sistem informasi telah banyak diterapkan di hampir seluruh sektor di Indonesia, termasuk industri perasuransian [1], [2]. Perkembangan ini mendesak industri perasuransian agar selalu bertransformasi dalam segala hal agar dapat tetap bersaing di tengah era digital [3] [4], tak terkecuali InsurCo. InsurCo merupakan salah satu perusahaan asuransi yang ada di bawah naungan Badan Usaha Milik Negara (BUMN) dengan jaminan kesejahteraan bagi setiap pesertanya dalam memperoleh perlindungan yang terbaik. Untuk memberikan pelayanan yang maksimal bagi pesertanya, InsurCo harus melakukan transformasi digital yang bertujuan untuk memberikan daya saing perusahaan untuk

bertahan terhadap perubahan teknologi digital dari masa ke masa, inovasi kompetitor, dan perubahan perilaku konsumen [5].

Dalam rangka menuju transformasi digital pada InsurCo, dibutuhkan beberapa perubahan struktural seperti penerapan sistem tata kelola berbasis teknologi informasi untuk proses bisnis yang lebih efisien dan terintegrasi [6]. Transisi organisasi melalui transformasi digital dapat meningkatkan kapabilitas organisasi dalam pengelolaan infrastruktur TI dan memberikan pengembangan terhadap produk atau layanan sehingga dapat memberikan daya saing dalam industri [7].

Tata kelola teknologi informasi memiliki pengaruh yang positif terhadap transformasi digital, dan dapat meningkatkan kinerja organisasi [8]. Keberlangsungan Tata kelola teknologi informasi tidak dapat dilepaskan dari manajemen Keamanan informasi, karena pada dasarnya keamanan informasi memiliki tujuan untuk menjamin kelangsungan bisnis, memitigasi risiko bisnis serta memastikan jalannya investasi bisnis dengan baik dan memaksimalkan peluang yang ada [9]. Hal ini sejalan dengan Peraturan Menteri BUMN Nomor PER-2/MBU/03/2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan BUMN mencakup penerapan tata kelola, tingkat kematangan serta manajemen risiko agar terciptanya pengelolaan TI yang lebih terstruktur, aman dan memiliki nilai manfaat bagi perusahaan [10].

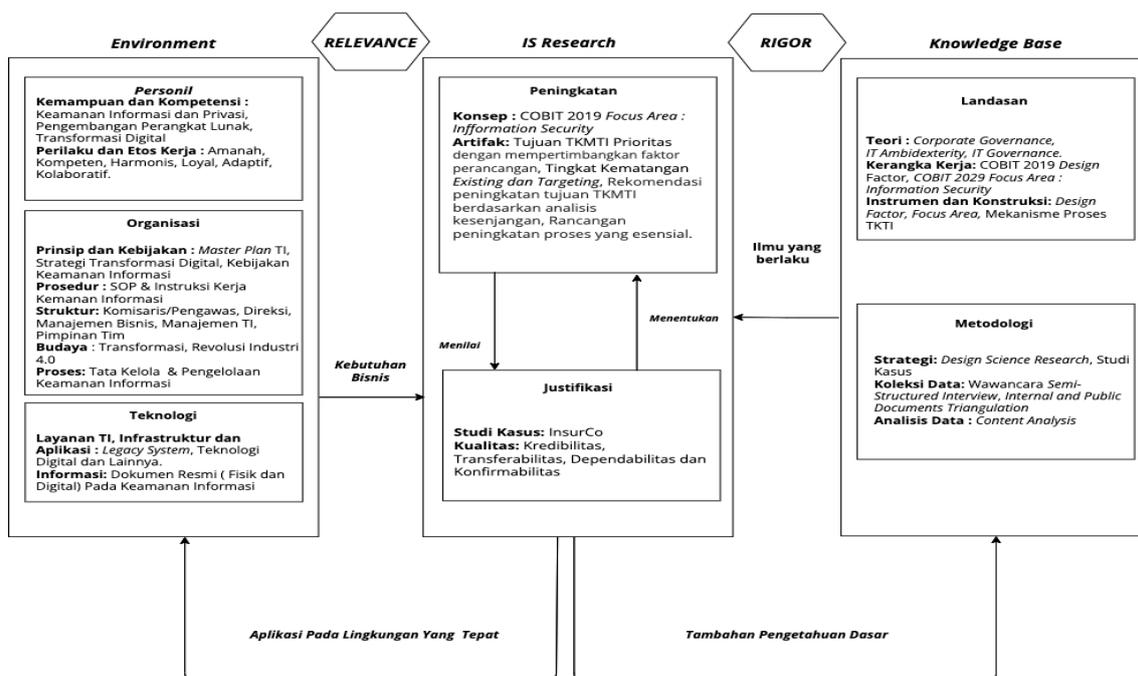
Akselerasi transformasi digital menjadi fokus Otoritas Jasa Keuangan dalam *Master Plan Sektor Jasa Keuangan 2021–2025* dengan tujuan menciptakan sektor jasa keuangan yang lebih modern, efisien, dan kompetitif di Indonesia. Selain itu, juga terdapat peraturan terkait yang mencakup keamanan data pribadi konsumen yaitu pedoman Otoritas Jasa Keuangan (POJK) Nomor 4/POJK.5/2021 yang menekankan semua perusahaan jasa keuangan Non-Bank wajib melindungi keamanan seluruh informasi dan rahasia serta keamanan data konsumen. Dengan adanya regulasi yang mendukung transformasi digital ini, akan menjadi pemicu bagi InsurCo dalam menyusun strategi perusahaan menuju transformasi digital, mengingat hasil studi sebelumnya menunjukkan bahwa InsurCo masih menjalankan pengelolaan TI tradisional secara menyeluruh, yang pada penerapannya masih memiliki kekurangan yang perlu dikembangkan untuk menghadapi tantangan transformasi digital [11], [12].

Di balik banyaknya manfaat yang didapatkan dalam penerapan Tata Kelola TI pada sektor keamanan informasi, juga terdapat ancaman terhadap keamanan informasi perusahaan [13]. Keamanan informasi merupakan upaya dalam memastikan serta menjamin dari semua ancaman yang berkaitan dengan fasilitas, data dan informasi dari penyalahgunaan pihak yang tidak memiliki hak atau tidak bertanggungjawab [14]. Selain itu, terdapat permasalahan keamanan informasi pada sektor perasuransian di Indonesia yang dapat dikatakan cukup kompleks dan berkaitan erat dengan ketersediaan data pribadi pelanggan serta kebijakan perusahaan terkait dengan pengelolaan data tersebut [15]. Dalam mengelola TI serta data pada perusahaan, dibutuhkan peran kerangka kerja TKMTI dengan standar internasional seperti COBIT, ITIL, ISO dan beberapa kerangka kerja lainnya dalam mendukung pengelolaan TI secara optimal [16]. COBIT 2019 adalah salah satu kerangka kerja yang digunakan sebagai praktik terbaik dalam mengelola teknologi informasi khususnya pada sektor keamanan informasi, karena pada pengimplementasiannya, COBIT 2019, memiliki bagian-bagian khusus yang membahas isu tertentu, dan dalam hal ini adalah *Focus Area Information Security* [17]

Oleh karena itu, penelitian ini telah merumuskan sejumlah pertanyaan penelitian, dalam rangka menyusun manajemen keamanan informasi untuk transformasi digital. Adapun pertanyaan penelitian utama ialah “Bagaimana tujuan TKMTI keamanan informasi yang dibutuhkan oleh InsurCo?” Yang diikuti oleh dua pertanyaan penelitian terkait dengan pertanyaan utama sebelumnya, yaitu “Bagaimana susunan rekomendasi optimalisasi kendali prioritas berdasarkan penilaian tujuh komponen saat ini dan ke depan?” Pertanyaan Penelitian Ketiga ialah “Bagaimana rancangan kendali optimal tujuh komponen tujuan TKMTI prioritas berdasarkan analisis kesenjangan yang telah dilakukan sebelumnya?” Untuk menjawab pertanyaan penelitian ini, kami melakukan pengumpulan data melalui proses wawancara semi terstruktur dan melalui metode *design science research* [18]

## 2. METODE PENELITIAN

Agar terstruktur dalam mencapai hasil yang diharapkan, penelitian ini menggunakan kerangka model berbasis *design science research (DSR)* [18]. Sebagaimana terlihat pada Gambar 1.

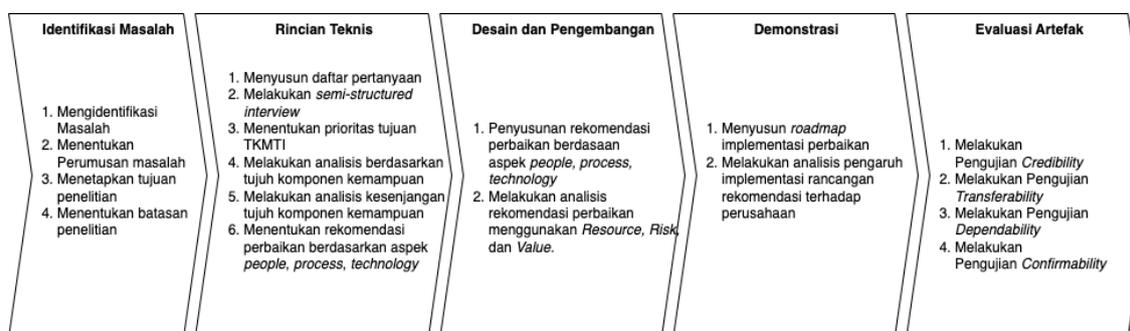


Gambar 1. Model Konseptual (Diadaptasi dari DSR Hevner [18])

Kerangka model konseptual pada penelitian ini memiliki tiga bagian utama, yang terdiri dari *environment*, *IS research* dan *knowledge base*. Ketiga bagian tersebut berperan dalam memudahkan pendefinisian masalah dan pemetaan masalah serta rincian. Penelitian ini bersifat kualitatif yang dimana pada pengimplementasiannya diperlukan sebuah analisis untuk mengetahui suatu permasalahan dengan mengumpulkan dan menganalisis sebuah data yang diperoleh melalui dokumen, data observasi dan wawancara [19].

Setelah itu, pengumpulan data pada penelitian ini dilakukan melalui metode wawancara semi terstruktur. Sehubungan dengan hal tersebut, penelitian ini dilakukan berdasarkan studi kasus untuk mendapatkan gambaran kondisi sebenarnya pada objek penelitian, serta agar lebih komprehensif [20], yang mana dalam penelitian ini akan menggunakan sistematika serta metodologi untuk berinteraksi secara sinergis dengan objek penelitian. Penelitian ini memiliki alur dan tahapan berbasis *design science research (DSR)*[21], sebagaimana terlihat pada

Gambar 2.



Gambar 2. Sistematika Penelitian (Diadaptasi dari DSR Hevner [22])

Tahap pertama penelitian dimulai dengan tahap identifikasi masalah. Pada tahap ini dilakukan pengidentifikasian masalah, perumusan masalah, penetapan tujuan serta penentuan batasan penelitian.

Tahap kedua merupakan tahap rincian teknis, yang dimana peneliti melakukan pengumpulan data melalui wawancara semi-terstruktur berdasarkan pertanyaan yang telah disusun sebelumnya. Setelah

data didapatkan, dilakukan prioritasi tujuan TKMTI dengan mempertimbangkan berbagai aspek meliputi prioritasi faktor desain[23] , area fokus [24], serta proses TKTI terhadap transformasi digital [25]. Setelah itu akan melakukan analisis penilaian tujuh komponen pada setiap tujuan TKMTI yang terpilih dengan menganalisis kesenjangan yang ditemukan dan menentukan perbaikan berdasarkan aspek *people*, *process* dan *technology* dari kesenjangan yang didapatkan.

Tahap ketiga merupakan tahap desain dan pengembangan, yang meliputi proses analisis rekomendasi perbaikan dengan menggunakan *resource*, *risk* dan *value* serta melakukan penyusunan rekomendasi perbaikan berdasarkan aspek *people*, *process* dan *technology*.

Tahap keempat atau tahap demonstrasi. Tahap ini meliputi proses penyusunan *roadmap* yang merupakan rekomendasi waktu pelaksanaan implementasi perbaikan dilakukan. Setelah itu, dilakukan analisis pengaruh sebelum dan setelah pengimplementasian rancangan perusahaan.

Tahap kelima atau evaluasi artefak, berdasarkan empat kriteria yang merupakan tolak ukur dalam melakukan evaluasi untuk menguji kualitas dalam penelitian kualitatif, yaitu pengujian *Credibility*, *Transferability*, *Dependability* dan *Confirmability* [26]. Setelah ke empat pengujian tersebut dilakukan, proses akan selesai.

### 3. HASIL DAN PEMBAHASAN

Pada penelitian ini, data yang didapatkan lalu dianalisis lebih lanjut untuk memperoleh informasi yang dapat membantu penelitian ini berlangsung. Terdapat dua jenis data yang berhasil didapatkan, terdiri dari data primer yang meliputi risiko umum serta kondisi internal dan data sekunder yang meliputi laporan dan rincian yang ada pada perusahaan serta regulasi yang berkaitan.

#### 3.1 Hasil Analisis Prioritas Tujuan TKMTI

Prioritasi tujuan TKMTI pada penelitian ini, didapatkan dengan mempertimbangkan 2 bagian dari COBIT 2019 yaitu faktor desain[27] dan area fokus keamanan informasi [28] serta mekanisme proses TKTI yang mempengaruhi TD [25], [29]. Setelah itu, dilakukan perhitungan perkalian terhadap 40 tujuan TKMTI dari ketiga aspek diatas yang menghasilkan prioritasi akhir seperti pada **Tabel 1**.

**Tabel 1.** Prioritasi Tujuan TKMTI

Tujuan TKMTI	Prioritasi Faktor Desain	Prioritisasi Area Fokus	Prioritisasi Mekanisme	Prioritisasi Akhir
DSS05 <i>Managed Security Services</i>	100	Inti (2)	5	1000
APO13 <i>Managed Security</i>	75	Inti (2)	5	750
APO12 <i>Managed Risk</i>	95	Relevan (1)	2	190

#### 3.2 Hasil Analisis Penilaian dan Kesenjangan Komponen Proses

Pada evaluasi kemampuan proses, InsurCo telah menetapkan target pemenuhan kematangan pada tingkat tiga (3) berdasarkan tujuan organisasi InsurCo agar dapat bersaing di era digital saat ini. Pada penilaian komponen proses jumlah *Capability level* yang ada, dibagi dengan jumlah keseluruhan pada manajemen praktik tersebut. Hasil analisis penilaian komponen proses didapatkan hasil sebesar 14,5 dari ketiga tujuan TKMTI pada kondisi saat ini, selengkapnya dapat dilihat pada Tabel 2.

**Tabel 2.** Penilaian Kemampuan Komponen Proses

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
<i>DSS05 Managed Security Services</i>		
DSS05.01	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
DSS05.02	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
DSS05.03	78% L ( <i>Largely Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3

Praktik Manajemen	Pencapaian	Tingkat Kemampuan
DSS05.04	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
DSS05.05	88% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
DSS05.06	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
DSS05.07	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
Total Nilai Terpenuhi:		17,0
Nilai Kemampuan:		2,4
<i>APO13 Managed Security</i>		
APO13.01	100% F ( <i>Fully Achieved</i> )	2
APO13.02	83% L ( <i>Largely Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
APO13.03	100% F ( <i>Fully Achieved</i> )	4
	100% F ( <i>Fully Achieved</i> )	5
Total Nilai Terpenuhi :		7,5
Nilai Kemampuan:		2,5
<i>APO12 Managed Risk.</i>		
APO12.01	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
APO12.02	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
	100% F ( <i>Fully Achieved</i> )	5
APO12.03	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
APO12.04	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
APO12.05	100% F ( <i>Fully Achieved</i> )	2
	100% F ( <i>Fully Achieved</i> )	3
APO12.06	100% F ( <i>Fully Achieved</i> )	3
	100% F ( <i>Fully Achieved</i> )	4
	100% F ( <i>Fully Achieved</i> )	5
Total Nilai Terpenuhi:		20
Nilai Kemampuan:		3,3

### 3.3 Hasil Analisis Penilaian dan Kesenjangan Komponen Struktur Organisasi

Setelah dilakukan analisis penilaian komponen struktur organisasi pada setiap prioritas tujuan TKMTI pada InsurCo, didapatkan hasil yang dapat dilihat pada Tabel 3.

**Tabel 3.** Penilaian Kemampuan Komponen Struktur Organisasi

Struktur Organisasi COBIT	Tujuan TKMTI	Kondisi Saat Ini
<i>Chief Information Officer</i>	DSS05, APO13, APO12, APO13, APO12.	Direktur Hubungan Kelembagaan membawahi Kepala Divisi Sistem Informasi, membawahi beberapa struktur organisasi seperti, Bidang Perencanaan dan Evaluasi TI, Bidang Pengembangan Aplikasi serta Bidang Operasional Sistem.
<i>Chief Information Security Officer</i>		
<i>Chief Technology Officer</i>		
<i>Chief Digital Officer</i>	APO12	
<i>Head Architect</i>	APO13, APO12, DSS05, APO13, APO12 APO12 APO12	Kepala Divisi Sistem Informasi, membawahi beberapa struktur organisasi seperti, Bidang Perencanaan dan Evaluasi TI, Bidang Pengembangan Aplikasi serta Bidang Operasional Sistem.
<i>Head Development</i>		
<i>Head IT Operations</i>		
<i>Head IT Administration</i>		

Struktur Organisasi COBIT	Tujuan TKMTI	Kondisi Saat Ini
<i>Privacy Officer</i>	DSS05, APO13, APO12	<i>Officer</i> Pengolahan dan Penyajian Data.
<i>Data Management Function</i>	APO12	
<i>Business Process Owners</i>	DSS05, APO13, APO12	Kepala Divisi Pengembangan Bisnis.
<i>Head Human Resources</i>	DSS05	Kepala Divisi Strategi SDM.
<i>Information Security Manager</i>	DSS05, APO13, APO12,	Kepala Bidang Operasional Sistem.
<i>Business Continuity Manager</i>	APO13, APO12,	
<i>Enterprise Risk Committee</i>	APO13, APO12,	Komite Eksekutif Manajemen Risiko.
<i>Project Management Office</i>	APO13, APO12.	Belum terdapat <i>Project Management Office</i>
<i>Service Manager</i>	APO13, APO12	Kepala Bidang Pengembangan Pelayanan.
<i>Chief Risk Officer</i>	APO12	Direktur Keuangan dan Manajemen Risiko membawahi Kepala Divisi Keuangan, Kepala Divisi Akuntansi, serta Kepala Divisi Manajemen Risiko.

Berdasarkan hasil penilaian kemampuan yang telah dilakukan pada komponen struktur organisasi, dapat diketahui bahwa pada komponen ini, InsurCo memiliki satu kesenjangan, yaitu belum memiliki posisi *Project Management Office*.

### 3.4 Hasil Analisis Penilaian dan Kesenjangan Komponen Prinsip, Kebijakan, Dan Kerangka

Setelah dilakukan analisis penilaian komponen prinsip, kebijakan, dan kerangka pada setiap prioritas tujuan TKMTI pada InsurCo, didapatkan hasil yang dapat dilihat pada **Tabel 4**.

**Tabel 4.** Penilaian Kemampuan Komponen Prinsip, Kebijakan, dan Kerangka

Kebijakan Yang Relevan	Kondisi Saat Ini
<b>DSS05 Managed Security Services.</b>	
Kebijakan Keamanan Informasi	SOP-ASA-SIM-10 Pengelolaan Keamanan Informasi
<b>APO13 Managed Security.</b>	
Keamanan Informasi Dan Kebijakan Privasi	PER_TI.01_18-AS_X_2020 SMKI, Dokumen Personel Sisfo, Kerangka Kerja serta Kebijakan SMKI.
<b>APO12 Managed Risk.</b>	
Kebijakan risiko perusahaan	MPTI 2020 dan prosedur Risiko TI
Kebijakan risiko <i>fraud</i>	Dokumen kebijakan risiko yang tercantum di dalam MPTI (Manajemen Proyek Teknologi Informasi) 2020 dan aplikasi Yammer dari Microsoft

Berdasarkan hasil penilaian kemampuan yang telah dilakukan pada komponen Prinsip, Kebijakan, dan Kerangka, dapat diketahui bahwa pada komponen ini, InsurCo tidak memiliki satupun kesenjangan.

### 3.5 Hasil Analisis Penilaian dan Kesenjangan Komponen Informasi

Setelah dilakukan analisis penilaian komponen prinsip, kebijakan, dan kerangka pada setiap prioritas tujuan TKMTI pada InsurCo, didapatkan hasil yang dapat dilihat pada

**Tabel 5.**

**Tabel 5.** Penilaian Kemampuan Komponen Informasi.

Praktik Manajemen	Hasil Informasi	Kondisi Saat Ini
<b>DSS05 Managed Security Services.</b>		
DSS05.01	<i>Malicious software prevention policy</i>	SOP_ASA_SIM_02 Proses Pemeliharaan Perangkat Lunak TI
	<i>Evaluations of potential threats</i>	Evaluasi informasi tinjauan produk vendor

<b>Praktik Manajemen</b>	<b>Hasil Informasi</b>	<b>Kondisi Saat Ini</b>
	<i>Information Security Management Reports</i>	SOP-ASA-SIM-10 Pengelolaan Keamanan Informasi
	<i>Information Security Service Catalog</i>	SOP-ASA-SIM-04 PROSES PENGELOLAAN <i>HELPDESK IT</i>
DSS05.02	<i>Connectivity security policy</i>	Kebijakan SMKI terkait kebijakan keamanan koneksi
	<i>Results of penetration tests</i>	<i>Vulnerability Assessment</i> pada SMKI
DSS05.03	<i>Security policies for model endpoint devices</i>	Belum dilakukan
DSS05.04	<i>Results of reviews of user accounts and privileges</i> <i>Approved user access rights</i>	Akses <i>privileges</i> pada pengguna tertentu.
DSS05.05	<i>Access logs</i> <i>Approved access requests</i>	Aplikasi Helpdesk
	<i>Access privileges</i>	Belum terdapat dokumen yang menjelaskan tipe pengguna dan akses yang dimiliki.
DSS05.06	<i>Inventory of sensitive documents and devices</i>	Dokumen Repository Management.
	<i>Security incident tickets</i>	Aplikasi Helpdesk.
DSS05.07	<i>Security incident characteristics</i> <i>Security event logs</i>	Aplikasi MRTG.
<b>APO13 Managed Security.</b>		
	<i>ISMS Scope Statement</i>	<i>PER_TI.01_18-AS_X_2020</i>
APO13.01	<i>ISMS Policy</i>	Kebijakan SMKI -Keberlanjutan Keamanan Informasi
	<i>Information security risk treatment plan</i>	<i>PER_TI.01_18-AS_X_2020</i> SMKI -Kerangka Kerja SMKI Kebijakan SMKI
APO13.02	<i>Information security business cases</i>	Kebijakan SMKI - Prasyarat Bisnis dan pengendalian akses SOP-ASA-SIM-10 Pengelolaan Keamanan Informasi
	<i>Recommendations for improving the information security management system (ISMS)</i>	Belum memiliki
APO13.03	<i>Information security management system (ISMS) audit reports</i>	Kebijakan SMKI - Evaluasi Kinerja SMKI (Hal 21) & SOP-ASA-SIM-10 PENGELOLAAN
<b>APO12 Managed Risk.</b>		
	<i>Emerging risk issues and factors</i>	
	<i>Data on risk events and contributing factors</i>	Dokumen Risk Register SISFO
APO12.01	<i>Data on the operating environment relating to risk</i> <i>Data on information security risk</i>	SOP-ASA-SIM-27 Proses Manajemen Risiko TI
	<i>Risk analysis results</i>	
	<i>I&amp;T risk scenarios</i>	SOP-ASA-SIM-27 Proses Manajemen Risiko TI
APO12.02	<i>Scope of risk analysis efforts</i> <i>Information security risk scenarios</i>	Kebijakan SMKI -Pemeriksaan <i>Technical Compliance (Penetration Testing)</i> -
	<i>Aggregated risk profile, including status of risk management actions</i>	SOP-ASA-SIM-27 Proses Manajemen Risiko TI
APO12.03	<i>Documented risk scenarios by line of business and function</i> <i>Information security risk profile</i>	Terdapat pada Laporan Pedoman BCM (Modul IT DRP) & Dokumen IT DRP Dokumen Risk Register SISFO

Praktik Manajemen	Hasil Informasi	Kondisi Saat Ini
APO12.04	<i>Risk analysis and risk profile reports for stakeholders</i>	Dokumen Risk Register SISFO
	<i>Results of third-party risk assessments</i>	(Dokumen SOA penerapan ISO 27001)
	<i>Opportunities for acceptance of greater risk</i>	Terdapat risk assessment
	<i>Information security risk response strategies</i>	Laporan Pedoman (Modul IT DRP) & Dokumen IT DRP
APO12.05	<i>Project proposals for reducing risk</i>	SOP-ASA-SIM-27 Proses Manajemen Risiko TI
	<i>Information security risk profile</i>	Dokumen Risk Register SISFO
	<i>Risk impact communication</i>	SOP-ASA-SIM-27 Proses Manajemen Risiko TI
APO12.06	<i>Risk-related root causes</i>	Dokumen Risk Register SISFO
	<i>Risk-related incident response plans</i>	Laporan Pedoman BCM (Modul IT DRP) & Dokumen IT DRP
	<i>Project proposals for reducing information security risk</i>	Risk register – Hasil Audit (hal 17) [BUKU 1]
		Tata Kelola TI – InsurCo 2018 v0.5 - Hasil Audit (hal 17) & SOP-ASA-SIM-27 Proses Manajemen Risiko TI

Berdasarkan hasil penilaian kemampuan yang telah dilakukan pada komponen informasi, dapat diketahui bahwa pada komponen ini, InsurCo memiliki tiga kesenjangan, yaitu belum memiliki dokumen pengelolaan keamanan *endpoint*, dokumen yang menjelaskan tipe pengguna dan akses, serta InsurCo belum memiliki dokumen terkait rekomendasi pengembangan SMKI.

### 3.6 Hasil Analisis Penilaian dan Kesenjangan Komponen Orang, Keterampilan, dan Kompetensi.

Setelah dilakukan analisis penilaian komponen Orang, Keterampilan, dan Kompetensi pada setiap prioritas tujuan TKMTI pada InsurCo, didapatkan hasil yang dapat dilihat pada **Tabel 6**.

**Tabel 6.** Penilaian Kemampuan Komponen Orang, Keterampilan, dan Kompetensi.

Keterampilan	Kondisi Saat Ini
<b>DSS05 Managed Security Services.</b>	
<i>Information security</i>	Pelatihan dan penanaman kesadaran yaitu dengan melakukan Pelatihan <i>IT Security (Networking and Application)</i> dan juga pelatihan dan sertifikasi ISO 27001
<i>Information security management</i>	Pelatihan dan pengembangan SDM terkait dengan proses Pelatihan COBIT dan Terdapat training pada manajemen keamanan informasi.
<i>Penetration testing</i>	Pemahaman mengenai proses <i>penetration testing</i> dalam pengelolaan dan penanganan uji coba software dan keamanan sistem dan Penetration Testing (PEN-T) yang dijelaskan pada tabel skill and <i>job matching</i> dan Sudah terdapat <i>awareness</i> dan <i>communication</i> dari Kadiv.
<i>Security administration</i>	Terdapat <i>Staff Service Desk</i> yang memiliki tanggung jawab terhadap log akses, Terdapat pada dokumen SOP-ASA-SIM-23 Prosedur Manajemen Akses Fisik
<b>APO13 Managed Security.</b>	
<i>Information security</i>	Pelatihan dan penanaman kesadaran yaitu dengan melakukan Pelatihan IT Security (Networking and Application) dan juga pelatihan dan sertifikasi ISO 27001
<i>Information security strategy development</i>	InsurCo telah memiliki keterampilan dalam menerapkan ISO 27001 sebagai pedoman standarisasi terkait keamanan informasi, tetapi InsurCo belum memiliki keterampilan rancangan serta pengembangan strategi keamanan informasi
<b>APO12 Managed Risk.</b>	
<i>Business risk management</i>	Terdapat beberapa pelatihan dan pengembangan SDM terkait dengan proses Pelatihan COBIT
<i>Information assurance</i>	Terdapat Staff Khusus terkait <i>service desk</i> yang memiliki peran memberikan informasi kepada end user mengenai proses yang berlangsung.
<i>Risk management</i>	Terdapat beberapa pelatihan dan pengembangan SDM terkait dengan proses Pelatihan COBIT dan juga terdapat <i>Risk Management Officer</i>

Berdasarkan hasil penilaian kemampuan yang telah dilakukan pada Orang, Keterampilan, dan Kompetensi, dapat diketahui bahwa pada komponen ini, InsurCo memiliki satu kesenjangan, yaitu belum memiliki keterampilan rancangan serta pengembangan strategi keamanan informasi.

### 3.7 Hasil Analisis Penilaian dan Kesenjangan Komponen Budaya, Etika, dan Perilaku.

Setelah dilakukan analisis penilaian komponen Budaya, Etika, dan Perilaku pada setiap prioritas tujuan TKMTI pada InsurCo, didapatkan hasil yang dapat dilihat pada **Tabel 7**.

**Tabel 7.** Penilaian Kemampuan Komponen Budaya, Etika, dan Perilaku.

<b>Elemen Kunci Budaya</b>	<b>Kondisi Saat Ini</b>
<b>DSS05 Managed Security Services</b>	
Ciptakan budaya kesadaran tentang tanggung jawab pengguna untuk menjaga praktik keamanan dan privasi.	InsurCo telah melakukan imbauan keamanan <i>Summary</i> melalui Surat serta melalui Microsoft Yammer (Surat Edaran Pengelolaan Password)
<b>APO13 Managed Security.</b>	
Menetapkan pedoman perilaku untuk melindungi informasi, sistem, dan infrastruktur perusahaan.	Organisasi memberlakukan Dokumen Service Level Guarantee (Perjanjian Kerahasiaan dan Larangan Pengungkapan) agar terhindar dari risiko dan privasi I&T.
<b>APO12 Managed Risk.</b>	
Untuk mendukung budaya risiko yang transparan dan partisipatif, manajemen senior harus menetapkan arah dan menunjukkan dukungan nyata dan nyata untuk penggabungan praktik risiko di seluruh perusahaan.	InsurCo telah memiliki divisi SAI untuk melaporkan dan mengkomunikasikan risiko secara khusus kepada <i>stakeholder</i> terkait.

Berdasarkan hasil penilaian kemampuan yang telah dilakukan pada komponen Budaya, Etika, dan Perilaku, dapat diketahui bahwa pada komponen ini, InsurCo tidak memiliki satupun kesenjangan.

### 3.8 Hasil Analisis Penilaian dan Kesenjangan Komponen Layanan, Infrastruktur, dan Aplikasi.

Setelah dilakukan analisis penilaian komponen layanan, infrastruktur, dan aplikasi pada setiap prioritas tujuan TKMTI pada InsurCo, didapatkan hasil yang dapat dilihat pada **Tabel 8**.

**Tabel 8.** Penilaian Kemampuan Komponen Layanan, Infrastruktur, dan Aplikasi.

<b>Rekomendasi Layanan, Infrastruktur, dan Aplikasi</b>	<b>Kondisi Saat Ini</b>
<b>DSS05 Managed Security Services.</b>	
<i>Directory services</i>	SSO ( <i>Single Sign On</i> )
<i>Email filtering systems</i>	Antivirus dan Anti Spam untuk pengontrolan Konten
<i>Identity and access management system</i>	Kontrol Akses terdapat pada Keamanan Data
<i>Security awareness services</i>	Microsoft Yammer
<i>Security information and event management (SIEM) tools</i>	InsurCo belum mengadaptasi layanan <i>Security operations center (SOC) services</i> dan SIEM
<i>Security operations center (SOC) services</i>	
<i>Third-party security assessment services</i>	ISO 27001
<i>URL filtering systems</i>	Terdapat aplikasi NgAF menuju server farm, firewall, extranet dan DMZ untuk perlindungan secara pusat & tools IDS dan IPS
<b>APO13 Managed Security.</b>	
<i>Configuration management tools</i>	Aplikasi <i>Service Desk</i> sebagai <i>repository</i> yang mencakup <i>hardware, Software</i> <i>Fitur Manage Engine</i>
<i>Security and privacy awareness services</i>	Aplikasi Microsoft Yammer
<i>Third-party security assessment services</i>	ISO 27001
<b>APO12 Managed Risk.</b>	
<i>Crisis management services</i>	Laporan Tanggap Bencana
<i>Governance, risk and compliance (GRC) tools</i>	COBIT 2019
<i>Risk analysis tools</i>	<i>Risk register</i> Sistem Informasi

Rekomendasi Layanan, Infrastruktur, dan Aplikasi	Kondisi Saat Ini
<i>Risk intelligence services</i>	

Berdasarkan hasil penilaian kemampuan yang telah dilakukan pada komponen budaya, etika, dan perilaku, dapat diketahui bahwa pada komponen ini, InsurCo memiliki satu kesenjangan, yaitu InsurCo belum mengadaptasi layanan *Security operations center (SOC) services*.

### 3.9 Hasil Analisis Potensi Pengembangan

Setelah melewati tahap analisis kesenjangan tujuh komponen pada masing-masing tujuan TKMTI yang terdiri dari yang terdiri dari tiga tujuan TKMTI, Hasil analisis potensi pengembangan yang telah didapatkan dipetakan menjadi tiga yaitu *people*, *process* dan *technology* yang bertujuan untuk meningkatkan efisiensi, produktivitas dan kualitas pada pengarah rekomendasi dalam tata kelola TI sektor keamanan informasi pada InsurCo. Pada potensi pengembangan aspek *people*, dapat dilihat pada tabel Tabel 9, yang menjelaskan bahwa dibutuhkannya pengembangan pada tujuan TKMTI APO13 *Managed Security* dan APO12 *Managed Risk*.

Tabel 9. Potensi Pengembangan Aspek People

Komponen Kemampuan	Type	Potensi Pengembangan
<b>APO13 <i>Managed Security</i> &amp; APO12 <i>Managed Risk</i>.</b>		
Struktur Organisasi	<i>Responsibility</i>	Melakukan penambahan tanggung jawab struktur organisasi <i>Project Management Office</i>
<b>APO13 <i>Managed Security</i></b>		
Komponen Orang, Keterampilan, dan Kompetensi	<i>Skills &amp; Awareness</i>	Meningkatkan pemahaman serta keterampilan individu terkait, dalam mendalami perancangan serta pengembangan strategi keamanan informasi

Pada potensi pengembangan aspek *process*, dapat dilihat pada tabel **Error! Not a valid bookmark self-reference.** yang menjelaskan bahwa dibutuhkannya pengembangan pada tujuan TKMTI DSS05 *Managed Security Services* dan APO13 *Managed Security*.

Tabel 10. Potensi Pengembangan Aspek Process

Komponen Kemampuan	Type	Potensi Pengembangan
<b>DSS05 <i>Managed Security Services</i>.</b>		
Proses	<i>Policy</i>	Mengembangkan kebijakan terkait keamanan <i>endpoint</i> yang lebih jelas dan mendetail
Proses	<i>Procedures</i>	mengembangkan prosedur penambahan pengamanan fisik atau pemeliharaan untuk melindungi perangkat <i>endpoint</i>
Informasi	<i>Record</i>	Merancang dan membuat dokumen informasi terkait kebijakan untuk keamanan <i>endpoint user</i>
Informasi	<i>Record</i>	Merancang dan membuat dokumen informasi terkait tipe pengguna dan akses yang dimiliki
<b>APO13 <i>Managed Security</i></b>		
Proses	<i>Policy</i>	Penambahan kebijakan terkait rencana penanganan isu keamanan informasi (SMKI) saat ini
Informasi	<i>Record</i>	Merancang dan membuat dokumen informasi terkait rekomendasi pengembangan SMKI atau Sistem Manajemen Keamanan Informasi

Pada potensi pengembangan aspek *technology*, dapat dilihat pada tabel **Tabel II** yang menjelaskan bahwa dibutuhkannya pengembangan pada tujuan TKMTI DSS05 *Managed Security Services*.

**Tabel 11.** Potensi Pengembangan Aspek Technology.

Komponen Kemampuan	Type	Potensi Pengembangan
<b>DSS05 Managed Security Services.</b>		
Layanan, Infrastruktur, dan Aplikasi	Tools	Mempersiapkan layanan pemantauan keamanan atau <i>Security operations center (SOC) services</i> dan SIEM yang proaktif dalam mendeteksi ancaman pada InsurCo secara <i>real-time</i>

**3.10 Analisis Resources, Risk, dan Value.**

Analisis RRV dibutuhkan dengan tujuan meningkatkan nilai yang dihasilkan dalam sebuah proyek serta menentukan prioritas dalam pelaksanaan sebuah proyek, analisis RRV terhadap perbaikan potensial pada InsurCo dengan mempertimbangkan penilaian *resources*, *risk*, dan *value* melalui penilaian berdasarkan nilai. Hasil nilai tiga (3) didapatkan apabila sumber daya yang digunakan dalam pelaksanaan proyek hanya berasal dari internal perusahaan, risiko kegagalan yang didapatkan hanya mempengaruhi satu unit perusahaan, dan apabila penerapannya berhasil dapat mempengaruhi seluruh unit perusahaan. Hasil nilai dua (2) didapatkan apabila sumber daya yang digunakan dalam pelaksanaan proyek berasal dari internal dan eksternal perusahaan, risiko kegagalan yang didapatkan mempengaruhi beberapa unit perusahaan, dan apabila penerapannya berhasil dapat mempengaruhi beberapa unit perusahaan. Hasil nilai satu (1) didapatkan apabila sumber daya yang digunakan dalam pelaksanaan proyek harus dari eksternal, risiko kegagalan yang didapatkan mempengaruhi seluruh unit perusahaan, dan apabila penerapannya berhasil mempengaruhi satu unit perusahaan, hasil dari analisis RRV dapat dijelaskan pada

Tabel 12.

**Tabel 12.** Hasil Analisis RRV

Potensi Pengembangan	Nilai Akhir	Prioritas Implementasi
Merancang dan membuat dokumen informasi terkait kebijakan untuk keamanan <i>endpoint user</i>	27	1
Merancang dan membuat dokumen informasi terkait tipe pengguna dan akses yang dimiliki	27	2
Melakukan penambahan tanggung jawab struktur organisasi <i>Project Management Office</i>	12	3
Mengembangkan kebijakan terkait keamanan <i>endpoint</i> yang lebih jelas dan mendetail	9	4
mengembangkan prosedur penambahan pengamanan fisik atau pemeliharaan untuk melindungi perangkat <i>endpoint</i>	6	5
Mempersiapkan layanan pemantauan keamanan atau <i>Security operations center (SOC) services</i> dan SIEM yang proaktif dalam mendeteksi ancaman pada InsurCo secara <i>real-time</i> , dengan melakukan analisis forensik dan memberikan respons yang cepat dalam penanganan insiden keamanan pada InsurCo.	6	6
Penambahan kebijakan terkait rencana penanganan isu keamanan informasi (SMKI) saat ini	6	7
Merancang dan membuat dokumen informasi terkait rekomendasi pengembangan SMKI atau Sistem Manajemen Keamanan Informasi	6	8
Meningkatkan pemahaman serta keterampilan individu terkait, dalam mendalami perancangan serta pengembangan strategi keamanan informasi	3	9

**3.11 Rekomendasi Aspek People**

Pada Aspek *People*, didapatkan dua kesenjangan pada APO13 *Managed Security* dan APO12 *Managed Risk*, yang pada perancangannya membutuhkan penambahan *Responsibility Project Management Office* terhadap komponen kemampuan struktur organisasi pada bidang pengembangan aplikasi InsurCo. Selain itu, juga dibutuhkan penambahan rekomendasi terhadap komponen Orang, Keterampilan, dan Kompetensi yaitu dengan penambahan pelatihan dan sertifikasi pada beberapa

kerangka kerja maupun standarisasi terkait strategi peningkatan sistem manajemen keamanan informasi.

### 3.12 Rekomendasi Aspek Process

Pengembangan aspek *process* berdasarkan kebutuhan InsurCo terhadap kesenjangan yang didapatkan pada tujuan TKMTI, yang mencakup dua ranah pengembangan kemampuan yaitu APO13 *Managed Security* dan DSS05 *Managed Security Services*. Pada komponen proses dibutuhkan peningkatan perancangan Standar Operasional Prosedur (SOP) terkait pengamanan perangkat fisik *Endpoint*, pada komponen Informasi dibutuhkan peningkatan perancangan Kebijakan TKMTI terkait pembuatan dokumen informasi terkait Pengembangan SMKI dan Tipe Dan Akses Pengguna serta peningkatan pada komponen kebijakan terkait Keamanan *Endpoint* dan pengembangan SMKI.

### 3.13 Rekomendasi Aspek Technology

Pengembangan aspek *technology* berdasarkan kebutuhan InsurCo terhadap kesenjangan yang didapatkan pada tujuan TKMTI, yang mencakup ranah pengembangan kemampuan DSS05 *Managed Security Services*. Pada komponen layanan, infrastruktur, dan aplikasi dibutuhkan peningkatan perancangan *tools* terkait layanan pemantauan keamanan atau *Security operations center (SOC) services* dan *Security information and event management (SIEM) tools*. Rekomendasi yang telah diberikan, diambil berdasarkan Gartner *Magic Quadrant Leaders* [30], [31].

### 3.14 Roadmap Implementasi

*Roadmap* atau peta jalan digunakan untuk menentukan waktu pelaksanaan rancangan rekomendasi yang telah dilakukan. Penyusunan peta jalan ini, didasari oleh prioritas RRV yang telah dilakukan pada proses sebelumnya. Perancangan implementasi ini dimulai dari Q1 (Januari – Maret) 2024 hingga Q4 (Oktober – Desember) 2024.

Tabel 13. Roadmap Implementasi

Inisiatif	Roadmap Timeline			
	2024			
	Q1	Q2	Q3	Q4
Penambahan tanggung jawab <i>Project Management Office</i> pada Divisi Pengembangan Aplikasi.				
Pemberian pelatihan dalam mendalami perancangan serta pengembangan strategi keamanan informasi, terhadap kerangka kerja atau praktik terbaik yang ada.				
Merancang dan membuat dokumen informasi terkait kebijakan untuk keamanan <i>endpoint user</i> .				
Merancang dan membuat dokumen informasi terkait tipe pengguna dan akses yang dimiliki.				
Mengembangkan kebijakan terkait keamanan <i>endpoint</i>				
Pengembangan prosedur penambahan pengamanan fisik atau pemeliharaan perangkat <i>endpoint</i> .				
Penambahan kebijakan audit terkait rencana penanganan isu keamanan informasi saat ini dan melakukan pembaruan terhadap prosedur yang telah ada.				
Merancang dan membuat dokumen informasi terkait rekomendasi pengembangan SMKI.				
Mempersiapkan layanan pemantauan keamanan atau <i>Security operations center (SOC) services</i> .				

### 3.15 Pengaruh Rancangan

Berdasarkan hasil penelitian yang telah dilakukan, menghasilkan rancangan perbaikan terhadap komponen yang memiliki kesenjangan dan pengaruhnya apabila diimplementasikan pada InsurCo dengan tujuan untuk mengetahui tingkat perubahan pada InsurCo. Pada Tabel 14 menunjukkan pengaruh rancangan komponen proses yang mengalami kenaikan sebesar 2.8 atau sebesar 8.81% pada ketiga tujuan TKMTI.

Tabel 14. Pengaruh Rancangan Komponen Proses

Tujuan TKMTI	Tingkat Kemampuan Sebelum Perbaikan	Tingkat Kemampuan Setelah Perbaikan
DSS05 <i>Managed Security Services</i>	2,4	2,8
APO13 <i>Managed Security</i>	2,5	4,6
APO12 <i>Managed Risk</i> .	3,0	3,3
<b>Total Nilai Kemampuan</b>	<b>2,7</b>	<b>3,5</b>

Tabel 15 menunjukkan pengaruh rancangan komponen struktur organisasi pada InsurCo yang menghasilkan penambahan tanggung jawab *Tanggung Jawab Project Management Office* ditambahkan pada struktur organisasi Kepala Bidang Pengembangan Aplikasi.

**Tabel 15.** Pengaruh Rancangan Komponen Struktur Organisasi

Sebelum Perbaikan	Setelah Perbaikan
<i>APO13 Managed Security dan APO12 Managed Risk</i>	
Belum Memiliki <i>Tanggung Jawab Project Management Office</i>	<i>Tanggung Jawab Project Management Office</i> ditambahkan pada struktur organisasi Kepala Bidang Pengembangan Aplikasi

Tabel 16 menunjukkan pengaruh rancangan komponen informasi pada InsurCo yang menghasilkan rekomendasi pembuatan dokumen informasi serta kebijakan.

**Tabel 16.** Pengaruh Rancangan Komponen Informasi.

Sebelum Perbaikan	Setelah Perbaikan
<i>DSS05 Managed Security Services</i>	
Tidak Memiliki <i>Security policies for model endpoint devices</i>	Dokumen informasi terkait kebijakan untuk keamanan <i>endpoint user</i> untuk melindungi perangkat <i>endpoint</i> masing-masing.
Belum terdapat dokumen yang menjelaskan tipe pengguna dan akses yang dimiliki.	Dokumen informasi terkait tipe pengguna dan akses yang dimiliki atau <i>Access Priviledge Document</i> .
<i>APO13 Managed Security.</i>	
belum memiliki dokumen informasi terkait rekomendasi pengembangan SMKI	Dokumen kebijakan audit terkait rencana penanganan isu keamanan informasi saat ini dan melakukan pembaruan terhadap prosedur yang telah ada untuk meningkatkan bentuk penanganannya serta pertahanan InsurCo apabila masalah terkait keamanan informasi ditemukan

Tabel 17 menunjukkan pengaruh rancangan komponen orang, keterampilan, dan kompetensi, yang menghasilkan rekomendasi peningkatan keterampilan merancang serta mengembangkan strategi keamanan informasi

**Tabel 17.** Pengaruh Rancangan Komponen Orang, Keterampilan, dan Kompetensi

Sebelum Perbaikan	Setelah Perbaikan
<i>APO13 Managed Security.</i>	
belum memiliki keterampilan merancang serta mengembangkan strategi keamanan informasi	Meningkatkan pemahaman serta keterampilan individu terkait, dalam mendalami perancangan serta pengembangan strategi keamanan informasi, dengan melakukan pemberian pelatihan kemampuan evaluasi komprehensif terhadap kerangka kerja atau praktik terbaik yang ada, seperti CISSP, CISA, CISM dan juga NIST SP 800-53

Pada Tabel 18 menunjukkan pengaruh rancangan komponen layanan, infrastruktur, dan aplikasi yang menghasilkan rekomendasi penambahan layanan pemantauan keamanan dengan menggunakan IBM Qradar.

**Tabel 18.** Pengaruh Rancangan Komponen Layanan, Infrastruktur, dan Aplikasi.

Sebelum Perbaikan	Setelah Perbaikan
<i>DSS05 Managed Security Services</i>	
Belum mengadaptasi layanan <i>Security operations center (SOC) services</i> dan SIEM atau layanan pemantauan keamanan	IBM Qradar

### 3.16 Pembahasan Hasil Studi

Pada penelitian sebelumnya terkait mekanisme TKTI yang berpengaruh terhadap TD pada industri asuransi dan perbankan [25], menghasilkan simpulan tentang pentingnya komponen TKTI hibrida yang terdiri dari pendekatan TKTI tradisional dan *agile*-adaptif yang berperan dalam mendukung pencapaian TD pada perusahaan, hal ini diakibatkan oleh kondisi lembaga keuangan tradisional saat ini memiliki aset yang signifikan serta diikuti risiko inheren yang cukup tinggi dan memerlukan regulasi yang ketat, walaupun asuransi pada dasarnya memiliki tingkatan kerumitan dan kematangan TI yang lebih rendah dibandingkan perbankan [29]. Sehingga, perusahaan *incumbent* seperti InsurCo dituntut untuk lebih *agile* dan adaptif untuk meningkatkan *customer experience* melalui percepatan *delivery* solusi digital, terutama untuk *customer-facing apps* yang membutuhkan fitur atraktif bagi pengguna, sambil secara hibrida tetap menerapkan pendekatan tradisional untuk mengawal solusi *tight-couple* yang berisiko tinggi dengan tujuan yang spesifik seperti implementasi sistem *core* pada asuransi [29].

Pada penelitian ini, ditemukan bahwa perusahaan studi kasus industri asuransi seperti InsurCo, memiliki kesenjangan pada area keamanan informasi, sebagai risiko inheren pada saat berakselerasi melalui TD dengan menerapkan pendekatan *delivery* solusi secara *agile* dan adaptif. Dalam rangka mengatasi kesenjangan yang ditemukan pada studi ini, digunakan pendekatan *Design Science Research* serta kerangka kerja COBIT 2019 *Focus Area Information Security Focus Area* sebagai kerangka kerja terbaru dari ISACA [24] yang ditujukan untuk memberikan solusi tata kelola dan keamanan informasi bagi InsurCo dalam mengawal kesuksesan TD menuju pencapaian kinerja organisasi.

## 4. KESIMPULAN

Penelitian ini memiliki keterbatasan yang dimana penyusunan manajemen keamanan informasi yang ditujukan bagi InsurCo dengan COBIT 2019 *Information Security* dilakukan secara khusus pada kondisi InsurCo. Pada penyusunan manajemen keamanan informasi yang ditujukan bagi InsurCo dengan COBIT 2019 *Information Security*, didapatkan tiga hasil prioritas tujuan TKMTI TKMTI yaitu *DSS05 Managed Security Service*, *APO13 Managed Security* serta *APO12 Managed Risk*.

Setelah melakukan analisis terhadap tujuh komponen dari ketiga tujuan TKMTI, didapatkan adanya sembilan (9) kesenjangan yang harus diperbaiki dalam mewujudkan pengelolaan TI pada sektor keamanan informasi secara ideal bagi InsurCo. Rekomendasi dari analisis serta perancangan manajemen keamanan informasi yang bersumber dari analisis terhadap kondisi InsurCo pada saat ini menghasilkan adanya sembilan (9) rancangan optimalisasi terhadap tiga aspek yaitu *people*, *process* dan *technology*. Penambahan rekomendasi pada aspek *people* menghasilkan penambahan *responsibility* atau tanggung jawab untuk mendukung pengendalian program atau proyek TI. Serta terdapat rekomendasi pelatihan yang bertujuan untuk meningkatkan keterampilan individu terkait pengembangan kerangka manajemen keamanan informasi. Pada aspek *process*, terdapat rekomendasi SOP terkait pemeliharaan serta pengamanan perangkat fisik, serta terdapat penambahan kebijakan dan juga pembuatan pedoman dokumen informasi. Adapun pada aspek *technology*, terdapat rekomendasi *tools* serta perbandingannya dalam hal penentuan yang paling tepat dalam melakukan pendeteksian, penganalisis ancaman keamanan secara menyeluruh dalam menghindari bahaya risiko keamanan informasi.

Penerapan waktu rekomendasi yang telah disebutkan didasarkan pada analisis RRV yang telah dilakukan yang menghasilkan roadmap implementasi serta pengaruh rancangan yang direkomendasikan. Hasil *assessment* tingkat kemampuan pada ketiga tujuan TKMTI pada kondisi awal menghasilkan nilai 2,7 dan setelah melakukan *assessment* dari rekomendasi yang telah diberikan mengalami peningkatan sebesar 0.8 yang menghasilkan nilai kemampuan 3,5 pada tingkat kemampuan setelah perbaikan atau sebesar 29,6% pada ketiga tujuan TKMTI.

Secara praktis penelitian ini dapat membantu InsurCo dalam menjadikan manajemen keamanan informasi sebagai prioritas dalam menuju transformasi, sedangkan secara akademis dapat dijadikan

referensi dalam melakukan perancangan manajemen keamanan informasi menggunakan COBIT 2019 *Information Security* untuk menuju pengelolaan manajemen keamanan informasi yang ideal pada perusahaan asuransi.

### Daftar Pustaka

- [1] M. S. Deby, R. Mulyana, L. Ramadani, and P. Korespodensi, "Analisis Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Asuransi B," *Journal of Information System*, vol. x, No. y, pp. x-y, 2022, doi: 10.33633/joins.vxyi.xxxx.
- [2] R. P. Wahyuni, R. Mulyana, L. Abdurrahman, and F. R. Industri, "Pengujian Model Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Asuransi B," *Jurnal Riset Komputer*, vol. 9, no. 5, pp. 2407–389, 2022, doi: 10.30865/jurikom.v9i1.9999.
- [3] C. Dewi Fortuna, R. Mulyana, and L. Ramadani, "Analisis Pengaruh Tata Kelola TI Pada Transformasi Digital Dan Kinerja Organisasi Bank A," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 10, no. 1, pp. 1–15, 2022, [Online]. Available: <https://jurnal.mdp.ac.id/index.php/jatisi/> ■1
- [4] S. Winasis, S. Riyanto, and E. Ariyanto, "Digital Transformation in the Indonesian Banking Industry: Impact on Employee Engagement.," *International Journal of Innovation, Creativity and Change.*, 2020.
- [5] K. Warner and M. Wañger, *Membangun kemampuan dinamis untuk transformasi digital: Proses yang berkelanjutan pembaruan strategis*. 2019.
- [6] G. Vial, "Understanding digital transformation: A review and a research agenda," *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118–144, Jun. 2019, doi: 10.1016/j.jsis.2019.01.003.
- [7] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review," in *Proc. 27th Annu. Am. Conf. Inf. Syst*, Twenty-Seventh Americas' Conference on Information Systems (AMCIS), 2021, pp. 1–10. [Online]. Available: <https://aisel.aisnet.org/amcis2021>
- [8] S. Vejseli and A. Rossmann, "Impact of IT Governance on Firm Performance A Literature Review.," *Association for Information Systems AIS Electronic Library (AISeL)*, 2017.
- [9] C. Chazar and M. A. Ramdhani, "Model Perencanaan Keamanan Sistem Informasi Menggunakan Pendekatan Metode Octave Dan ISO 27001:2005," in *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*, Bandung, May 2016.
- [10] Menteri Badan Usaha Milik Negara, *Peraturan Menteri Badan Usaha Milik Negara tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara. Indonesia: BN 2023 ( 262 ) : 230 hlm, 2023. 2023. Accessed: Jul. 09, 2023. [Online]. Available: https://jdih.bumn.go.id/peraturan/PER-2-MBU-03-2023*
- [11] U. Artha, R. Mulyana, and L. Ramadani, "Analisis Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Asuransi A," *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, 2022.
- [12] G. Khaerunnisa, R. Mulyana, L. Abdurrahman, and S. Informasi, "Pengujian Pengaruh Tata Kelola TI Terhadap Transformasi Digital Dan Kinerja Asuransi A Menggunakan Structural Equation Modeling," *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 2022.
- [13] P. Paryati, "KEAMANAN SISTEM INFORMASI," *Seminar Nasional Informatika*, 2008, [Online]. Available: [www.upnyk.ac.id](http://www.upnyk.ac.id)
- [14] B. Metivier, *Fundamental Objectives of Information Security*. 2017.
- [15] A. Ayu D., T. Anindyajati, and A. Ghoffar, "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital," Jakarta, 2019.
- [16] P. M. Dewi, R. Fauzi, and R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework COBIT 2019 Dengan Domain Build, Acquire and Implement: Studi Kasus Bank XYZ," *e-Proceeding of Engineering*, vol. 8, no. 5, p. 9672, 2021.
- [17] B. Panjaitan, L. Abdurrahman, and R. Mulyana, "Menggunakan Kontrol Annex : Studi Kasus Data Center Pt. Xyz The Development Of Information Security Management System Implementation Based On ISO 27001: 2013 Using Annex Control : In Pt. Xyz Case Study Data Center," 2021.
- [18] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," 2004. [Online]. Available: <https://www.jstor.org/stable/25148625>
- [19] G. Damaskinidis, "Qualitative Research and Subjective Impressions in Educational Contexts," *Am J Educ Res*, vol. 5, no. 12, pp. 1228–1233, Dec. 2017, doi: 10.12691/education-5-12-10.
- [20] Suharsimi. Arikunto, *Prosedur Penelitian : Suatu Pendekatan Praktik, Edisi Revisi VI*, Edisi Revisi VI. PT Rineka Cipta, 2006.
- [21] P. Johannesson and E. Perjons, *An Introduction to Design Science*. Cham: Springer International Publishing, 2014. doi: 10.1007/978-3-319-10632-8.
- [22] A. Hevner and S. Chatterjee, *Design Research in Information Systems*, vol. 22. in *Integrated Series in Information Systems*, vol. 22. Boston, MA: Springer US, 2010. doi: 10.1007/978-1-4419-5653-8.

- [23] ISACA, *COBIT2019: Implementing and Optimizing an Information and Technology Governance Solution.*, vol. a. 2018.
- [24] ISACA, *COBIT Focus Area : Information Security In COBIT® 2019 Framework.* 2020.
- [25] 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), Lisbon, 2023, 2023.*
- [26] A. K. Shenton, “Strategies for ensuring trustworthiness in qualitative research projects,” *Education for Information*, vol. 22, no. 2, pp. 63–75, 2004, doi: 10.3233/EFI-2004-22201.
- [27] ISACA, *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution.* 2018. [Online]. Available: <http://linkd.in/ISACAOOfficial>
- [28] ISACA, *COBIT Focus Area: Information Security.* 2020. [Online]. Available: [www.isaca.org](http://www.isaca.org)
- [29] 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)*, no. AI-IS-ASIA, pp. 1–16, Jun. 2022.
- [30] A. K. Kavanagh, T. Bussa, and G. Sadowski, “Magic Quadrant for Security Information and Event Management,” Feb. 2020. [Online]. Available: <https://www.gartner.com/doc/reprints?id=1-1YEDHXVD&ct=200219&st=sb>
- [31] M. Horvath, D. Gardner, Bhat Manjunath, R. Chugh, and A. Zhao, “Magic Quadrant for Application Security Testing,” May 2023.



**ZONasi: Jurnal Sistem Informasi**

is licensed under a [Creative Commons Attribution International \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)