

KONSEP MANAJEMEN RESIKO TERPADU. STUDI KASUS PT TELKOM DATA CENTER

Proposal Tugas Akhir

Oleh

**Timothy Haposan Simanjuntak
18222137**



**PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
Desember 2025**

LEMBAR PENGESAHAN

KONSEP MANAJEMEN RESIKO TERPADU. STUDI KASUS PT TELKOM DATA CENTER

Proposal Tugas Akhir

Oleh

**Timothy Haposan Simanjuntak
18222137**

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Proposal Tugas Akhir ini telah disetujui dan disahkan
di Bandung, pada tanggal 5 Desember 2025

Pembimbing

Dr. Ir. Arry Akhmad Arman, M.T.

NIP. 196504141991021001

DAFTAR ISI

DAFTAR GAMBAR	v
DAFTAR TABEL	vi
DAFTAR KODE	vii
I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Rumusan Masalah	3
I.3 Tujuan	4
I.4 Batasan Masalah	4
I.5 Metodologi	5
I.5.1 Analisis Kebutuhan (<i>Requirement Analysis</i>)	5
I.5.2 Perancangan Sistem (<i>System Design</i>)	6
I.5.3 Implementasi (<i>Implementation</i>)	6
I.5.4 Pengujian dan Validasi (<i>Testing & Validation</i>)	6
II STUDI LITERATUR	7
II.1 Pendahuluan	7
II.2 Tata Kelola Perusahaan dan Pengendalian Internal	7
II.2.1 <i>Good Corporate Governance (GCG)</i>	7
II.2.2 COSO Internal Control Framework	8
II.3 Manajemen Risiko Korporasi (<i>Enterprise Risk Management</i>)	9
II.3.1 Standar ISO 31000:2018	9
II.3.2 Regulasi Manajemen Risiko BUMN	9
II.3.3 Taksonomi dan Klasifikasi Risiko	10
II.3.4 Parameter Pengukuran dan Penilaian Risiko	10
II.3.5 Instrumen Pemantauan: KRI dan LED	10
II.4 Arsitektur Sistem Informasi Manajemen Risiko	11
II.4.1 Konsep Sistem Terintegrasi (<i>Integrated Architecture</i>)	11
II.4.2 Transformasi Proses Bisnis (<i>Business Process Reengineering</i>)	11
II.5 Perancangan Data dan Kualitas Informasi	11
II.5.1 Pemodelan Data Relasional Berbasis Regulasi	11
II.5.2 Integritas Data dan Audit Trail dalam Konteks RBIA	12
II.5.3 Praktik Terbaik Tata Kelola Data	13
II.6 Metodologi Pengembangan Perangkat Lunak (<i>SDLC</i>)	13

III ANALISIS MASALAH	14
III.1 Analisis Kondisi Saat Ini	14
III.1.1 Arsitektur Sistem Saat Ini (<i>Current Architecture</i>)	14
III.2 Analisis Proses Bisnis Eksisting (<i>Business Process Analysis</i>)	16
III.2.1 Proses Bisnis Utama (<i>BPMN Level 0</i>)	17
III.2.2 Analisis Sub-Proses Identifikasi Risiko	18
III.2.3 Analisis Sub-Proses Pelaporan Insiden	19
III.2.4 Analisis Sub-Proses Registrasi & Validasi Mitigasi	19
III.2.5 Analisis Sub-Proses Formasi Mitigasi Risiko	20
III.2.6 Analisis Sub-Proses Pemantauan Risiko	21
III.3 Implikasi Permasalahan (Analisis <i>PIECES</i>)	21
III.4 Analisis Kebutuhan Sistem	22
III.4.1 Kebutuhan Fungsional (<i>Functional Requirements</i>)	22
III.4.2 Kebutuhan Non-Fungsional (<i>Non-Functional Requirements</i>)	24
III.5 Analisis Alternatif Solusi	24
III.5.1 Alternatif 1: Perangkat Lunak GRC Komersial (<i>Commercial Off-The-Shelf / COTS</i>)	25
III.5.2 Alternatif 2: Platform Low-Code/No-Code	26
III.5.3 Alternatif 3: Pengembangan Aplikasi Web Kustom (<i>Custom Web Application</i>)	26
III.5.4 Evaluasi dan Pemilihan Solusi (<i>Weighted Scoring</i>)	27
IV DESAIN KONSEP SOLUSI	29
IV.1 Model Konseptual Sistem Usulan	29
IV.1.1 Arsitektur Data Relasional (<i>Comprehensive Data Architecture</i>)	29
IV.1.2 Arsitektur Alur Sistem Tingkat Tinggi (<i>High-Level Process Architecture</i>)	30
IV.1.3 Detil Alur Kerja Sub-Modul (<i>Sub-Module Workflows</i>)	32
IV.1.3.1 Modul Tata Kelola (<i>Governance Module</i>)	32
IV.1.3.2 Modul Objektif & Kinerja (<i>Objective Module</i>)	33
IV.1.3.3 Modul Manajemen Risiko Inti (<i>Risk Management Module</i>)	33
IV.1.3.4 Modul Indikator Risiko Kunci (<i>KRI Module</i>)	34
IV.1.3.5 Modul Insiden Kerugian (<i>Loss Event Module</i>)	35
IV.2 Analisis Komparatif (<i>Before vs After</i>)	35
V RENCANA SELANJUTNYA	39
V.1 Rencana Implementasi	39
V.1.1 Linimasa Penggerjaan (<i>Timeline</i>)	39

V.1.2	Kebutuhan Sumber Daya Pelaksanaan	40
V.2	Desain Pengujian dan Evaluasi	41
V.2.1	Verifikasi Desain (<i>Design Verification</i>)	41
V.2.2	Validasi Pengguna (<i>User Validation</i>)	42
V.3	Analisis Risiko dan Mitigasi	42
LAMPIRAN A. DATA PENDUKUNG ANALISIS KEPUTUSAN		44

DAFTAR GAMBAR

II.1 Komponen COSO Internal Control Framework	8
III.1 Diagram Proses Bisnis Level 0 (<i>Existing</i>)	17
III.2 Sub-Proses Identifikasi Risiko (<i>As Is</i>)	18
III.3 Sub-Proses Pelaporan Insiden (<i>As Is</i>)	19
III.4 Sub-Proses Registrasi & Validasi Mitigasi (<i>As Is</i>)	20
III.5 Sub-Proses Formasi Mitigasi Risiko (<i>As Is</i>)	20
III.6 Sub-Proses Pemantauan Risiko (<i>As Is</i>)	21
III.7 Diagram Sebab-Akibat Masalah (<i>Ishikawa/Fishbone Diagram</i>)	22
IV.1 <i>Entity Relationship Diagram (ERD)</i> Komprehensif	31
IV.2 Arsitektur Alur Sistem Usulan / BPMN Level 0 Baru.	32
IV.3 Alur Kerja Modul Governance.	33
IV.4 Alur Kerja Modul Objektif.	33
IV.5 Alur Kerja Modul Risk Management.	34
IV.6 Alur Kerja Modul KRI.	34
IV.7 Alur Kerja Modul Loss Event.	35
V.1 <i>Gantt chart</i> periode pertama.	39
V.2 <i>Gantt chart</i> periode kedua.	40
V.3 <i>Gantt chart</i> periode ketiga.	40

DAFTAR TABEL

III.1	Kebutuhan Fungsional Sistem Manajemen Risiko Terpadu	23
III.1	Kebutuhan Fungsional Sistem Manajemen Risiko Terpadu	24
III.2	Matriks Penilaian Alternatif Solusi	27
IV.1	Perbandingan Sistem Eksisting dan Sistem Usulan	36
V.1	Rencana Kebutuhan Sumber Daya Pelaksanaan	41
V.2	Analisis Risiko dan Mitigasi Proyek	42
3	<i>Pairwise comparison matrix</i> untuk penentuan bobot opsi	44
4	Tinjauan finansial model untuk ketiga opsi (<i>Detail</i>)	44

DAFTAR KODE

BAB I

PENDAHULUAN

I.1 Latar Belakang

Dalam lanskap korporasi modern yang penuh ketidakpastian, keberlangsungan perusahaan sangat bergantung pada tata kelola perusahaan (*Good Corporate Governance*) yang kokoh, di mana Sistem Pengendalian Internal (SPI) berbasis kerangka kerja COSO menjadi tulang punggungnya. COSO menekankan bahwa pengendalian internal bukan sekadar prosedur administratif, melainkan mekanisme strategis yang membutuhkan integrasi data yang solid untuk mendeteksi risiko sejak dini. Efektivitas mekanisme ini sangat ditentukan oleh kemampuan organisasi dalam mengelola informasi risiko secara efisien guna memberikan keyakinan memadai (*reasonable assurance*) terhadap pencapaian tujuan.

Urgensi integrasi sistem ini semakin nyata di sektor Badan Usaha Milik Negara (BUMN) Indonesia melalui Peraturan Menteri Nomor PER-5/MBU/09/2022. Regulasi ini mewajibkan transformasi fundamental dari manajemen risiko yang terfragmentasi (*silo-based*) menuju tata kelola risiko terintegrasi (*Integrated Risk Management*). Secara spesifik, regulasi ini menuntut BUMN untuk menyelenggarakan sistem yang mampu mengonsolidasikan informasi risiko secara menyeluruh, menghubungkan taksonomi risiko dengan strategi korporasi, serta mendukung pengambilan keputusan yang cepat dan berbasis data (Kementerian BUMN, 2022).

Namun, implementasi mandat integrasi ini di lapangan, khususnya pada PT Telkom Data Center sebagai penyedia infrastruktur digital kritikal, menghadapi tantangan operasional yang nyata. Meskipun manajemen risiko diakui sebagai proses vital, pelaksanaannya saat ini masih berjalan tidak efisien dan tidak efektif yang tercermin dalam permasalahan mendasar pada tiga domain utama:

- 1. Efisiensi Waktu Proses.** Dalam domain ini, praktik manajemen risiko masih

terjebak dalam pendekatan konvensional yang didominasi oleh proses manual dan birokrasi berbasis dokumen fisik atau *spreadsheet* yang diedarkan secara berjenjang. Alur kerja ini mengakibatkan siklus persetujuan dan pembaruan risiko memakan waktu yang lama (*high cycle time*) mengingat kompleksitas dan persebaran informasi, sehingga respons manajemen terhadap ancaman baru sering kali terlambat (*lagging*). Auditor internal pun menghabiskan waktu berharga hanya untuk mengompilasi data administratif ketimbang melakukan analisis strategis.

2. **Akurasi Data dan Pembentukan Wawasan (*Insight Generation*).** Ketergantungan pada input manual meningkatkan kerentanan terhadap *human error* dan inkonsistensi data. Ketiadaan sistem yang mampu mengagregasi data secara *real-time* menyebabkan manajemen puncak mengalami apa yang disebut sebagai *risk blindness*. Laporan yang dihasilkan bersifat statis dan historis, gagal menyajikan wawasan representatif kondisi *real time* yang diperlukan untuk pengambilan keputusan cepat di tengah dinamika bisnis infrastruktur digital yang bergerak cepat (Walker, 2020).
3. **Interkoneksi Data.** Ini adalah masalah paling kritis. Saat ini data risiko, Indikator Kinerja Utama (*Key Risk Indicators/KRI*), dan Tujuan Perusahaan (*Objectives*) tersimpan dalam "silo" yang terisolasi. Upaya taktis seperti penggunaan penyimpanan awan (*cloud storage*) bersama hanya berhasil mendigitalkan dokumen, namun gagal memperbaiki disintegrasi logika data. Akibatnya, tidak ada hubungan relasional (kausalitas) yang terbangun antara profil risiko dengan kinerja strategis. Tanpa interkoneksi ini, dampak domino dari kegagalan operasional terhadap target korporasi menjadi sulit dideteksi sejak dulu (Al-Baidhani, 2019).

Kesenjangan antara tuntutan regulasi BUMN akan "sumber kebenaran tunggal" (*Single Source of Truth*) dengan realitas sistem manual yang rapuh pada ketiga domain inilah yang menjadi urgensi tugas akhir ini. Diperlukan sebuah lompatan dari sekadar digitalisasi dokumen (memindahkan kertas ke layar) menuju digitalisasi proses dan sistem. Oleh karena itu, tugas akhir ini difokuskan pada perancangan arsitektur sistem informasi manajemen risiko terpadu yang tidak hanya mendigitalkan formulir risiko, tetapi juga memetakan hubungan kausalitas antar-elemen risiko secara sistematis. Perancangan ini ditujukan untuk menutup celah inefisiensi pelaporan dan menyediakan landasan teknis bagi penerapan *Three Lines Model* yang efektif di lingkungan PT Telkom Data Center.

I.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan utama yang dihadapi adalah kesenjangan antara tuntutan regulasi BUMN yang ketat dengan realitas operasional yang masih manual dan terfragmentasi. Secara spesifik, rumusan masalah dalam tugas akhir ini dirincikan ke dalam tiga poin utama sebagai berikut:

a. Efisiensi Proses (Lambannya E2E Risk Management & Auditing)

Proses manajemen risiko dari hulu ke hilir (*End-to-End*) serta aktivitas audit internal berjalan lamban. Hal ini disebabkan oleh ketergantungan pada proses manual dan penyimpanan data yang tersebar (terfragmentasi) di berbagai lokasi. Kondisi ini mengakibatkan waktu siklus pelaporan menjadi panjang, sehingga respons terhadap risiko menjadi tidak lincah dan kegiatan audit terhambat oleh proses administratif pengumpulan data.

Permasalahan: *Bagaimana merancang arsitektur sistem yang mampu mengefisiensikan alur kerja (workflow) manajemen risiko dan audit untuk mengatasi kelambatan proses akibat pengelolaan data yang manual dan tersebar?*

b. Akurasi Data dan Penarikan Insight (Kesulitan Input & Analisis)

Penggunaan *spreadsheet* yang padat dan kompleks untuk input manual rentan terhadap kesalahan manusia (*human error*), yang berdampak langsung pada akurasi data. Selain itu, format data yang kaku dan sulit dicerna menyulitkan manajemen untuk menarik wawasan (*insight*) strategis. Akibatnya, pengambilan keputusan menjadi sulit dilakukan karena data tidak tersaji dalam format yang mudah diterima dan dianalisis.

Permasalahan: *Bagaimana merancang antarmuka dan logika sistem yang dapat meminimalisir kesalahan input manual serta menyajikan visualisasi data yang mempermudah penarikan insight bagi manajemen?*

c. Interkoneksi Data (Strategic Blind Spot & Hilangnya Konteks)

Data risiko yang tidak saling terhubung mengakibatkan munculnya "Strategic Blind Spot". Konteks dari setiap risiko menjadi pudar karena hilangnya keterhubungan logis dengan elemen lain. Tanpa interkoneksi data yang sistematis, pemahaman mengenai dampak risiko terhadap tujuan strategis menjadi kabur, sehingga mitigasi yang dilakukan sering kali kehilangan konteks utamanya.

Permasalahan: *Bagaimana memetakan hubungan data yang saling terinterkoneksi untuk menghilangkan "blind spot" strategis dan memastikan konteks setiap risiko tetap terjaga hubungannya dengan tujuan perusahaan?*

I.3 Tujuan

Tujuan utama dari tugas akhir ini adalah menghasilkan cetak biru (*blueprint*) arsitektur sistem manajemen risiko terpadu yang dirancang untuk mentransformasi operasional manual menjadi ekosistem digital yang terintegrasi. Perancangan ini ditujukan untuk menjawab ketiga permasalahan di atas melalui pengembangan spesifikasi teknis pada lapisan bisnis, data, dan aplikasi.

Secara spesifik, tujuan tugas akhir ini adalah:

1. **Merancang Efisiensi Proses (Business Process Architecture):**
Menghasilkan rancangan ulang proses bisnis dan alur kerja digital yang terbukti secara teoritis mampu memangkas birokrasi manual. Tujuannya adalah mempercepat siklus pelaporan risiko (*cycle time*) dan memudahkan proses audit melalui sentralisasi alur kerja.
2. **Merancang Validasi & Visualisasi Data (Application & Interface Design):**
Merancang arsitektur antarmuka dan logika aplikasi yang meminimalisir peluang kesalahan input (*human error*) serta menyediakan dasbor analitik. Tujuannya adalah menjamin akurasi data yang masuk dan menyajikannya kembali dalam bentuk wawasan (*insight*) visual yang mudah dipahami oleh manajemen untuk pengambilan keputusan.
3. **Merancang Interkoneksi Konteks Strategis (Data Architecture):**
Merancang model data relasional yang secara sistematis menghubungkan entitas risiko, indikator kinerja (KRI), dan tujuan strategis perusahaan. Tujuannya adalah menghilangkan sekat informasi (*silos*) sehingga setiap risiko yang teridentifikasi selalu memiliki konteks yang jelas terhadap dampak strategisnya.

I.4 Batasan Masalah

Mengingat kompleksitas dan luasnya cakupan manajemen risiko korporasi, serta fokus tugas akhir pada aspek perancangan sistem, batasan masalah ditetapkan sebagai berikut:

1. Secara teknis, luaran tugas akhir ini berupa dokumen perancangan sistem (*system design document*) dan purwarupa perangkat lunak (*software prototype*) yang fungsional. Tahap konstruksi kode program (*coding*) dilakukan sebagai sarana realisasi rancangan untuk kebutuhan validasi, bukan sebagai pengembangan produk komersial skala penuh (*full-scale production*).
2. Fokus perancangan meliputi tiga lapisan utama arsitektur, yaitu:

- **Lapisan Bisnis:** Perancangan ulang proses bisnis (*business process reengineering*) manajemen risiko.
 - **Lapisan Data:** Perancangan skema basis data relasional untuk mengintegrasikan data risiko yang terfragmentasi.
 - **Lapisan Aplikasi:** Perancangan arsitektur aplikasi dan antarmuka pengguna (*user interface*).
3. Ruang lingkup fungsional difokuskan pada siklus inti manajemen risiko (identifikasi, penilaian, mitigasi, pelaporan) menggunakan data simulatif yang merepresentasikan karakteristik PT Telkom Data Center, serta yang didasari tuntutan regulasi oleh mandat BUMN.
 4. Implementasi kode program difokuskan pada realisasi fungsi utilitas dan efisiensi proses sesuai rancangan. Aspek teknis mendalam seperti optimasi performa tinggi, keamanan siber tingkat lanjut, atau skalabilitas infrastruktur awan (*cloud scalability*) bukan merupakan fokus utama, selama sistem dapat beroperasi stabil untuk membuktikan konsep (*proof of concept*) dan validasi pengguna.
 5. Evaluasi rancangan dilakukan melalui pengujian fungsional dan kegunaan (*usability testing*) pada purwarupa aplikasi yang dibangun, guna membuktikan peningkatan efisiensi alur kerja dibandingkan proses manual.

I.5 Metodologi

Tugas akhir ini mengadopsi metodologi *Software Development Life Cycle* (SDLC) dengan model *Waterfall* yang disesuaikan untuk kebutuhan penelitian. Model ini dipilih karena karakteristiknya yang sistematis dan sekuensial, memastikan bahwa setiap aspek perancangan (mulai dari analisis kebutuhan hingga struktur data) telah terdefinisi secara matang sebelum direalisasikan dalam bentuk kode program.

I.5.1 Analisis Kebutuhan (*Requirement Analysis*)

Tahap ini berfokus pada eksplorasi masalah untuk menetapkan spesifikasi sistem yang akurat. Kegiatan utama mencakup:

- **Wawancara Lapangan:** Melakukan wawancara terhadap pengguna sistem manajemen risiko *As-Is* di PT Telkom Data Center untuk memetakan titik inefisiensi.
- **Studi Literatur dan Regulasi:** Menganalisis Peraturan Menteri BUMN No. PER-5/MBU/09/2022 dan standar ISO 31000 untuk menyusun kebutuhan fungsional sistem yang patuh regulasi (*compliance*).

- **Definisi Kebutuhan:** Merumuskan kebutuhan fungsional (fitur sistem) dan non-fungsional (kinerja dan batasan) sebagai acuan perancangan.

I.5.2 Perancangan Sistem (*System Design*)

Tahap ini menerjemahkan spesifikasi kebutuhan menjadi rancangan teknis yang komprehensif pada tiga lapisan arsitektur:

- **Perancangan Proses Bisnis:** Memodelkan ulang alur kerja menggunakan BPMN (*To-Be Process*) untuk menjawab masalah efisiensi proses.
- **Perancangan Data:** Menyusun *Entity Relationship Diagram* (ERD) untuk memetakan interkoneksi antara risiko, KRI, dan tujuan strategis.
- **Perancangan Aplikasi:** Mengembangkan desain antarmuka pengguna dan arsitektur perangkat lunak yang mendukung kebutuhan fungsional dan non-fungsional.

I.5.3 Implementasi (*Implementation*)

Tahap ini merupakan realisasi dari dokumen perancangan menjadi purwarupa perangkat lunak yang fungsional (*working prototype*). Fokus utama tahap ini adalah penulisan kode program (*coding*) untuk membangun fungsi-fungsi utilitas utama sistem, seperti modul input risiko, *dashboard* analitik, dan otomatisasi alur kerja, guna membuktikan kelayakan konsep yang dirancang.

I.5.4 Pengujian dan Validasi (*Testing & Validation*)

Tahap akhir bertujuan untuk memverifikasi bahwa sistem yang dibangun telah memenuhi tujuan efisiensi dan akurasi. Pengujian dilakukan melalui:

- **Validasi Fungsional (*Black Box Testing*):** Memastikan seluruh fitur berjalan sesuai logika bisnis yang dirancang dan bebas dari *error* kritis.
- **Validasi Utilitas:** Menguji apakah alur kerja sistem baru mampu memberikan efisiensi waktu dan kemudahan akses informasi dibandingkan proses manual, sesuai dengan rumusan masalah yang ditetapkan.

BAB II

STUDI LITERATUR

II.1 Pendahuluan

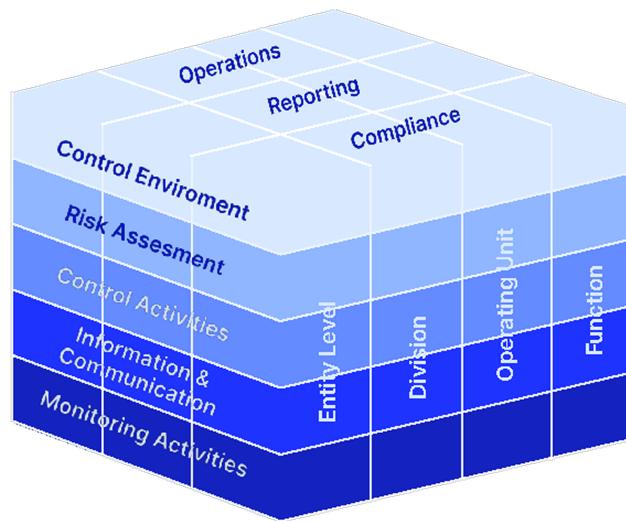
Bab ini menguraikan landasan teoretis dan kerangka konseptual yang menjadi fondasi dalam perancangan sistem manajemen risiko terpadu. Pembahasan dimulai dari konsep tata kelola perusahaan dan pengendalian internal sebagai payung besar, dilanjutkan dengan kerangka kerja manajemen risiko berdasarkan standar internasional dan regulasi BUMN, serta diakhiri dengan tinjauan teknis mengenai arsitektur sistem informasi, perancangan data, dan transformasi proses bisnis. Studi literatur ini bertujuan memberikan pemahaman komprehensif mengenai integrasi antara kepatuhan regulasi dengan solusi teknologi informasi.

II.2 Tata Kelola Perusahaan dan Pengendalian Internal

II.2.1 *Good Corporate Governance (GCG)*

Good Corporate Governance (GCG) merupakan seperangkat peraturan yang mengatur hubungan antara pemegang saham, pengurus (pengelola) perusahaan, pihak kreditur, pemerintah, karyawan, serta para pemegang kepentingan internal dan eksternal lainnya yang berkaitan dengan hak-hak dan kewajiban mereka (FCGI, 2011).

Dalam konteks BUMN, penerapan GCG bukan sekadar kepatuhan, melainkan strategi untuk meningkatkan nilai ekonomi dan sosial. Prinsip dasar GCG meliputi Transparansi (*Transparency*), Akuntabilitas (*Accountability*), Pertanggungjawaban (*Responsibility*), Kemandirian (*Independency*), dan Kewajaran (*Fairness*). Tugas akhir ini berfokus pada aspek **Transparansi** dan **Akuntabilitas**, yang diwujudkan melalui digitalisasi pelaporan risiko untuk menghilangkan asimetri informasi antar-unit kerja.



Gambar II.1 Komponen COSO Internal Control Framework

II.2.2 COSO Internal Control Framework

Untuk menjamin terlaksananya GCG, diperlukan sistem pengendalian internal yang efektif. Kerangka kerja yang menjadi standar global adalah *COSO Internal Control - Integrated Framework*. COSO (2013) mendefinisikan pengendalian internal sebagai proses yang dipengaruhi oleh dewan direksi, manajemen, dan personel lain, yang dirancang untuk memberikan keyakinan memadai tentang pencapaian tujuan dalam kategori: operasi, pelaporan, dan kepatuhan.

Lima komponen COSO yang relevan dengan perancangan sistem ini adalah:

Lingkungan Pengendalian (*Control Environment*)

Budaya sadar risiko di organisasi.

Penilaian Risiko (*Risk Assessment*)

Mekanisme identifikasi dan analisis risiko (fokus utama sistem ini).

Aktivitas Pengendalian (*Control Activities*)

Kebijakan dan prosedur mitigasi.

Informasi dan Komunikasi

Sistem yang memastikan aliran data risiko berjalan lancar (fokus integrasi data).

Pemantauan (*Monitoring*)

Evaluasi berkelanjutan melalui audit internal.

II.3 Manajemen Risiko Korporasi (*Enterprise Risk Management*)

II.3.1 Standar ISO 31000:2018

ISO 31000:2018 menyediakan pedoman universal mengenai cara mengelola risiko yang dihadapi organisasi. Standar ini menekankan bahwa tujuan manajemen risiko adalah penciptaan dan perlindungan nilai (*value creation and protection*).

Proses manajemen risiko menurut ISO 31000 terdiri dari elemen-elemen yang akan diadopsi ke dalam alur logika sistem, yaitu:

1. **Komunikasi dan Konsultasi:** Fitur notifikasi dan kolaborasi dalam sistem.
2. **Penetapan Lingkup, Konteks, dan Kriteria:** Pengaturan parameter *Risk Appetite* dan *Risk Tolerance*.
3. **Penilaian Risiko (*Risk Assessment*):** Terdiri dari Identifikasi, Analisis (menentukan probabilitas dan dampak), dan Evaluasi Risiko.
4. **Perlakuan Risiko (*Risk Treatment*):** Rencana mitigasi atau *action plan*.
5. **Pemantauan dan Tinjauan:** Audit berkala terhadap profil risiko.

II.3.2 Regulasi Manajemen Risiko BUMN

Kementerian BUMN melalui Peraturan Menteri Nomor PER-5/MBU/09/2022 menetapkan kewajiban penerapan manajemen risiko yang terintegrasi. Beberapa poin krusial dari regulasi ini yang menjadi syarat fungsional sistem adalah:

- **Three Lines Model:** Sistem harus memfasilitasi peran tiga lini pertahanan:
 - *Lini Pertama (Unit Operasional):* Pemilik risiko (*risk owner*) yang melakukan input dan mitigasi harian.
 - *Lini Kedua (Unit Manajemen Risiko):* Pemantau kepatuhan dan agregator laporan.
 - *Lini Ketiga (Audit Internal):* Pemberi *assurance* independen.
- **Integrasi Strategis:** Risiko tidak boleh berdiri sendiri, melainkan harus dipetakan terhadap Sasaran Strategis BUMN dan Indikator Kinerja Utama (*Key Performance Indicators*).

II.3.3 Taksonomi dan Klasifikasi Risiko

Untuk memungkinkan agregasi data yang efektif dalam sistem terpadu, diperlukan struktur klasifikasi risiko yang baku, atau disebut taksonomi risiko. Taksonomi ini mencegah duplikasi dan memastikan konsistensi pelaporan antar-unit (Chapman, 2011). Komponen taksonomi meliputi:

- Kategori Risiko: Pengelompokan level tertinggi, biasanya terdiri dari Risiko Strategis, Risiko Operasional, Risiko Finansial, dan Risiko Kepatuhan.
- Tema Risiko: Sub-kategori yang lebih spesifik yang mengelompokkan risiko berdasarkan kesamaan domain atau akar penyebab, misalnya "Kegagalan Infrastruktur IT" atau "Kesalahan Manusia".
- Kelompok Peristiwa Risiko Agregasi: Kumpulan kejadian risiko individu yang serupa yang dapat digabungkan untuk melihat dampak sistemik.

II.3.4 Parameter Pengukuran dan Penilaian Risiko

Sistem manajemen risiko memerlukan parameter kuantitatif dan kualitatif yang jelas untuk mengukur eksposur risiko:

- **Selera Risiko (*Risk Appetite*):** Jumlah dan jenis risiko yang siap diterima oleh organisasi dalam rangka mengejar tujuan strategisnya.
- **Risiko Inheren (*Inherent Risk*):** Tingkat risiko alami yang melekat pada suatu aktivitas atau proses bisnis sebelum dilakukan upaya mitigasi.
- **Risiko Residual (*Residual Risk*):** Tingkat risiko yang masih tersisa setelah kontrol internal atau upaya mitigasi diterapkan.
- **Matriks Tingkat Risiko (*Risk Matrix/Heatmap*):** Alat visualisasi yang memetakan risiko berdasarkan dua sumbu: Probabilitas dan Dampak. Matriks ini membagi risiko ke dalam zona warna (misal: Hijau, Kuning, Merah) untuk menentukan prioritas.

II.3.5 Instrumen Pemantauan: KRI dan LED

Selain penilaian risiko berkala, sistem modern memerlukan instrumen pemantauan dinamis:

- *Key Risk Indicators (KRI)* Metrik yang digunakan untuk memberikan sinyal peringatan dini (*early warning signal*) mengenai peningkatan eksposur risiko di area tertentu (Moeller, 2013). Berbeda dengan KPI yang mengukur kinerja masa lalu (*lagging*), KRI bersifat prediktif (*leading*).
- *Loss Event Database (LED)* Pangkalan data yang mencatat kerugian operasional yang benar-benar terjadi secara historis. LED berfungsi sebagai

alat validasi untuk menguji akurasi prediksi risiko (*back-testing*) dan menjadi basis pengetahuan (*knowledge base*).

II.4 Arsitektur Sistem Informasi Manajemen Risiko

II.4.1 Konsep Sistem Terintegrasi (*Integrated Architecture*)

Sistem *Enterprise Risk Management* (ERM) terintegrasi dirancang untuk memusatkan data risiko dalam satu repositori tunggal untuk menciptakan "sumber kebenaran tunggal" (*Single Source of Truth*). Secara arsitektural, tugas akhir ini mengadopsi struktur berlapis (*n-tier architecture*) yang terdiri dari tiga lapisan utama:

1. **Lapisan Data (*Data Layer*):** Fondasi sistem yang berfungsi menyimpan entitas risiko, mitigasi, dan log audit. Desain lapisan ini harus menjamin integritas referensial.
2. **Lapisan Bisnis (*Business Logic Layer*):** Menangani aturan bisnis (*business rules*) yang kompleks, seperti algoritma penilaian risiko (*scoring*) otomatis dan logika alur persetujuan berjenjang.
3. **Lapisan Aplikasi & Antarmuka (*Application & Presentation Layer*):** Antarmuka pengguna yang disesuaikan dengan peran *Three Lines Model*, menyajikan dasbor analitik bagi manajemen puncak dan formulir input bagi unit operasional.

II.4.2 Transformasi Proses Bisnis (*Business Process Reengineering*)

Peralihan dari proses manual ke digital menuntut dilakukannya Perancangan Ulang Proses Bisnis (BPR). Proses manual yang cenderung serial, birokratis, dan berbasis kertas perlu diubah menjadi alur kerja digital yang paralel dan otomatis. Dalam konteks tugas akhir ini, notasi BPMN (*Business Process Model and Notation*) digunakan untuk memodelkan alur kerja masa depan (*To-Be*). Tujuannya adalah mengeliminasi aktivitas yang tidak bernilai tambah (*non-value added activities*) dan mempercepat waktu siklus (*cycle time*).

II.5 Perancangan Data dan Kualitas Informasi

II.5.1 Pemodelan Data Relasional Berbasis Regulasi

Kualitas informasi manajemen risiko sangat bergantung pada desain skema basis data yang mampu mengakomodasi kompleksitas pelaporan korporasi. Mengacu pada mandat Permen BUMN No. PER-2/MBU/03/2023 Pasal 22

mengenai Taksonomi Risiko dan PER-5/MBU/09/2022 Pasal 30 tentang Pelaporan, perancangan sistem ini memetakan entitas data krusial sebagai berikut:

- **Risk Taxonomy:** Katalog induk yang menyimpan standarisasi hierarki risiko.
- **Risk Profile & Register:** Tabel transaksional utama yang mencatat profil risiko spesifik, mencakup nilai *Inherent Risk* dan *Residual Risk*.
- **Mitigation & Costing:** Entitas yang mencatat rencana tindakan serta data anggaran biaya mitigasi dan realisasinya.
- **Loss Event Database (LED):** Entitas untuk mencatat insiden kerugian historis.
- **Key Risk Indicators (KRI) & Thresholds:** Entitas parameter peringatan dini yang terhubung langsung dengan risiko.

Relasi antar-entitas ini dirancang untuk mendukung pelaporan agregat secara otomatis, sehingga manajemen dapat memantau eksposur risiko secara *real-time* berdasarkan kategori strategis.

II.5.2 Integritas Data dan Audit Trail dalam Konteks RBIA

Salah satu kelemahan fatal penggunaan *spreadsheet* adalah ketiadaan jejak audit yang handal. Dalam perancangan sistem ERM ini, fitur *Audit Trail* menjadi kebutuhan non-fungsional kritis yang mendukung metodologi Audit Internal Berbasis Risiko (*Risk-Based Internal Audit - RBIA*). Sistem harus dirancang untuk mencatat setiap perubahan data (*create, update, delete*) beserta stempel waktu (*timestamp*) dan identitas pengguna yang melakukan perubahan.

Untuk memenuhi standar audit BUMN, sistem wajib memfasilitasi audit terhadap aspek risiko utama:

1. **Risiko Strategis:** Keselarasan dengan RJPP dan RKAP.
2. **Risiko Operasional:** Keandalan IT, proses bisnis, dan *human error*.
3. **Risiko Kepatuhan:** Ketaatan terhadap regulasi.
4. **Risiko Keuangan:** Akurasi data laporan keuangan.

Agar data risiko dinyatakan valid (sah) secara audit, sistem harus menjamin kelengkapan komponen risiko (*Risk Components*) pada setiap *record*:

- **Identitas Risiko:** Deskripsi kejadian, penyebab, dan dampak.
- **Atribut Penilaian:** Skor *Likelihood* dan *Impact*.
- **Kepemilikan (Risk Ownership):** Unit kerja dan personil penanggung jawab.
- **Efektivitas Kontrol:** Status pelaksanaan mitigasi dan bukti pendukung (*evidence*).

Mekanisme ini penting untuk memastikan bahwa riwayat perubahan profil

risiko dapat ditelusuri validitasnya (*traceability*) dan tidak dapat disangkal (*non-repudiation*) (Gartner, 2024).

II.5.3 Praktik Terbaik Tata Kelola Data

Keberhasilan implementasi sistem bergantung pada tata kelola data yang kuat. Mengacu pada kerangka kerja DAMA-DMBOK (*DAMA International*, 2017), praktik terbaik yang diadopsi meliputi:

- **Data Stewardship (Perwalian Data):** Penunjukan *Data Stewards* yang jelas untuk setiap domain data risiko.
- **Manajemen Kualitas Data:** Sistem dirancang dengan mekanisme validasi otomatis untuk memastikan:
 - *Akurasi (Accuracy)*
 - *Kelengkapan (Completeness)*
 - *Konsistensi (Consistency)*
 - *Ketepatan Waktu (Timeliness)*
- **Standarisasi Metadata dan Kamus Data:** Penerapan Kamus Data (*Data Dictionary*) yang terpusat untuk mencegah ambiguitas semantik.

II.6 Metodologi Pengembangan Perangkat Lunak (*SDLC*)

Software Development Life Cycle (SDLC) adalah kerangka kerja logis untuk mengembangkan perangkat lunak sistem informasi. Mengingat batasan tugas akhir ini, model *Waterfall* dinilai paling relevan. Tahapan yang diadopsi meliputi:

1. **Requirement Analysis:** Mengumpulkan kebutuhan pengguna dan regulasi.
2. **System Design:** Merancang arsitektur data, aplikasi, dan UI/UX.
3. **Implementation:** Tahap konstruksi kode program (*coding*) untuk membangun purwarupa.
4. **Testing:** Verifikasi fungsional dan validasi pengguna.

BAB III

ANALISIS MASALAH

Bab ini menguraikan analisis mendalam terhadap kondisi sistem manajemen risiko yang sedang berjalan (*current state*) serta merumuskan kebutuhan sistem usulan (*future state*). Analisis didasarkan pada observasi terhadap arsitektur, data, dan proses bisnis di PT Telkom Data Center, serta kesenjangananya dengan mandat regulasi Peraturan Menteri BUMN No. PER-5/MBU/09/2022 tentang Penerapan Manajemen Risiko Terintegrasi.

III.1 Analisis Kondisi Saat Ini

Berdasarkan hasil observasi dan wawancara pendahuluan, proses manajemen risiko di PT Telkom Data Center saat ini masih dijalankan menggunakan pendekatan manual yang terdesentralisasi. Untuk memahami akar permasalahan secara holistik, analisis kondisi saat ini dipetakan ke dalam tiga dimensi utama: arsitektur sistem, alur informasi, dan perangkat yang digunakan.

III.1.1 Arsitektur Sistem Saat Ini (*Current Architecture*)

Secara arsitektural, model operasional yang berjalan saat ini adalah "Arsitektur Berbasis Berkas Awan Terfragmentasi" (*Fragmented Cloud-File Architecture*). Dalam model ini, tulang punggung data perusahaan bukanlah sebuah basis data terpusat, melainkan koleksi ribuan berkas *spreadsheet* yang tersebar di berbagai folder unit kerja dalam layanan awan (seperti *Google Drive/OneDrive*).

Kondisi ini menciptakan fenomena "Ilusi Integrasi". Karena berkas dapat diakses secara daring, manajemen berasumsi bahwa sistem telah terintegrasi. Namun, kenyataan teknis di lapangan menunjukkan bahwa data-data tersebut tersimpan dalam *silo* yang terisolasi secara logika. Tidak ada skema basis data relasional (*relational database*) yang mengikat satu fail dengan fail lainnya, sehingga integritas

dan interkoneksi data sepenuhnya bergantung pada disiplin manual manusia, bukan validasi sistem.

Kelemahan fundamental dari arsitektur ini bermanifestasi pada tiga aspek kritis:

1. Inefisiensi Proses Akibat Pemantauan Pasif (*The Latency Trap*)

Meskipun berkas berada di awan, arsitektur ini bersifat pasif. Sistem tidak memiliki mekanisme notifikasi otomatis (*state-based triggers*) untuk memberi tahu manajer risiko ketika sebuah unit melakukan pembaruan atau ketika risiko kritis muncul. Akibatnya, pemantauan menjadi aktivitas yang sangat manual dan memakan waktu (latensi tinggi).

Studi Kasus Lapangan 1 (Inefisiensi Risk Management):

Seorang *Risk Officer* harus melakukan ”patroli digital” setiap akhir bulan dengan membuka lebih dari 20 tautan *spreadsheet* unit yang berbeda satu per satu hanya untuk mengecek apakah ada pembaruan. Seringkali, waktu terbuang hanya untuk menemukan bahwa 15 dari 20 unit belum melakukan pengisian, atau tautan fail telah kedaluwarsa/berubah izin aksesnya, memaksa petugas untuk menghubungi unit satu per satu via *WhatsApp* untuk meminta akses ulang.

Studi Kasus Lapangan 2 (Friksi Interaksi & Revisi): Proses finalisasi profil dan approval risiko sering kali macet dalam siklus tak berarah akibat saluran komunikasi yang terdistribusi. Sebagai contoh, ketika *Risk Officer* memberikan catatan revisi pada *spreadsheet* Unit Operasional (misal: ”lengkapi biaya mitigasi”), sistem tidak mengirim notifikasi. Komunikasi harus dilakukan manual via *WhatsApp*.

Masalah muncul ketika Unit Operasional telah melakukan revisi sesuai arahan, namun lupa melakukan konfirmasi balik via chat kepada *Risk Officer*. Akibatnya, dokumen tersebut didiamkan (”mangkrak”) selama 2 minggu karena *Officer* berasumsi unit belum merevisi, sementara Unit berasumsi dokumen sudah selesai. Proses iterasi yang seharusnya selesai dalam hitungan jam menjadi berminggu-minggu akibat terpisahnya konteks data (di fail) dan konteks diskusi (di aplikasi pesan).

2. Kerentanan Akurasi Data Tidak Terstruktur

Penggunaan *spreadsheet* sebagai basis data utama, meskipun dilakukan secara daring, membawa risiko inheren berupa ketidakkonsistenan struktur data. Fleksibilitas sel pada *spreadsheet* memungkinkan pengguna di unit kerja

untuk mengubah format tanggal, menyisipkan kolom baru, atau menimpa rumus (*overwrite formula*) secara tidak sengaja. Hal ini menyebabkan kegagalan saat data mencoba ditarik ke level korporat.

Studi Kasus Lapangan (Akurasi): Saat penyusunan laporan triwulanan, dasbor agregat korporat mendadak menampilkan error #REF! atau data kosong. Setelah ditelusuri selama 4 jam, ditemukan penyebabnya adalah satu staf di Unit Operasional menyisipkan kolom "Keterangan Tambahan" di tengah tabel *Risk Register* mereka, yang menggeser posisi kolom pembacaan rumus master. Selain itu, variasi penulisan "High", "Tinggi", dan "H" pada kolom level risiko menyebabkan data tidak terhitung akurat dalam grafik rekapitulasi.

3. Fragmentasi Konteks Strategis (*The Logical Disconnect*)

Kelemahan paling kritis adalah terputusnya hubungan antara risiko operasional dengan tujuan strategis. Secara fisik, fail "Profil Risiko Unit" tersimpan di folder operasional, sementara fail "Laporan Kinerja Strategis (KRI)" tersimpan di folder perencanaan. Karena tidak ada kunci penghubung (*Foreign Key*) antar-fail ini, sistem gagal memetakan dampak kausalitas.

Studi Kasus Lapangan (Interkoneksi): Ketika terjadi insiden server *downtime* (Risiko Operasional), unit teknis mencatatnya dan memitigasinya. Namun, karena data ini tidak terhubung dengan fail KRI Strategis, manajemen puncak tidak mendapatkan peringatan bahwa insiden tersebut telah menurunkan "Indeks Kepuasan Pelanggan" di bawah ambang batas aman. Manajemen baru menyadari korelasi ini pada rapat evaluasi bulan berikutnya, di mana momentum untuk melakukan intervensi strategis sudah terlambat (*Strategic Blind Spot*).

III.2 Analisis Proses Bisnis Eksisting (*Business Process Analysis*)

Untuk memvalidasi permasalahan inefisiensi waktu dan fragmentasi data yang telah diuraikan sebelumnya, dilakukan pemetaan proses bisnis eksisting menggunakan notasi *Business Process Model and Notation* (BPMN). Pemetaan ini membedah alur kerja manajemen risiko secara granular, mulai dari level korporat hingga level aktivitas unit, guna mengidentifikasi titik-titik kemacetan (*bottlenecks*) dan aktivitas redundant yang menghambat kelincahan organisasi.

III.2.1 Proses Bisnis Utama (BPMN Level 0)

Pada tingkat strategis, proses bisnis manajemen risiko di PT Telkom Data Center terdiri dari lima fase utama. Analisis terhadap diagram BPMN Level 0 (Gambar 3.2) difokuskan pada dua dimensi kerentanan utama yang menjadi sumber ineffisiensi dan kesalahan data saat ini, yaitu:



Gambar III.1 Diagram Proses Bisnis Level 0 (*Existing*)

- **Input Data Sensitif (Sensitive Data Input):** Fase yang rentan terhadap kerusakan model data (*broken model*), kesalahan input (*human error*), dan konflik versi (*version control issues*).
- **Proses Iteratif & Interaktif (Iterative & Interactive Process):** Fase yang membutuhkan kolaborasi intensif namun terhambat oleh *bottleneck* komunikasi karena ketidadaan platform terpadu.

Berikut adalah pembedahan masalah pada setiap fase proses berdasarkan dua dimensi tersebut:

1. Identifikasi Risiko (Fase Data Sensitif)

- *Aktivitas:* Unit kerja menginput kejadian risiko, penyebab, dan dampak ke dalam spreadsheet.
- *Masalah Akurasi:* Fase ini sangat sensitif terhadap format input. Tanpa validasi sistem (hanya mengandalkan kolom Excel), pengguna sering memasukkan kategori risiko yang tidak baku (contoh: menulis "Ops" alih-alih "Operasional").
- *Dampak:* Kesalahan taksonomi ini menyebabkan data gagal teragregasi secara otomatis di tingkat korporat, menciptakan "Data Hantu" yang ada di fail unit tapi tidak muncul di laporan direksi.

2. Penilaian dan Pemetaan Risiko (Fase Iteratif & Interaktif)

- *Aktivitas:* Diskusi antara Risk Owner dan Manajer untuk menentukan skor Kemungkinan dan Dampak.
- *Masalah Iterasi:* Penentuan skor risiko membutuhkan negosiasi dan kalibrasi. Saat ini, diskusi ini terjadi di saluran terpisah (WhatsApp/Rapat Luring) dan tidak terekam dalam sistem.
- *Dampak:* Hilangnya konteks historis. Ketika skor risiko berubah dari "High" menjadi "Medium", tidak ada jejak audit (*trail*) yang

menjelaskan alasan penurunan skor tersebut, apakah karena mitigasi efektif atau intervensi subjektif.

3. Pembentukan Mitigasi Risiko (Fase Gabungan: Sensitif & Iteratif)

- *Aktivitas:* Perencanaan anggaran, jadwal, dan strategi penanganan risiko.
- *Masalah Data Sensitif:* Input data anggaran dan tanggal di spreadsheet sangat rentan terhadap kerusakan rumus (*broken formulas*) jika pengguna menyisipkan kolom baru atau mengubah format mata uang.
- *Masalah Interaktif:* Fase ini melibatkan siklus persetujuan anggaran. Dokumen sering kali ”ping-pong” (bolak-balik) antara unit dan manajemen via email untuk revisi, menyebabkan latensi proses yang tinggi.

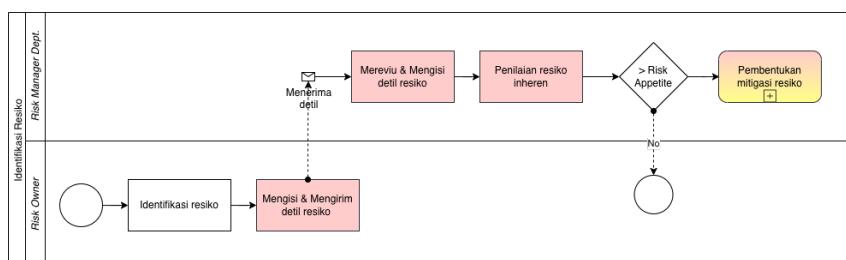
4. Registrasi Mitigasi Risiko (Fase Data Sensitif)

- *Aktivitas:* Finalisasi profil risiko untuk dikunci menjadi laporan resmi (*baseline*).
- *Masalah Versi Kontrol:* Dalam lingkungan berbasis fail, sering muncul isu duplikasi versi fail (misal: Risk_Reg_Final_V1.xlsx vs Risk_Reg_Final_V2_Revisi.xlsx).
- *Dampak:* Manajemen sering kali mengambil keputusan berdasarkan versi data yang salah/usang karena kebingungan menentukan mana fail yang menjadi ”Sumber Kebenaran Tunggal” (*Single Source of Truth*).

5. Pemantauan Risiko (Fase Iteratif & Interaktif)

- *Aktivitas:* Pelaporan progres mitigasi dan pengumpulan bukti (*evidence*).
- *Masalah Iterasi:* Ini adalah fase dengan friksi tertinggi. Auditor harus menagih bukti secara manual, dan auditee mengirim bukti secara parsial.
- *Dampak:* Proses audit menjadi lambat karena waktu habis untuk administrasi pengumpulan fail, bukan evaluasi efektivitas mitigasi.

III.2.2 Analisis Sub-Proses Identifikasi Risiko



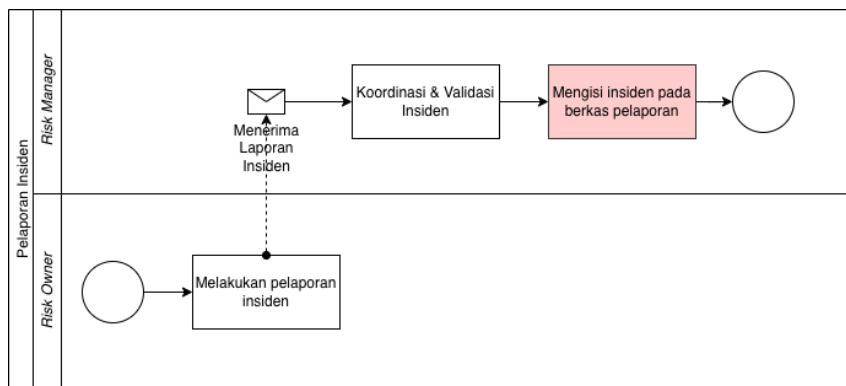
Gambar III.2 Sub-Proses Identifikasi Risiko (*As Is*)

Sub-proses ini memiliki titik lemah signifikan pada aspek validasi input.

Masalah Utama: *Human Error* pada Penerapan Standar Baku dan data terisolasi.

Analisis: Meskipun perusahaan memiliki beberapa matriks data set yang baku, penerapannya pada *spreadsheet* bergantung sepenuhnya pada ketelitian pengguna. Tidak ada *system enforcement* yang mencegah pengguna memasukkan nilai dampak yang tidak logis atau bertentangan dengan standar, sehingga validitas profil risiko inheren menjadi diragukan. Selain itu identifikasi risiko yang kurang lengkap akibat tidak dipetakan dengan *data point* strategis lainnya.

III.2.3 Analisis Sub-Proses Pelaporan Insiden



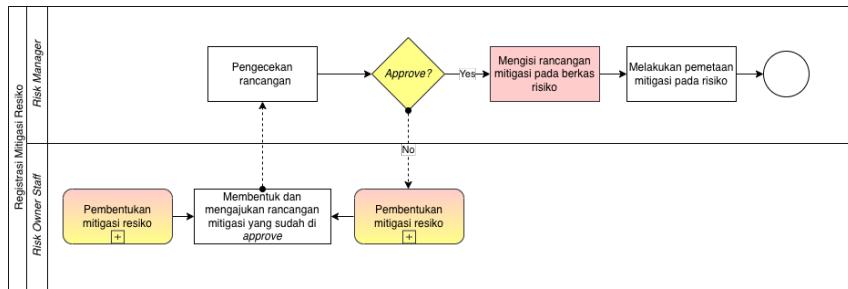
Gambar III.3 Sub-Proses Pelaporan Insiden (*As Is*)

Sub-proses ini menunjukkan adanya diskoneksi data yang kritikal.

Masalah Utama: Inkonsistensi Format dan Data Terisolasi.

Analisis: Pencatatan insiden pada log terpisah dengan terminologi yang berbeda dari *Risk Register* menyebabkan kegagalan rekonsiliasi data. Sistem tidak dapat secara otomatis menghubungkan kejadian nyata dengan prediksi risiko, menghilangkan peluang pembelajaran organisasi (*organizational learning*) untuk mengkalibrasi profil risiko di masa depan.

III.2.4 Analisis Sub-Proses Registrasi & Validasi Mitigasi



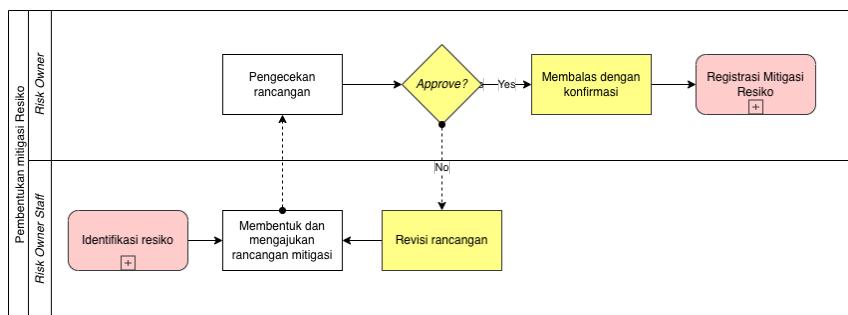
Gambar III.4 Sub-Proses Registrasi & Validasi Mitigasi (*As Is*)

Sub-proses ini merupakan titik kemacetan (*bottleneck*) utama dalam siklus manajemen risiko.

Masalah Utama: *The Iteration Barrier* (Hambatan Iterasi).

Analisis: Kebutuhan akan revisi dokumen memicu siklus komunikasi manual yang tidak efisien. Ketidakhadiran notifikasi sistem menyebabkan dokumen revisi sering kali terabaikan ("mangkrak") dalam waktu lama karena menunggu konfirmasi manual via aplikasi pesan, menghambat penyelesaian laporan korporat.

III.2.5 Analisis Sub-Proses Formasi Mitigasi Risiko



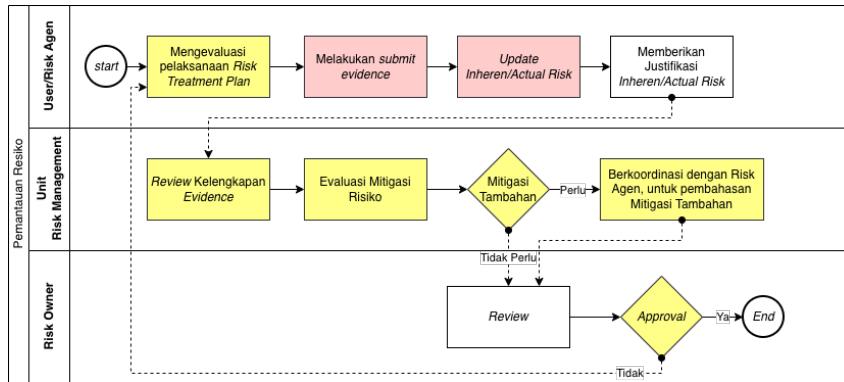
Gambar III.5 Sub-Proses Formasi Mitigasi Risiko (*As Is*)

Sub-proses ini mengindikasikan adanya redundansi aktivitas input data.

Masalah Utama: Penanganan Ganda Data (*Double Handling*).

Analisis: Staf sering kali harus menginput data yang sama dua kali: satu untuk persetujuan internal unit, dan satu lagi untuk pelaporan ke sistem korporat. Hal ini terjadi karena ketidadaan fitur *collaborative drafting* yang memungkinkan persetujuan berjenjang dalam satu platform yang sama.

III.2.6 Analisis Sub-Proses Pemantauan Risiko



Gambar III.6 Sub-Proses Pemantauan Risiko (*As Is*)

Sub-proses ini memiliki kompleksitas administrasi tertinggi.

Masalah Utama: Administrasi Bukti Terdesentralisasi.

Analisis: Bukti mitigasi tersebar di berbagai penyimpanan lokal. Proses verifikasi mengharuskan auditor meminta data secara berulang (*interactive fetch*). Ketiadaan repositori terpusat yang terhubung langsung dengan item risiko membuat audit trail menjadi lemah dan proses audit menjadi tidak efisien.

III.3 Implikasi Permasalahan (Analisis PIECES)

Berdasarkan analisis arsitektur dan proses bisnis di atas, permasalahan struktural yang dihadapi PT Telkom Data Center dipetakan menggunakan kerangka kerja PIECES (*Performance, Information, Economics, Control, Efficiency, Service*):

- **Performance (Kinerja):**
 - **Waktu Siklus Tinggi (High Cycle Time):** Ketergantungan pada konsolidasi manual dan persetujuan via surel menyebabkan respons mitigasi bersifat reaktif dan lambat.
 - **Responsivitas Rendah:** Sistem manual tidak mampu memberikan peringatan dini (*early warning*) secara *real-time* saat terjadi eskalasi risiko.
- **Information (Informasi):**
 - **Ambiguitas Data:** Isu *version control* akibat fail terpisah menyebabkan perbedaan data antara laporan unit dan korporat.
 - **Strategic Blind Spots:** Absennya integrasi antara risiko operasional dengan KRI/Objective mengakibatkan manajemen kehilangan

visibilitas dampak strategis.

- **Economics (Ekonomi):**

- **Inefisiensi Sumber Daya:** Waktu staf tersita untuk aktivitas administratif bernilai tambah rendah (rekapitulasi), alih-alih analisis strategi.

- **Control (Pengendalian):**

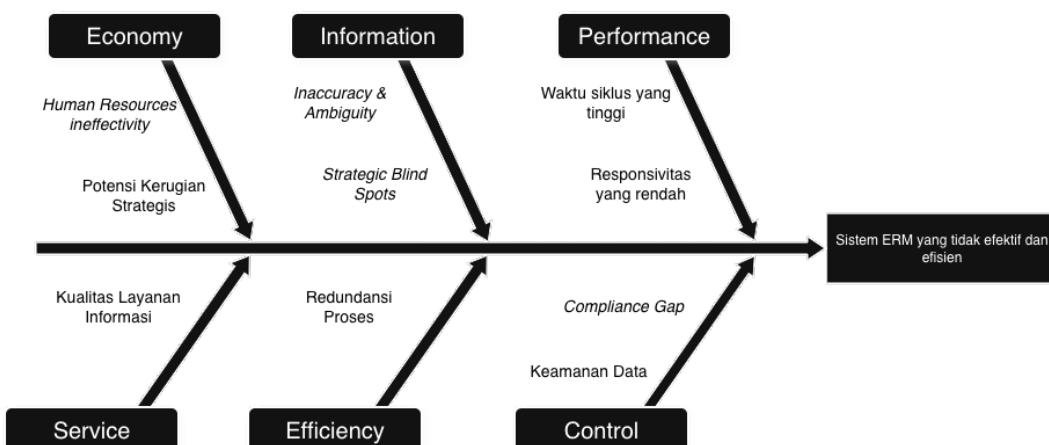
- **Kesenjangan Audit (Audit Gap):** Penggunaan saluran informal menghilangkan jejak audit (*audit trail*), menyulitkan pemenuhan standar PER-5/MBU/09/2022.

- **Efficiency (Efisiensi):**

- **Redundansi Proses:** Duplikasi input data yang sama di berbagai level pelaporan akibat ketiadaan basis data terpusat.

- **Service (Layanan):**

- **Kualitas Informasi Rendah:** Manajemen puncak tidak mendapatkan data akurat dan *real-time* untuk pengambilan keputusan strategis.



Gambar III.7 Diagram Sebab-Akibat Masalah (*Ishikawa/Fishbone Diagram*)

III.4 Analisis Kebutuhan Sistem

Berdasarkan permasalahan struktural yang telah diuraikan dalam analisis PIECES serta kesenjangan pada proses bisnis eksisting, dirumuskan spesifikasi kebutuhan sistem untuk perancangan Sistem Manajemen Risiko Terpadu. Perumusan kebutuhan ini ditujukan tidak hanya sebagai daftar fitur, melainkan sebagai solusi langsung terhadap masalah fragmentasi data, inefisiensi audit, dan ketidaksesuaian regulasi yang menghambat operasional saat ini.

III.4.1 Kebutuhan Fungsional (*Functional Requirements*)

Tabel III.1 Kebutuhan Fungsional Sistem Manajemen Risiko Terpadu

ID	Kebutuhan Fungsional	Deskripsi (<i>Input - Proses - Output</i>)
MODUL 1: MANAJEMEN DATA RISIKO (<i>RISK REGISTER</i>)		
FR-01	Sistem harus memvalidasi input data risiko sesuai taksonomi baku.	<p>Input: Data Risiko via Formulir Digital.</p> <p>Proses: Validasi format, tipe data, dan kelengkapan <i>mandatory fields</i>.</p> <p>Output: Data risiko terstruktur dan standar.</p>
FR-02	Sistem harus mengkalkulasi skor risiko secara otomatis.	<p>Input: Parameter Dampak dan Kemungkinan.</p> <p>Proses: Kalkulasi algoritma berdasarkan matriks <i>Risk Appetite</i>.</p> <p>Output: Skor dan Level Risiko yang objektif.</p>
MODUL 2: INTEGRASI STRATEGIS (<i>STRATEGY MAP</i>)		
FR-03	Sistem harus memetakan relasi antara Risiko, KRI, dan Objektif.	<p>Input: Pemilihan relasi entitas.</p> <p>Proses: Mapping basis data relasional (<i>many-to-many</i>).</p> <p>Output: Visualisasi keterkaitan dampak strategis.</p>
MODUL 3: ALUR KERJA & KOLABORASI (<i>WORKFLOW</i>)		
FR-04	Sistem harus menyediakan alur persetujuan digital berjenjang.	<p>Input: Pengajuan dokumen.</p> <p>Proses: Routing dokumen ke penyetuju, notifikasi otomatis.</p> <p>Output: Status dokumen terbarukan dan log persetujuan.</p>
FR-05	Sistem harus mengelola siklus revisi dan diskusi.	<p>Input: Komentar revisi.</p> <p>Proses: Notifikasi <i>real-time</i> ke inisiator, pencatatan riwayat komentar.</p> <p>Output: Jejak audit komunikasi dan revisi.</p>
MODUL 4: PELAPORAN INSIDEN (<i>LOSS EVENT</i>)		
FR-06	Sistem harus mencatat dan menghubungkan insiden (<i>loss event</i>) dengan risiko terkait.	<p>Input: Data Insiden, ID Risiko.</p> <p>Proses: Rekonsiliasi data kejadian nyata dengan profil risiko.</p> <p>Output: Riwayat insiden pada detail risiko untuk kalibrasi skor.</p>
MODUL 5: PEMANTAUAN BUKTI (<i>EVIDENCE MANAGEMENT</i>)		

Tabel III.1 Kebutuhan Fungsional Sistem Manajemen Risiko Terpadu

ID	Kebutuhan Fungsional	Deskripsi (<i>Input - Proses - Output</i>)
FR-07	Sistem harus menyediakan repositori bukti terpusat.	Input: Unggah berkas bukti mitigasi. Proses: Validasi format dan penautan ke <i>Action Plan</i> . Output: Tautan bukti yang terorganisir dan mudah diaudit.
MODUL 6: PELAPORAN & VISUALISASI (REPORTING)		
FR-08	Sistem harus menghasilkan Peta Risiko (<i>Heat Map</i>) dan laporan agregat otomatis.	Input: Filter data periode/unit. Proses: Agregasi data <i>real-time</i> dari seluruh unit. Output: Visualisasi dasbor interaktif dan laporan siap cetak.

III.4.2 Kebutuhan Non-Fungsional (*Non-Functional Requirements*)

Kebutuhan non-fungsional mendefinisikan batasan kualitas dan kendala lingkungan yang harus dipenuhi sistem untuk menjamin keberterimaan operasional dan kepatuhan audit.

- **Integritas Data (Data Integrity):** Sistem harus menjamin validitas hubungan antar-data melalui skema basis data relasional (*Referential Integrity*) untuk menghilangkan redundansi dan inkonsistensi yang terjadi pada arsitektur spreadsheet.
- **Auditabilitas (Auditability):** Sistem wajib menyediakan *Immutable Audit Log* yang merekam seluruh riwayat perubahan data (siapa, kapan, apa), guna mengatasi masalah "Kesenjangan Audit" dan memfasilitasi verifikasi bukti.
- **Keamanan & Kepatuhan (Security & Compliance):** Penerapan *Role-Based Access Control* (RBAC) untuk memastikan segregasi tugas yang tegas antara Pemilik Risiko dan Manajer Risiko sesuai model *Three Lines of Defense*.

III.5 Analisis Alternatif Solusi

Untuk menjawab kebutuhan sistem yang telah dirumuskan, dilakukan evaluasi komparatif terhadap tiga pendekatan pengembangan sistem yang umum digunakan dalam industri. Evaluasi ini dilakukan secara multidimensi mencakup perspektif pengguna (*User*), bisnis (*Business*), operasional (*Operational*), dan teknis

(*Technical*) guna menentukan solusi yang paling optimal bagi PT Telkom Data Center.

III.5.1 Alternatif 1: Perangkat Lunak GRC Komersial (*Commercial Off-The-Shelf/COTS*)

Pendekatan ini melibatkan adopsi platform GRC global yang sudah mapan (contoh: *SAP GRC*, *ServiceNow*, *RSA Archer*).

- **Perspektif Pengguna (*User Perspective*):**

Usability: Sistem COTS cenderung memiliki antarmuka yang kompleks dan padat fitur (*bloated*). Kurva pembelajaran (*learning curve*) sangat curam bagi pengguna awam di unit operasional.

Adoption: Risiko resistensi pengguna cukup tinggi karena alur kerja sistem sering kali terasa kaku dan tidak selaras dengan budaya kerja lokal, memaksa pengguna mengubah cara kerja mereka demi mengikuti sistem.

- **Perspektif Bisnis (*Business Perspective*):**

ROI & Revenue: Memiliki biaya total kepemilikan (*Total Cost of Ownership*) yang sangat tinggi, mencakup lisensi tahunan yang mahal. Untuk skala purwarupa tugas akhir, *Return on Investment* (ROI) sangat rendah atau negatif.

Strategic Value: Menawarkan kepatuhan standar internasional (ISO/NIST) secara instan ("out of the box"), namun kurang fleksibel untuk mengakomodasi nuansa regulasi lokal spesifik BUMN tanpa kustomisasi mahal.

- **Perspektif Operasional (*Operational Perspective*):**

Implementation: Proses implementasi lambat dan rumit, membutuhkan keterlibatan konsultan eksternal tersertifikasi.

SLA: Ketergantungan penuh pada vendor support untuk penyelesaian isu kritis.

- **Perspektif Teknis (*Technical Perspective*):**

Scalability & Security: Sangat unggul dalam keamanan dan skalabilitas data skala masif.

Maintainability: Arsitektur bersifat "Black Box". Tim IT internal sulit melakukan pemeliharaan atau penyesuaian logika inti secara mandiri (*vendor lock-in*).

III.5.2 Alternatif 2: Platform Low-Code/No-Code

Pendekatan ini menggunakan platform pengembangan visual cepat (contoh: *Microsoft PowerApps, Mendix, OutSystems*).

- **Perspektif Pengguna (*User Perspective*):**

Usability: Antarmuka umumnya standar dan familiar (terutama jika berbasis ekosistem Microsoft), sehingga mudah diterima pengguna.

Satisfaction: Kepuasan pengguna baik untuk fungsi sederhana, namun sering menurun ketika aplikasi menjadi lambat saat menangani logika bisnis yang kompleks.

- **Perspektif Bisnis (*Business Perspective*):**

ROI: Biaya pengembangan awal rendah (*low barrier to entry*), namun biaya operasional dapat membengkak eksponensial karena model lisensi per-pengguna (*per-user licensing*).

Strategic Value: Efektif untuk mendigitalkan formulir sederhana, namun kurang ideal sebagai aset strategis jangka panjang untuk sistem inti korporasi (Core ERM).

- **Perspektif Operasional (*Operational Perspective*):**

Implementation: Sangat cepat (*rapid deployment*). Sumber daya pengembang tidak memerlukan keahlian koding yang mendalam.

Resources: Memerlukan manajemen tata kelola IT yang ketat untuk mencegah fenomena *Shadow IT* (aplikasi liar yang tidak terstandar).

- **Perspektif Teknis (*Technical Perspective*):**

Scalability: Terbatas. Performa cenderung menurun signifikan saat menangani relasi data yang kompleks (*many-to-many*) antara ribuan baris risiko dan KRI.

Maintainability: Logika bisnis sering kali tersebar di berbagai komponen visual ("Spaghetti Logic"), menyulitkan dokumentasi dan pemeliharaan jangka panjang.

III.5.3 Alternatif 3: Pengembangan Aplikasi Web Kustom (*Custom Web Application*)

Pendekatan ini melibatkan pembangunan sistem secara mandiri (*in-house*) menggunakan kerangka kerja modern (contoh: React, Node.js, Laravel).

- **Perspektif Pengguna (*User Perspective*):**

Usability: Antarmuka dapat dirancang 100% *fit-for-purpose*, hanya menampilkan fitur yang relevan bagi Risk Owner, sehingga sangat intuitif.

Adoption: Tingkat adopsi potensial paling tinggi karena alur sistem dirancang mengikuti mental model pengguna saat ini, bukan sebaliknya.

- **Perspektif Bisnis (*Business Perspective*):**

ROI: Efisiensi biaya tinggi. Tidak ada biaya lisensi berulang (*No Recurring License Cost*). Investasi terfokus pada pengembangan awal (*CapEx*).

Strategic Value: Organisasi memiliki hak kekayaan intelektual (IP) penuh atas sistem. Logika pemetaan strategi (Risiko-KRI-Objektif) dapat dibentuk presisi sesuai mandat PER-5/MBU/09/2022.

- **Perspektif Operasional (*Operational Perspective*):**

Implementation: Membutuhkan sumber daya pengembang yang kompeten, namun memberikan kendali penuh atas linimasa proyek.

Resources: Dapat dijalankan pada infrastruktur server standar yang sudah dimiliki perusahaan atau lingkungan lokal (*localhost*) untuk fase purwarupa.

- **Perspektif Teknis (*Technical Perspective*):**

Scalability: Arsitektur dapat dirancang modular agar mudah dikembangkan (*scale-up*) sesuai kebutuhan masa depan.

Security & Maintainability: Kendali penuh atas keamanan data (termasuk penerapan Audit Trail yang *immutable*). Pemeliharaan kode sepenuhnya berada di tangan tim internal dengan dokumentasi yang terstandar.

III.5.4 Evaluasi dan Pemilihan Solusi (*Weighted Scoring*)

Untuk menentukan keputusan secara objektif, dilakukan penilaian kuantitatif menggunakan Matriks Keputusan Berbobot. Bobot ditentukan berdasarkan prioritas tugas akhir dan kendala organisasi BUMN (Efisiensi Biaya dan Kepatuhan Regulasi menjadi prioritas utama).

Tabel III.2 Matriks Penilaian Alternatif Solusi

Kriteria Perspektif	Bobot	COTS	Low-Code	Custom App
Perspektif Pengguna (<i>Usability & Adopsi</i>)	29.8%	2	4	5
Perspektif Bisnis (Biaya & Kesesuaian Regulasi)	43.7%	2	3	5
Perspektif Operasional (Kemudahan Implementasi)	10%	2	5	3
Perspektif Teknis (Fleksibilitas Data & Audit)	16.5%	4	2	5
TOTAL SKOR (<i>Weighted</i>)	100%	2.60	3.70	4.80
<i>Keterangan Skor: 1 (Sangat Buruk) - 5 (Sangat Baik)</i>				

Kesimpulan Pemilihan: Berdasarkan analisis di atas, Pengembangan Aplikasi Web Kustom memperoleh skor tertinggi (4.70). Solusi ini unggul signifikan dalam aspek Bisnis dan Teknis, yang merupakan prioritas utama untuk menjawab tantangan integrasi data yang kompleks dan kebutuhan kepatuhan regulasi yang spesifik tanpa membebani organisasi dengan biaya lisensi yang tidak perlu. Meskipun upaya implementasi teknisnya lebih tinggi dibandingkan Low-Code, fleksibilitas arsitektur yang ditawarkan sebanding dengan nilai strategis yang dihasilkan.

BAB IV

DESAIN KONSEP SOLUSI

Bab ini menguraikan perancangan konseptual dari Sistem Manajemen Risiko Terpadu yang diusulkan untuk mengatasi permasalahan fragmentasi data dan inefisiensi proses di PT Telkom Data Center. Desain solusi ini menerjemahkan kebutuhan fungsional yang telah didefinisikan pada bab sebelumnya menjadi arsitektur sistem yang konkret, mencakup arsitektur alur kerja modul (*Process Architecture*) dan arsitektur data (*Data Architecture*).

IV.1 Model Konseptual Sistem Usulan

Solusi yang dikembangkan adalah aplikasi berbasis web (*web-based application*) yang dirancang dengan pendekatan modular namun terintegrasi penuh pada lapisan basis data. Berbeda dengan sistem lama yang berorientasi pada dokumen (*document-centric*), sistem usulan ini berorientasi pada data (*data-centric*), di mana setiap entitas informasi saling terhubung untuk membentuk ekosistem tata kelola risiko yang utuh.

IV.1.1 Arsitektur Data Relasional (*Comprehensive Data Architecture*)

Fondasi dari integrasi sistem ini adalah desain basis data relasional yang kuat. Gambar 4.7 (ERD) menggambarkan transformasi dari struktur data datar (*flat*) menjadi terstruktur. Berikut adalah analisis mendalam mengenai komponen-komponen kunci dalam arsitektur data tersebut:

1. Sentralitas Tabel Risk Register

Tabel *Risk Register* (berwarna hijau) bertindak sebagai entitas pusat (*hub*). Berbeda dengan *spreadsheet* yang menyimpan semua data dalam satu baris, tabel ini hanya menyimpan atribut inti risiko, sementara atribut lainnya disimpan sebagai referensi (*Foreign Key*):

- *Risk_ID* sebagai *Primary Key*.

• Control_ID, Objectif_ID, KRI_ID sebagai *Foreign Keys*.
Implikasi: Perubahan pada nama kontrol atau deskripsi objektif cukup dilakukan satu kali di tabel induknya, dan akan terupdate otomatis di seluruh risiko yang terkait. Ini menjamin konsistensi data 100%.

2. Integrasi Strategi via Modul Objectif

Tabel *Objectif* memiliki relasi langsung dengan *Risk Register*. Lebih dalam lagi, tabel *Performance Indicator* terhubung dengan *Objectif*.

Implikasi: Sistem dapat melacak secara granular: "Jika Risiko A terjadi, Indikator Kinerja B akan terganggu, yang pada akhirnya menggagalkan Objektif C". Rantai kausalitas ini tidak mungkin dipetakan dalam sistem manual sebelumnya.

3. Standarisasi Kontrol via Modul Governance

Tabel *Control* dan *Framework* (berwarna merah) menyimpan perpustakaan kontrol baku.

Implikasi: Auditor dapat dengan mudah memverifikasi apakah kontrol yang diterapkan di lapangan (*Risk Register*) sudah sesuai dengan standar kepatuhan yang diwajibkan (*Framework*). Atribut *Desired Control Maturity* dan *Current Control Maturity* pada tabel *Control* memungkinkan analisis kesenjangan (*gap analysis*) kapabilitas unit.

4. Akuntabilitas via Modul User & Unit

Tabel *User* dan *Unit* (berwarna biru) tidak sekadar daftar nama, tetapi pengelola hak akses (RBAC).

Implikasi: Setiap baris data risiko memiliki "tuan" yang jelas. Kolom *Risk_Owner* dan *Risk_Agent* dalam tabel *Risk Register* memastikan bahwa tanggung jawab mitigasi tidak lagi ambigu.

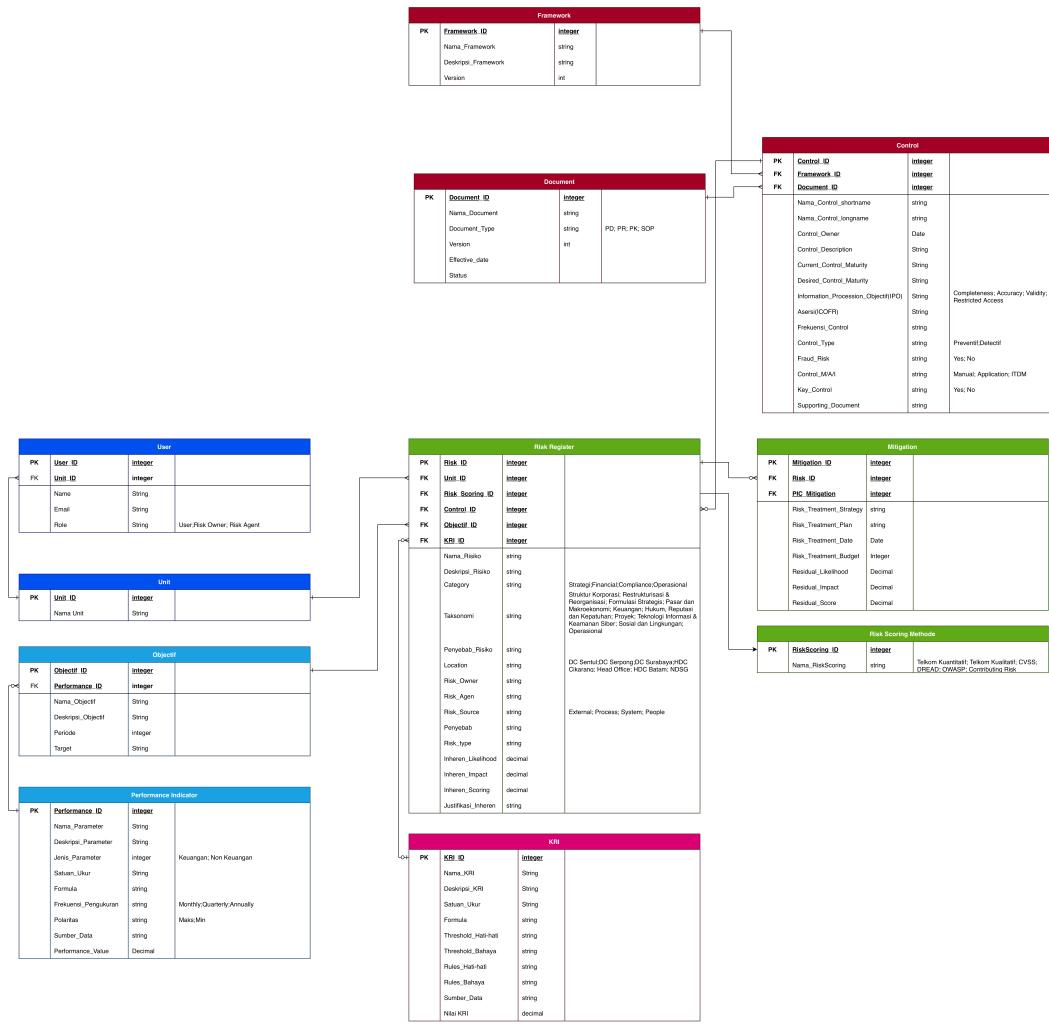
5. Mekanisme Umpaman Balik via Modul Mitigation & KRI

Tabel *Mitigation* mencatat *Residual Risk* (skor sisa setelah mitigasi), sementara tabel *KRI* mencatat pemicu eksternal.

Implikasi: Memungkinkan perhitungan dinamis. Jika status mitigasi selesai, skor *Residual Risk* di *Risk Register* dapat turun otomatis. Sebaliknya, jika Nilai KRI di tabel *KRI* melonjak, status risiko bisa berubah menjadi "Waspada" secara otomatis.

IV.1.2 Arsitektur Alur Sistem Tingkat Tinggi (*High-Level Process Architecture*)

Setelah fondasi data terbentuk, perancangan dilanjutkan pada lapisan proses bisnis. Gambar 4.2 mengilustrasikan transformasi radikal dari alur kerja linear-manual menjadi ekosistem proses yang terintegrasi dan sirkular. Desain ini ditujukan untuk



Gambar IV.1 Entity Relationship Diagram (ERD) Komprehensif.

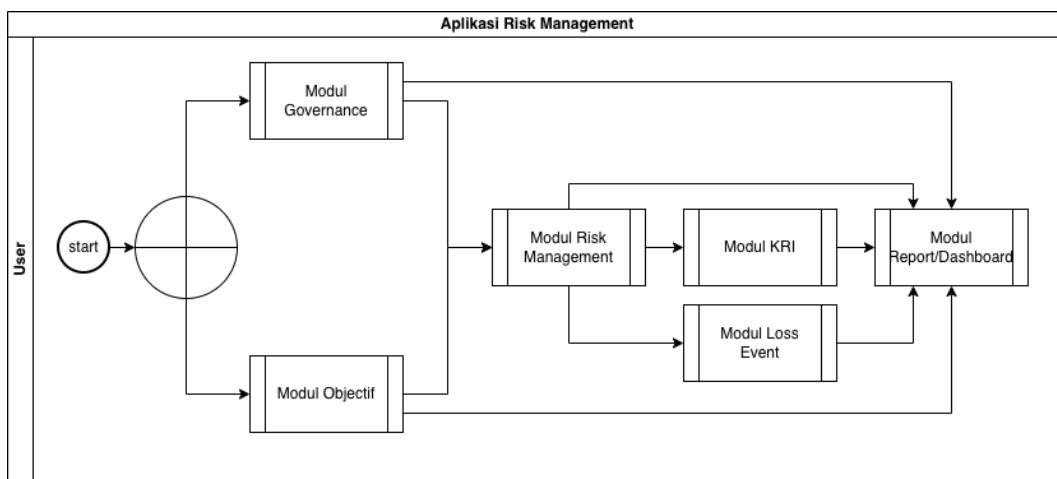
memecahkan masalah inefisiensi alur kerja (*process latency*) yang diidentifikasi pada Bab 3.

Paralelisasi Inisiasi Data (Hulu): Berbeda dengan sistem lama di mana identifikasi risiko sering dilakukan tanpa konteks, sistem usulan menerapkan mekanisme inisiasi paralel. Alur dimulai dengan percabangan (*parallel gateway*) menuju Modul Governance dan Modul Objectif. Mekanisme ini secara sistemik memaksa organisasi untuk mendefinisikan "Aturan Main" (*Governance*) dan "Tujuan Strategis" (*Objectif*) terlebih dahulu, memastikan setiap risiko yang didaftarkan memiliki landasan konteks yang kuat.

Sentralisasi Operasional (Tengah): Output dari inisiasi hulu tersebut dikonsolidasikan ke dalam Modul Risk Management. Modul ini bertindak sebagai mesin pemroses utama yang menggantikan fungsi *spreadsheet*

manual, mengubah input statis menjadi data dinamis yang siap dikelola.

Integrasi Hilir dan Umpang Balik: Hasil pengelolaan risiko tidak berhenti sebagai arsip mati, melainkan didistribusikan ke Modul KRI dan Modul Loss Event untuk pemantauan spesifik. Data dari modul hilir ini kemudian diumpang balik secara otomatis ke Modul Report/Dashboard, menciptakan siklus informasi tertutup yang memungkinkan pengambilan keputusan eksekutif berbasis data *real-time*.



Gambar IV.2 Arsitektur Alur Sistem Usulan / BPMN Level 0 Baru.

IV.1.3 Detil Alur Kerja Sub-Modul (*Sub-Module Workflows*)

Untuk memberikan gambaran operasional yang lebih granular, berikut adalah analisis mendalam terhadap alur kerja lima sub-modul utama. Penjabaran ini menyoroti bagaimana desain alur kerja baru (*To-Be Process*) secara spesifik mengeliminasi titik-titik kelemahan (*pain points*) yang ditemukan pada proses eksisting (*As-Is Process*).

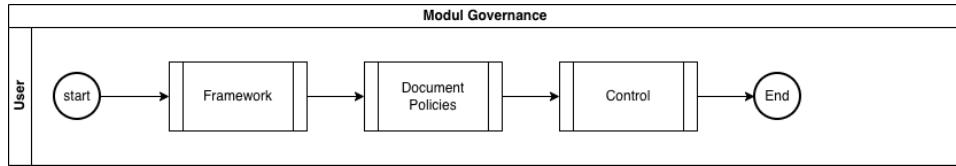
IV.1.3.1 Modul Tata Kelola (*Governance Module*)

Modul ini dirancang sebagai solusi atas permasalahan variabilitas data input yang tidak terstruktur (*unstructured data integrity issues*).

Analisis Alur Kerja: Sebagaimana divisualisasikan pada diagram, proses berjalan secara sekuensial dimulai dari *Start* → *Framework* → *Document Policies* → *Control* → *End*.

Mekanisme Perbaikan Sistem: Alur ini menegakkan standarisasi data melalui hierarki kebijakan yang ketat. Sistem tidak mengizinkan pendefinisian kontrol

secara *ad-hoc* (bebas ketik) seperti pada *spreadsheet*. Sebaliknya, pengguna diwajibkan menurunkan Standar Internasional (Framework) menjadi Kebijakan Internal, yang kemudian diterjemahkan menjadi Katalog Kontrol baku. Hal ini menjamin konsistensi terminologi di seluruh unit kerja dan memfasilitasi audit kepatuhan yang efisien.



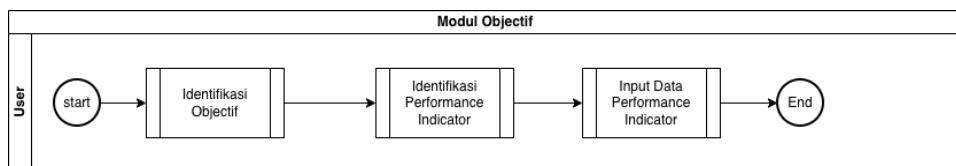
Gambar IV.3 Alur Kerja Modul Governance.

IV.1.3.2 Modul Objektif & Kinerja (*Objective Module*)

Modul ini dikembangkan untuk menjawab isu *"Strategic Blind Spots"* di mana risiko operasional sering kali terputus dari konteks tujuan bisnis perusahaan.

Analisis Alur Kerja: Proses dimulai dari *Start* → Identifikasi Objektif → Identifikasi *Performance Indicator* → Input Data *Performance Indicator* → *End*.

Mekanisme Perbaikan Sistem: Dengan mewajibkan pendefinisian Sasaran Strategis (*Objective*) dan Indikator Kinerja (KPI) di awal proses, sistem menciptakan prasyarat relasional. Risiko yang didaftarkan pada tahap selanjutnya harus dipetakan dampaknya terhadap entitas objektif ini. Desain ini memastikan terciptanya keselarasan strategis (*Strategic Alignment*), sehingga manajemen dapat memantau risiko bukan hanya sebagai masalah teknis, tetapi sebagai ancaman terhadap pencapaian target kinerja.



Gambar IV.4 Alur Kerja Modul Objektif.

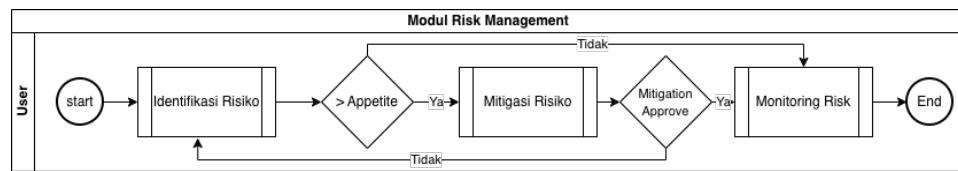
IV.1.3.3 Modul Manajemen Risiko Inti (*Risk Management Module*)

Ini adalah inti operasional sistem yang menggantikan proses manual dengan alur logika otomatis, bertujuan untuk mengatasi hambatan iterasi (*iteration barrier*) dan latensi persetujuan.

Analisis Alur Kerja:

- *Identifikasi Risiko*: Mengambil referensi baku dari Modul Governance & Objective untuk meminimalisir input bebas.
- *Appetite (Decision Gateway)*: Sistem melakukan validasi otomatis skor risiko terhadap matriks selera risiko (*Risk Appetite*). Jika risiko berada di bawah ambang batas, alur dipotong langsung ke pemantauan, mengeliminasi birokrasi yang tidak perlu.
- *Mitigation Approve (Decision Gateway)*: Mendigitalkan proses persetujuan. Jika rencana ditolak (*No*), alur secara otomatis dikembalikan (*loop back*) ke inisiator untuk revisi.

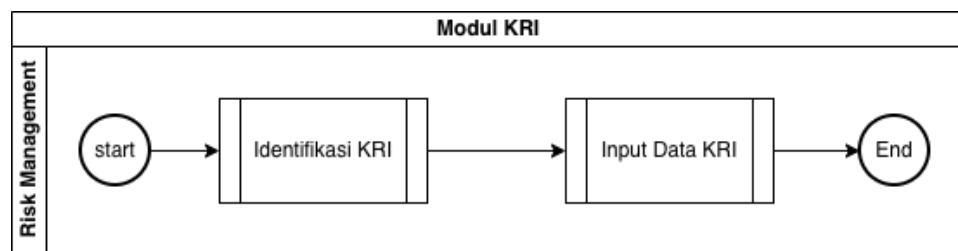
Mekanisme Perbaikan Sistem: Fitur *loop back* otomatis pada diagram ini secara efektif menghilangkan fenomena "dokumen mangkrak" akibat miskomunikasi manual. Status dokumen menjadi transparan, dan notifikasi sistem memastikan siklus revisi berjalan tanpa jeda waktu yang signifikan, mempercepat waktu siklus (*cycle time*) pelaporan risiko secara keseluruhan.



Gambar IV.5 Alur Kerja Modul Risk Management.

IV.1.3.4 Modul Indikator Risiko Kunci (KRI Module)

Modul ini mentransformasi paradigma pemantauan dari pasif-reaktif menjadi proaktif, menjawab kebutuhan akan sistem peringatan dini.



Gambar IV.6 Alur Kerja Modul KRI.

Analisis Alur Kerja: Alur didesain sederhana: *Start* → Identifikasi KRI → Input Data KRI → *End*, namun memiliki dampak implikasi yang besar.

Mekanisme Perbaikan Sistem: Dengan memisahkan input KRI dari laporan kinerja operasional biasa, sistem dapat menetapkan ambang batas (*threshold*)

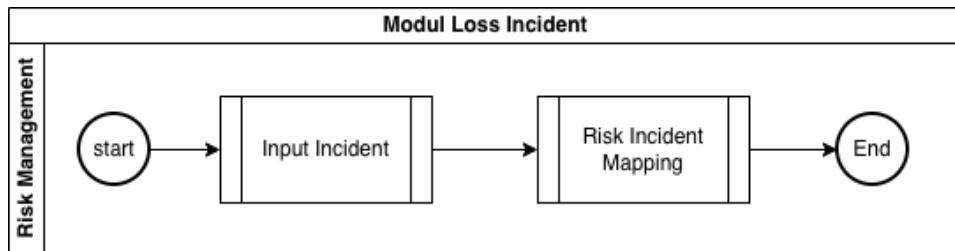
pemicu risiko secara mandiri. Ketika data realisasi diinput, sistem dapat memicu peringatan otomatis jika ambang batas terlampaui, mengatasi masalah keterlambatan respon manajemen yang sebelumnya terjadi akibat menunggu rekapitulasi laporan bulanan.

IV.1.3.5 Modul Insiden Kerugian (*Loss Event Module*)

Modul ini berfungsi sebagai memori institusi untuk mengatasi fragmentasi data insiden yang sebelumnya tersebar di berbagai log terpisah.

Analisis Alur Kerja: Alur kunci pada modul ini adalah *Start* → Input Incident → Risk Incident Mapping → *End*.

Mekanisme Perbaikan Sistem: Langkah *Risk Incident Mapping* merupakan inovasi kritis yang wajibkan setiap pencatatan insiden untuk ditautkan (*tagged*) secara digital ke profil risiko yang relevan di database. Mekanisme ini menjamin bahwa data sejarah kerugian tidak hilang, melainkan terakumulasi sebagai basis data empiris untuk memvalidasi dan mengkalibrasi prediksi risiko di masa depan, meningkatkan akurasi profil risiko secara berkelanjutan.



Gambar IV.7 Alur Kerja Modul Loss Event.

IV.2 Analisis Komparatif (*Before vs After*)

Penerapan desain konsep solusi di atas menawarkan transformasi signifikan dibandingkan dengan kondisi sistem saat ini. Tabel 4.1 merangkum perbandingan karakteristik utama antara sistem manual eksisting (Bab 3) dengan desain solusi sistem usulan (Bab 4).

Tabel IV.1 Perbandingan Sistem Eksisting dan Sistem Usulan

Dimensi Komparasi	Kondisi Saat Ini (<i>Current State</i>) - Masalah Utama	Desain Solusi Usulan (<i>Future State</i>)
1. Arsitektur Data	<p>Masalah: Isolasi Data (<i>Data Silos</i>) Kesulitan mengagregasi informasi karena data tersimpan parsial tanpa standar.</p> <p>Terfragmentasi: Data tersebar di ratusan fail spreadsheet lokal di tiap unit. Tidak ada <i>Master Data</i> yang baku.</p>	<p>Terpusat (Centralized): Menggunakan basis data relasional tunggal (<i>Single Source of Truth</i>). Taksonomi risiko terstandarisasi via <i>Master Data</i>.</p>
2. Alur Proses	<p>Masalah: Inefisiensi & Latensi Proses manual menyebabkan "dokumen mangkrak" dan siklus pelaporan lambat.</p> <p>Linear & Manual: Proses berjalan sekuensial dengan "lempar-tangkap" dokumen via email. Rawan kemacetan (<i>bottleneck</i>) tanpa notifikasi.</p>	<p>Terintegrasi & Otomatis: Alur kerja berbasis sistem (<i>System Workflow</i>). Status dokumen terpantau <i>real-time</i> dan notifikasi persetujuan berjalan otomatis.</p>
(Berlanjut ke halaman berikutnya)		

Dimensi Komparasi	Kondisi Saat Ini (<i>Current State</i>)	Desain Solusi Usulan (<i>Future State</i>)
3. Konektivitas Strategis	<p>Masalah: Strategic Blind Spot Ketidakmampuan melihat dampak risiko operasional terhadap tujuan perusahaan.</p> <p>Terputus (<i>Disconnected</i>): Risiko operasional tidak terhubung langsung dengan Sasaran Perusahaan. Hubungan bersifat asumsi manual.</p>	Terpetakan (<i>Mapped</i>): Relasi <i>many-to-many</i> antara Risiko, KRI, dan Objektif terkunci dalam database. Dampak strategis terlihat jelas.
4. Validitas & Audit	<p>Masalah: Audit Gap & Non-Repudiation Kesulitan memverifikasi siapa yang mengubah data dan kapan.</p> <p>Rendah: Persetujuan informal (WhatsApp) sulit dilacak. Tidak ada log perubahan data (<i>Audit Trail</i>).</p>	Tinggi: Penerapan <i>Role-Based Access Control</i> (RBAC) dan pencatatan <i>Immutable Audit Log</i> untuk setiap perubahan data.
5. Pelaporan	<p>Masalah: Information Lag Keputusan terlambat diambil karena data tidak tersedia saat dibutuhkan.</p> <p>Statis & Lagging: Laporan rekapitulasi manual bulanan yang sering kali sudah kadaluwarsa saat dibaca manajemen.</p>	Dinamis & Real-time: Dasbor eksekutif yang di-generate otomatis dari data langsung (<i>live data</i>), mendukung keputusan cepat.

Melalui desain konsep ini, solusi yang diusulkan tidak hanya mendigitalisasi proses manual, tetapi secara fundamental mengubah arsitektur informasi manajemen risiko

PT Telkom Data Center menjadi lebih tangguh, akuntabel, dan bernilai strategis.

BAB V

RENCANA SELANJUTNYA

Bab ini menguraikan strategi komprehensif untuk mentransformasikan desain konsep Sistem Manajemen Risiko Terpadu menjadi artefak perancangan yang konkret dan teruji. Rencana ini disusun untuk menjamin bahwa pelaksanaan Tugas Akhir berjalan secara terstruktur, efisien, dan menghasilkan luaran yang valid sesuai dengan standar akademik serta kebutuhan operasional PT Telkom Data Center.

V.1 Rencana Implementasi

Implementasi dalam konteks penelitian ini difokuskan pada realisasi artefak desain sistem (*system design artifacts*) dan purwarupa antarmuka (*interface prototype*). Pendekatan ini diambil mengingat batasan masalah yang menargetkan penyusunan rancangan sistem komprehensif, bukan pengembangan kode program fungsional secara penuh.

V.1.1 Linimasa Pengerjaan (*Timeline*)

Linimasa pengerjaan disusun mencakup seluruh rangkaian kegiatan mulai dari investigasi awal hingga evaluasi akhir pasca-sidang. Setiap tahapan dirancang secara sekkuensial namun adaptif, memastikan ketersediaan waktu yang memadai untuk iterasi desain berdasarkan umpan balik. Pelaksanaan Tugas Akhir

	September				October				November				December			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Penentuan topik																
Pencarian dosen pembimbing																
Penulisan Bab 1																

Gambar V.1 *Gantt chart* periode pertama.

diproyeksikan berlangsung dari periode persiapan pada Oktober 2024 hingga penyelesaian akhir pada Februari 2026.

	January				February				March				April			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Penulisan Bab 1																
Penulisan Bab 2																
Survei kuisisioner																
Penulisan Bab 3																
Scope Definition																
Problem Analysis																
Requirement Analysis																
Logical Design																
Physical Design & Integration																

Gambar V.2 *Gantt chart* periode kedua.

Pada tahap penyusunan proposal (hingga awal 2025), fokus utama adalah pematangan konsep dan analisis masalah. Tahap inti perancangan visual dan *prototyping* akan dilaksanakan secara intensif pada pertengahan hingga akhir tahun 2025, memberikan ruang yang cukup untuk iterasi desain yang matang sebelum evaluasi final di awal 2026.

	May				Juni				Juli			
	1	2	3	4	1	2	3	4	1	2	3	4
Penulisan Bab 3												
Physical Design & Integration												
Testing												
Penulisan Bab 4												

Gambar V.3 *Gantt chart* periode ketiga.

V.1.2 Kebutuhan Sumber Daya Pelaksanaan

Untuk mendukung proses perancangan dan pengujian yang optimal, diperlukan serangkaian perangkat keras dan lunak yang spesifik. Pemilihan alat didasarkan pada standar industri desain produk digital saat ini untuk memastikan hasil rancangan yang profesional dan mudah dikomunikasikan kepada pemangku kepentingan.

Tabel V.1 Rencana Kebutuhan Sumber Daya Pelaksanaan

Komponen	Deskripsi & Spesifikasi	Fungsi Utama
Alat Survey	<i>Figma prototype</i> dan <i>Google Forms</i>	Menjalankan prototype untuk diuji pengguna, serta langsung penarikan survey kualitatif dan kuantitatif melalui <i>Google Forms</i> .
Pemodelan Sistem	<i>Draw.io</i>	Menyusun diagram alur proses (<i>BPMN</i>), diagram data (<i>ERD</i>), dan arsitektur informasi secara terstruktur.
Desain Antarmuka	<i>Figma (Berbasis Cloud)</i>	Platform utama untuk merancang antarmuka (UI) dari tingkat <i>wireframe</i> hingga <i>high-fidelity</i> , serta membuat prototipe interaktif (<i>clickable</i>).
Pengolahan Data	<i>Microsoft Excel / Google Sheets</i>	Mengelola data simulasi (<i>dummy data</i>) untuk Taksonomi Risiko dan KRI yang akan diinput ke dalam desain.
Dokumentasi	<i>LaTeX</i>	Penyusunan laporan tugas akhir dan manajemen sitasi literatur secara otomatis.

Data yang digunakan dalam perancangan ini adalah data simulasi yang dikonstruksi menyerupai karakteristik operasional PT Telkom Data Center, guna menjaga kerahasiaan data perusahaan namun tetap memberikan konteks yang realistik saat pengujian.

V.2 Desain Pengujian dan Evaluasi

Evaluasi merupakan tahapan kritis untuk menjamin kualitas luaran penelitian. Mengingat luaran berupa rancangan sistem, evaluasi dilakukan melalui dua pendekatan utama: Verifikasi Desain dan Validasi Pengguna.

V.2.1 Verifikasi Desain (*Design Verification*)

Verifikasi adalah proses penjaminan mutu internal untuk memastikan bahwa rancangan sistem telah mengakomodasi seluruh kebutuhan teknis yang didefinisikan sebelumnya.

- **Metode:** *Requirement Traceability Matrix* (RTM).

- **Prosedur:** Penulis akan memetakan setiap poin Spesifikasi Kebutuhan Fungsional (FR-01 s.d. FR-14) terhadap elemen antarmuka yang telah dibuat.
- **Contoh:** Untuk FR-04 (Pemetaan Risiko-KRI), akan diverifikasi ketersediaan fitur *dropdown* atau *linkage* pada halaman *Mockup Risk Register*.

V.2.2 Validasi Pengguna (*User Validation*)

Validasi bertujuan mengukur penerimaan rancangan oleh calon pengguna potensial.

- **Metode:** *Usability Testing* dengan pendekatan *Task-Based Scenario*.
- **Partisipan:** Responden terbatas yang merepresentasikan peran *Risk Owner* (Lini 1) dan *Risk Manager* (Lini 2).
- **Instrumen Pengukuran:**
 - **Tingkat Keberhasilan (*Completion Rate*):** Persentase skenario tugas yang berhasil diselesaikan pengguna tanpa bantuan.
 - **Kepuasan Pengguna (*User Satisfaction*):** Diukur menggunakan kuesioner *System Usability Scale (SUS)* atau Skala Likert (1-5) untuk dimensi kemudahan (*Ease of Use*) dan kegunaan (*Usefulness*).

V.3 Analisis Risiko dan Mitigasi

Setiap proyek penelitian memiliki ketidakpastian. Analisis risiko berikut disusun untuk mengantisipasi potensi hambatan yang dapat mengganggu linimasa atau kualitas hasil penelitian, beserta strategi mitigasi yang proaktif.

Tabel V.2 Analisis Risiko dan Mitigasi Proyek

Kategori Risiko	Potensi Risiko	Strategi Mitigasi (<i>Mitigation Strategy</i>)
Akses Data	Kesulitan mendapatkan struktur data riil atau akses wawancara lanjutan dengan pihak perusahaan karena kesibukan operasional.	Menggunakan referensi standar industri (ISO 31000, COSO) dan laporan tahunan BUMN sejenis untuk merekonstruksi data simulasi yang valid secara logis.
		Berlanjut ke halaman berikutnya...

Tabel V.2 – lanjutan dari halaman sebelumnya

Kategori Risiko	Potensi Risiko	Strategi Mitigasi (<i>Mitigation Strategy</i>)
Kualitas Desain	Prototipe visual dinilai terlalu abstrak atau "kurang nyata" oleh responden, sehingga bias dalam hasil pengujian.	Menerapkan prinsip <i>High-Fidelity Design</i> dengan detail visual tinggi (warna, tipografi, interaksi mikro) di Figma agar pengalaman penggunaan menyerupai aplikasi asli.
Lingkup	Terjadinya <i>Scope Creep</i> (pelebaran fitur) saat proses perancangan detil, di mana keinginan untuk menambah fitur estetik mengaburkan fungsi utama.	Melakukan pembekuan kebutuhan (<i>Requirement Freeze</i>) yang ketat setelah Bab III disetujui. Ide fitur tambahan didokumentasikan sebagai saran pengembangan (<i>future works</i>).
Waktu	Keterlambatan dalam proses iterasi desain akibat revisi berulang yang tidak terencana.	Menetapkan batasan jumlah iterasi mayor per modul dan menjadwalkan sesi asistensi rutin untuk mendapatkan umpan balik dini.

Melalui perencanaan yang terstruktur serta mitigasi risiko yang matang, diharapkan pelaksanaan Tugas Akhir ini dapat berjalan lancar dan menghasilkan rancangan sistem yang memberikan nilai tambah signifikan bagi tata kelola risiko PT Telkom Data Center.

LAMPIRAN A. DATA PENDUKUNG ANALISIS KEPUTUSAN

Tabel 3 *Pairwise comparison matrix* untuk penentuan bobot opsi

Criteria	Business	Technical	User	Operational	Calculated Weight
<i>Business</i>	1	2	3	5	43.7%
<i>Technical</i>	0.5	1	3	5	29.8%
<i>User</i>	0.33	0.33	1	3	16.5%
<i>Operational</i>	0.2	0.2	0.33	1	10.0%

Tabel 4 Tinjauan finansial model untuk ketiga opsi (*Detail*)

Option	Efficiency		Avoided Fines		Cost		Subtotal
	Time Cut	Cost Saved	Prob.	Cost Saved	CAPEX	OPEX (5Yr)	
<i>Low Code</i>	15%	Rp16,875,000	80%	Rp100,000,000	Rp15,000,000	Rp50,000,000	Rp51,875,000
<i>Rent</i>	60%	Rp67,500,000	40%	Rp300,000,000	Rp0	Rp250,000,000	Rp117,500,000
<i>Custom Web</i>	75%	Rp84,375,000	30%	Rp350,000,000	Rp75,000,000	Rp10,000,000	Rp349,375,000