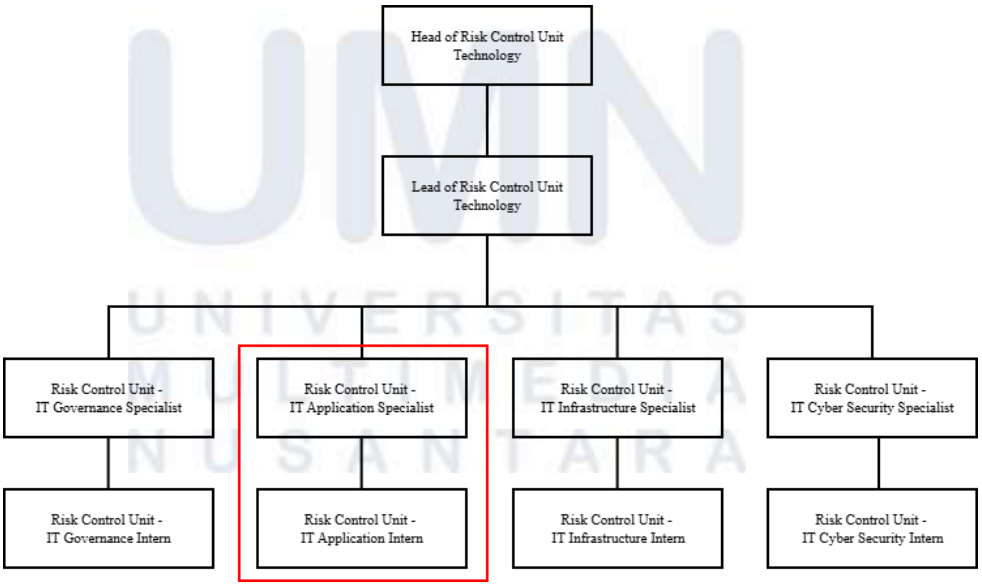
BAB III
PELAKSANAAN KERJA

3.1 Kedudukan dan Koordinasi

3.1.1 Kedudukan

Posisi *Risk Control Unit Technology Intern* di PT Bank CIMB Niaga Tbk diisi oleh lima orang mahasiswa aktif yang berasal dari berbagai universitas di Indonesia. Unit ini berada di bawah naungan *Head of Risk Control Unit – Technology*, yang membawahi empat bagian utama, yaitu RCU – *IT Application*, RCU – *IT Infrastructure*, RCU – *IT Cyber Security*, dan RCU – *IT Governance*. Struktur organisasi tersebut ditunjukkan pada Gambar 3.1 yang menggambarkan hubungan hierarkis antar komponen serta posisi peserta magang di dalam unit. Meskipun setiap komponen memiliki fokus dan metode kerja yang berbeda, seluruh unit kerja saling terintegrasi dan senantiasa berupaya memastikan bahwa proses penilaian risiko teknologi informasi dapat berjalan secara efisien, konsisten, dan berorientasi pada kebutuhan bisnis.



Gambar 3.1. Diagram Hierarki Divisi Risk Control Unit

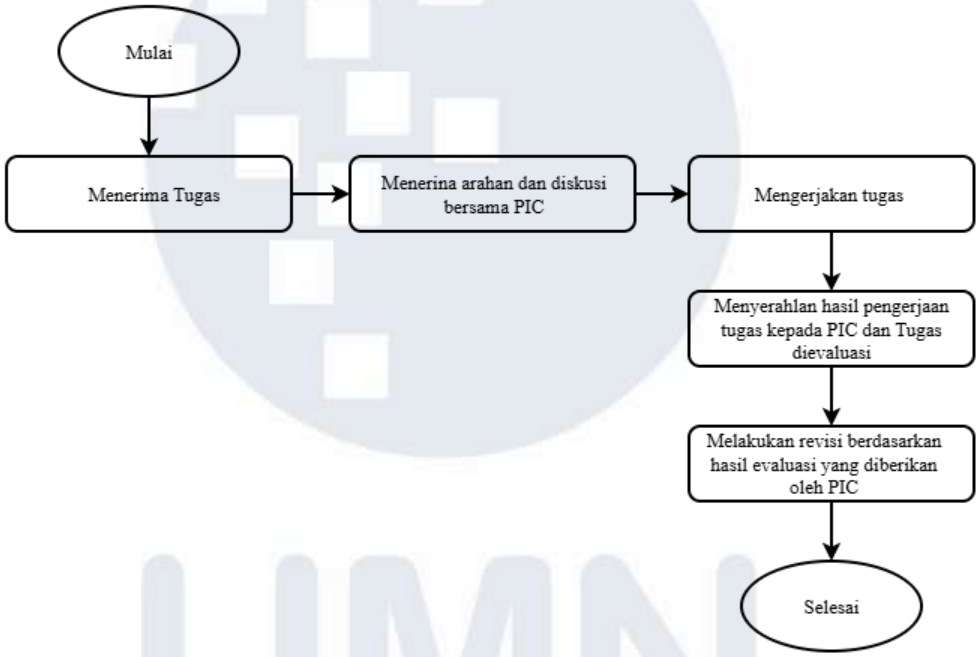
Penunjukan *Person in Charge* (*PIC*) dilakukan berdasarkan penempatan *intern* pada subunit masing-masing, sehingga setiap *intern* memiliki pembimbing langsung yang memahami ruang lingkup tugas yang dijalankan. Seluruh hasil pekerjaan yang dilakukan oleh *intern* wajib dilaporkan kepada *PIC* terkait sebagai bagian dari mekanisme *monitoring*, validasi, dan evaluasi kinerja. Walaupun pelaksanaan tugas harian berada di bawah arahan *PIC*, hasil kerja *intern* tetap berada dalam pengawasan *Head of Risk Control Unit – Technology* melalui koordinasi rutin dan pelaporan berkala antarbagian. Mekanisme ini bertujuan untuk memastikan keselarasan pekerjaan *intern* dengan tujuan unit serta menjaga kualitas hasil kerja agar sesuai dengan standar pengendalian risiko yang ditetapkan.

Selain struktur kerja yang jelas, lingkungan kerja di *Risk Control Unit – Technology* juga dikenal kondusif dan suportif. Hubungan profesional antara *intern* dan anggota tim terjalin dengan baik, ditandai dengan komunikasi yang terbuka dan sikap saling menghargai. *Intern* diberikan ruang untuk bertanya, berdiskusi, serta menyampaikan pendapat maupun ide yang berkaitan dengan pelaksanaan tugas. Suasana kerja yang kolaboratif ini tidak hanya membantu *intern* dalam menyelesaikan pekerjaan, tetapi juga mendorong proses pembelajaran yang berkelanjutan. Dengan dukungan tim yang responsif dan lingkungan kerja yang positif, *intern* dapat mengembangkan pemahaman yang lebih komprehensif mengenai pengelolaan risiko teknologi informasi dalam konteks industri perbankan.

3.1.2 Koordinasi

Kerja sama yang efektif antara mahasiswa magang dan pihak perusahaan menjadi salah satu faktor kunci dalam mendukung kelancaran pelaksanaan program magang. Struktur koordinasi yang tertata dengan baik tidak hanya mempermudah proses penyampaian tugas, tetapi juga membantu mahasiswa memahami ekspektasi, standar kerja, serta prioritas yang ditetapkan oleh unit terkait. Melalui mekanisme koordinasi yang jelas, setiap tugas yang diberikan dapat dikerjakan secara terarah dan sesuai dengan

kebutuhan organisasi. Hasil pekerjaan mahasiswa kemudian dapat dievaluasi secara langsung oleh *Person in Charge* (*PIC*) pada hari yang sama dengan waktu penugasan, sehingga proses perbaikan dan penyempurnaan dapat dilakukan secara cepat dan efektif. Pola koordinasi yang terstruktur ini memberikan kesempatan bagi mahasiswa untuk mengasah kemampuan komunikasi, manajemen waktu, serta tanggung jawab profesional dalam lingkungan kerja yang nyata.



Gambar 3.2. Bagan Alur Koordinasi

Gambar 3.2 menunjukkan bagan alur koordinasi dalam pelaksanaan kegiatan magang. Proses koordinasi diawali dengan pemberian tugas oleh *Person in Charge* (*PIC*), yang disertai dengan arahan awal dan sesi diskusi untuk memastikan kesamaan pemahaman terkait tujuan, ruang lingkup, serta tenggat waktu pekerjaan. Tahap diskusi ini menjadi penting untuk meminimalkan kesalahan interpretasi dan memastikan mahasiswa memahami konteks tugas secara menyeluruh. Setelah arahan diberikan, mahasiswa melaksanakan tugas sesuai dengan instruksi yang telah disampaikan, baik secara mandiri maupun melalui koordinasi lanjutan dengan tim apabila diperlukan.

Hasil pengerjaan tugas kemudian diserahkan kembali kepada *PIC* untuk dilakukan evaluasi dan pemberian umpan balik. Apabila ditemukan kekurangan atau diperlukan penyesuaian, *intern* akan melakukan revisi berdasarkan masukan yang diberikan hingga hasil pekerjaan dinyatakan sesuai dengan standar yang ditetapkan. Alur koordinasi ini memastikan setiap tahapan pekerjaan berjalan secara sistematis, komunikatif, dan terkontrol, serta mendorong terciptanya hubungan kerja yang profesional antara mahasiswa magang dan pihak perusahaan. Selain itu, pola koordinasi yang diterapkan juga membantu *intern* memahami dinamika kerja di lingkungan korporasi, khususnya dalam hal pelaporan, evaluasi, dan penyempurnaan hasil kerja secara berkelanjutan.

3.2 Tugas yang Dilakukan

Program magang yang dijalankan selama enam bulan memberikan kesempatan bagi mahasiswa untuk memperoleh pengalaman langsung dalam memahami dinamika pengawasan risiko di bidang teknologi informasi, khususnya dalam lingkungan industri perbankan yang memiliki tingkat kompleksitas dan regulasi yang tinggi. Penulis ditempatkan pada posisi *Risk Control Unit – IT Application Intern* di PT Bank CIMB Niaga Tbk, dengan peran utama membantu tim dalam memastikan proses pengendalian risiko terhadap sistem dan aplikasi berjalan sesuai dengan ketentuan internal perusahaan serta regulasi yang berlaku. Penempatan ini memberikan wawasan praktis mengenai bagaimana fungsi pengendalian risiko diterapkan dalam operasional teknologi informasi secara nyata.

Selama periode magang, penulis berpartisipasi dalam berbagai kegiatan yang berkaitan dengan analisis, evaluasi, dan pemantauan risiko teknologi. Kegiatan yang dilakukan tidak hanya bersifat administratif, tetapi juga melibatkan pemahaman terhadap konteks temuan dan implikasinya terhadap keamanan serta keandalan sistem. Beberapa aktivitas utama meliputi penelaahan hasil temuan audit pada memo *Application Security Requirement* (*ASR*), serta pemeriksaan ketersediaan dan kelengkapan dokumen pendukung seperti *Control Issues Management* (*CIM*) dan *Memo Ketentuan Kewajiban* (*MKK*). Melalui keterlibatan

dalam kegiatan tersebut, penulis memperoleh pemahaman mengenai alur tindak lanjut temuan audit serta pentingnya dokumentasi sebagai bagian dari pengendalian risiko. Selain kegiatan analisis dokumen, penulis juga berkontribusi dalam pengembangan dashboard *Power BI* untuk monitoring *Control Issues Management*. Dashboard yang dikembangkan berfungsi untuk menampilkan status tindak lanjut temuan secara visual dan interaktif, sehingga memudahkan tim dalam memantau progres penyelesaian, mengidentifikasi temuan yang masih terbuka, serta mendukung proses pengambilan keputusan berbasis data. Pemanfaatan visualisasi data ini memberikan gambaran nyata mengenai peran teknologi dalam meningkatkan efektivitas proses monitoring dan pelaporan risiko di unit kerja.

Seluruh aktivitas magang dijalankan di bawah supervisi *Person in Charge* (*PIC*) dari bagian *IT Application*. Mahasiswa magang dituntut untuk mampu bekerja secara mandiri, memiliki tingkat ketelitian yang tinggi dalam pengolahan data, serta tetap menjaga koordinasi yang baik dengan tim. Selain itu, mahasiswa juga diharapkan mampu menyesuaikan hasil kerja dengan kebutuhan unit serta standar operasional yang berlaku di *Risk Control Unit – Technology*. Pola kerja ini melatih mahasiswa untuk bertanggung jawab terhadap setiap tugas yang diberikan sekaligus memahami budaya kerja profesional di lingkungan perbankan. Sebagai bentuk dokumentasi dan evaluasi pelaksanaan kegiatan, Tabel 3.1 menyajikan rincian realisasi program kerja yang telah dilaksanakan selama periode magang, yang disusun dengan mengacu pada rencana kegiatan yang tercantum dalam Tabel 1.2

Tabel 3.1. Realisasi Program Kerja Magang.

No.	Aktivitas	Minggu ke-	Tanggal Mulai Aktivitas	Tanggal Akhir Aktivitas
1.	**Melakukan review atas proses dan identifikasi risiko pada unit kerja IT & Cyber Security, dan**	**17 September 2025 – 10 Oktober 2025**	**17 September 2025**	**6 Oktober 2025**

No.	Aktivitas	Minggu ke-	Tanggal Mulai Aktivitas	Tanggal Akhir Aktivitas
	memastikan impleentasi sudah sesuai dengan kebijakan dan prosedur yang berlaku			
1.1	Melakukan identifikasi aplikasi terdampak temuan audit tahun 2021 – 2025 dan melakukan pendokumentasian tingakt *criticality* berdasarkan nilai yang telah ditetapkan dalam memo audit.	17 September 2025 – 26 September 2025	17 September 2025	26 September 2025
1.2	Mengelompokkan temuan berdasarkan kategori risiko untuk mendukung proses analisis dan penilaian efektivitas pengendalian.	29 September 2025 – 6 Oktober 2025	29 September 2025	6 Oktober 2025
2.	**Melakukan review dan analisa atas pengelolaan akses Privilaged UserID (PUID) untuk emmastikan akses dikelolas ecara memadai.**	**15 September 2025 – 16 September 2025**	**15 September 2025**	**16 September 2025**
2.1	Membuat flowchart terkait proses pengajuan	15 September 2025 – 16	15 September 2025	16 September 2025

No.	Aktivitas	Minggu ke-	Tanggal Mulai Aktivitas	Tanggal Akhir Aktivitas
	peminjaman PUID berdasarkan SOP.	September 2025		
3.	**Melakukan review dan koordinasi dengan unit kerja IT & Cyber Security untuk memastikan temuan hasil security assesment sudah ditindaklanjuti dan/sudah memiliki rencana perbaikan.**	**8 Oktober 2025 – 20 Oktober 2025**	**8 Oktober 2025**	**20 Oktober 2025**
3.1	Mengolah data apliksi temuan dari memo ASR ke dalam Excel.	8 Oktober 2025 – 15 Oktober 2025	8 Oktober 2025	15 Oktober 2025
3.2	Memeriksa ketersediaan Control issues Management (CIM) dan Memo Ketentuan Kewajiban (MKK) pada masing-masing aplikasi serta mendokumentasikan status penanganan dan rencana tindak lanjut.	16 Oktober 2025 – 20 Oktober 2025	16 Oktober 2025	20 Oktober 2025
4.	**Membuat dashboard monitoring Control Issues**	**3 November 2025 – November 2025**	**3 November 2025**	**3 Desember 2025**

No.	Aktivitas	Minggu ke-	Tanggal Mulai Aktivitas	Tanggal Akhir Aktivitas
	Management (CIM).			
4.1	Merapikan dan menyiapkan data di Excel agar siap diolah di PowerBI.	5 November 2025 – 11 November 2025	5 November 2025	3 Desember 2025
4.2	Mengembangkan dashboard interaktif di Power BI untuk memonitor status CIM.	13 November 2025 – 19 November 2025	13 November 2025	19 November 2025

Dalam pelaksanaan tugas selama program magang di *Risk Control Unit – Technology*, khususnya pada subunit *IT Application*. Berikut beberapa *tools* utama yang digunakan selama program magang berlangsung:

1. Microsoft Excel

Microsoft Excel adalah aplikasi spreadsheet yang banyak digunakan dalam berbagai bidang bisnis dan industri untuk mengelola, menganalisis, dan memvisualisasikan data secara sistematis [16]. Excel memungkinkan pengguna membuat tabel, grafik, serta analisis data menggunakan berbagai rumus dan fungsi, mulai dari yang sederhana seperti SUM dan AVERAGE, hingga fungsi lanjutan seperti VLOOKUP, INDEX-MATCH, dan fungsi logika kompleks [17], [18]. Selain itu, Excel memiliki fitur *pivot table* untuk merangkum data besar, conditional formatting untuk menyoroti informasi penting, serta filter dan sort untuk mempermudah analisis data [19]. Selama magang, Excel digunakan untuk mengelola dan menganalisis data hasil audit aplikasi, melakukan review memo *Application Security Requirement* (ASR), dan mengolah data *Control Issues Management* (CIM). Dengan Excel, proses pembersihan data dan penyelarasan informasi dari berbagai sumber dapat dilakukan dengan lebih cepat dan akurat.

2. Power BI

Power BI adalah platform business intelligence (BI) dari Microsoft yang memungkinkan pengguna untuk mengintegrasikan, menganalisis, dan memvisualisasikan data dari berbagai sumber secara interaktif [20]. Dengan Power BI, data dapat disajikan dalam bentuk dashboard dan laporan visual yang mudah dipahami, seperti grafik, tabel, peta, dan indikator performa (KPIs), sehingga mempermudah pemantauan informasi secara real-time dan mendukung pengambilan keputusan berbasis data [21]. Platform ini juga memiliki fitur transformasi dan pemodelan data melalui *Power Query* dan DAX (Data Analysis Expressions), serta mendukung integrasi otomatis dengan berbagai sumber data seperti Excel, SharePoint, dan SQL Server. Selama magang, Power BI digunakan untuk membuat dashboard monitoring Control Issues Management (CIM). Dashboard ini menampilkan status temuan kontrol, kategori risiko, dan progres tindak lanjut. Dengan kemampuan Power BI untuk memperbarui data secara otomatis dari Excel, setiap perubahan data langsung tercermin di dashboard tanpa perlu input manual, sehingga mengurangi risiko kesalahan dan memastikan akurasi informasi yang disajikan.

3. Draw.io

Draw.io adalah aplikasi berbasis web untuk membuat diagram, flowchart, dan visualisasi proses kerja [22]. Aplikasi ini memungkinkan pengguna menggambarkan alur kerja, hubungan antarproses, serta struktur sistem secara jelas dan terstruktur. Selama program magang, Draw.io digunakan untuk membuat flowchart aktivitas peminjaman *Privilaged UserID* (PUID). Diagram ini membantu tim memahami setiap tahapan proses, mulai dari perencanaan, pengembangan, hingga pengujian aplikasi. Selain itu, visualisasi ini berguna untuk mempermudah koordinasi antarunit dan memastikan setiap langkah pekerjaan terdokumentasi dengan baik.

4. Microsoft Teams

Microsoft Teams adalah platform kolaborasi yang menyediakan berbagai fitur komunikasi berbasis *chat*, panggilan suara dan video, rapat daring, dan ruang kerja tim yang memungkinkan kolaborasi secara *real-time* [23]. Teams mendukung integrasi dengan berbagai aplikasi Microsoft lainnya, seperti Outlook, Excel, Power BI, dan SharePoint, sehingga mempermudah koordinasi dan alur kerja antaranggota tim. Selama program magang, Teams menjadi media komunikasi utama antara intern dan *Person in Charge* (PIC). Intern dapat menerima arahan tugas, mengajukan pertanyaan terkait pekerjaan, dan berdiskusi mengenai strategi penyelesaian tugas secara cepat. Teams juga digunakan untuk mengevaluasi hasil kerja melalui sesi review daring, sehingga intern dan PIC dapat memberikan masukan secara langsung. Penggunaan Teams meningkatkan efektivitas komunikasi, mempercepat proses pengambilan keputusan, dan memastikan setiap anggota tim selalu update terhadap perkembangan tugas.

Tools–tools tersebut digunakan selama program magang dan memiliki peran yang sangat penting dalam mendukung penyelesaian setiap tugas di subunit IT *Application, Risk Control Unit – Technology*. Pemanfaatan *tools* yang tepat membantu memastikan bahwa seluruh aktivitas kerja dapat dilakukan secara sistematis, terstruktur, dan sesuai dengan standar operasional yang berlaku di lingkungan perbankan. Kegiatan magang ini berlangsung selama kurang lebih lima bulan, dimulai sejak 11 September 2025 hingga berakhir sesuai dengan jadwal yang telah ditetapkan, sehingga membutuhkan dukungan *tools* yang mampu menunjang efisiensi kerja dalam jangka waktu yang cukup panjang. Selama periode magang tersebut, penulis tidak hanya menggunakan *tools* sebagai sarana teknis pendukung pekerjaan, tetapi juga sebagai bagian dari proses pembelajaran terhadap alur kerja dan tata kelola teknologi informasi di lingkungan perbankan. Setiap *tools* digunakan secara terintegrasi untuk mendukung proses analisis, dokumentasi, monitoring, dan koordinasi, sehingga pekerjaan dapat diselesaikan secara lebih efektif dan akurat. Penggunaan tools ini juga membantu penulis dalam memahami

keterkaitan antara hasil audit aplikasi, pengelolaan temuan kontrol, serta proses tindak lanjut yang harus dilakukan oleh unit terkait.

3.3 Uraian Pelaksanaan Kerja

3.3.1 Review identifikasi risiko pada unit kerja IT & Cyber Security.

Pada tahap ini, penulis melakukan proses review terhadap aktivitas dan data terkait pengelolaan risiko di unit kerja *IT* & *Cyber Security*, khususnya yang berhubungan dengan tindak lanjut temuan IT Audit. *Review* dilakukan dengan menelaah data temuan audit yang diberikan oleh mentor, memahami konteks permasalahan pada setiap temuan, dan mengidentifikasi aplikasi teknologi informasi yang terdampak. Selain itu, penulis melakukan analisis awal untuk menilai apakah risiko-risiko yang muncul sudah dikelola sesuai kebijakan, prosedur, dan mekanisme pengendalian yang berlaku di perusahaan. Proses tersebut mencakup verifikasi kelengkapan informasi seperti kategori temuan, tingkat kritikalitas, status tindak lanjut, dan kesesuaian antara temuan dan kontrol yang seharusnya diterapkan. Hasil review tersebut menjadi landasan untuk mengelompokkan temuan berdasarkan tingkat criticality dan kategori risiko yang kemudian digunakan dalam proses monitoring dan evaluasi efektivitas pengendalian di unit *IT* & *Cyber Security.*

3.3.1.1 Melakukan identifikasi aplikasi terdampak temuan IT Audit tahun 2021 – 2025 dan mendokumentasikan tingkat criticality berdasarkan nilai yang telah ditetapkan dalam memo audit.

Pada tahap ini, data temuan IT Audit diperoleh dalam bentuk file Excel dari mentor. Data tersebut berisi kumpulan temuan yang berasal dari auditor eksternal dan internal, seperti PwC, Deloitte, Bank Indonesia, OJK, dan audit internal. File tersebut mencakup periode tahun 2021–2025 dan memuat sejumlah kolom utama, antara lain nomor temuan, auditor, permasalahan/risiko/rekomendasi, tanggapan unit terkait, kategori temuan, progress status, target penyelesaian, status temuan, dan status action plan.

Struktur data dapat dilihat pada Tabel 3.2 mengenai data temuan dari IT Audit.

Langkah awal yang dilakukan adalah memahami setiap baris data untuk mengidentifikasi konteks temuan dan aplikasi yang terdampak. Pada tahap ini, penulis menerima tiga file Excel terpisah yang memuat data temuan IT Audit untuk periode 2021 – 2022, 2023, dan 2024 – 2025. Masing-masing file masih terdiri dari beberapa sheet, seperti sheet temuan dari Deloitte, PwC, Bank Indonesia, OJK, dan auditor internal. Agar proses analisis dapat dilakukan secara menyeluruh, penulis membuat sebuah *workbook* baru dan menggabungkan seluruh data dari berbagai *sheet* tersebut, dari BI, OJK, PwC, Deloitte, maupun internal menjadi satu dataset terpadu yang mencakup periode 2021 hingga 2025.

Tabel 3. 2. Data IT Audit tahun 2021 - 2022

No	Audit	Permasalahan	Tanggapan	Kategori Temuan
1	LHA DL	Kontrol keamanan aplikasi A belum sepenuhnya memenuhi standar ASR dan masih terdapat temuan yang belum ditutup.	Unit aplikasi akan melakukan perbaikan kontrol keamanan dan mengajukan retesting ASR	Medium
2	OJK	Berdasrkan pemeriksaan dokumen Daftar Aplikasi, terdapat 4 aplikasi yang belum dilakukan validasi sesuai versi terkini, yaitu: 1. Aplikasi B 2. Tools C Sesuai dengan SE OJK No	Unit terkait telah melakukan identifikasi terhadap aplikasi yang tercantum dalam temuan tersebut. Selanjutnya, unit akan melakukan proses validasi dan pembaruan Daftar Aplikasi sesuai	Medium

No	Audit	Permasalahan	Tanggapan	Kategori Temuan
		21/SEOJK.03/2017 tentang penerapan	dengan versi terkini untuk Aplikasi B, dan Tools C.	
3	LHA EP	Kelemahan kontrol keamanan akses tools E melalui mobile device, di antaranya belum diterapkannya pengaturan keamanan akses secara konsisten pada seluruh perangkat, belum optimalnya mekanisme.	Setuju dengan temuan audit. Unit terkait akan memperkuat kontrol keamanan akses tools E melalui mobile device dengan melakukan peninjauan kebijakan keamanan, penerapan pengaturan keamanan tambahan, serta optimalisasi monitoring akses.	Meidum
4	Tematic Audit	Kelemahan pengelolaan Aplikasi C karena belum terdapat pengaturan yang jelas/pihak yang ditunjuk sebagai petugas dan penanggung jawab pengelolaan Aplikasi C, yaitu belum ditetapkannya application owner dan application custodian secara formal.	Setuju dengan temuan audit. Unit terkait akan menetapkan penanggung jawab pengelolaan Aplikasi C serta pembagian peran dan tanggung jawab secara formal.	High
5	LHA TSD	Pengelolaan perubahan pada	Setuju dengan temuan audit. Unit	Medium

No	Audit	Permasalahan	Tanggapan	Kategori Temuan
		Aplikasi F belum sepenuhnya didukung dengan proses change management yang memadai. Beberapa perubahan aplikasi belum melalui pengujian dan persetujuan formal, sehingga berpotensi menimbulkan gangguan operasional.	terkait akan memperkuat penerapan change management pada Aplikasi F dengan memastikan setiap perubahan melalui proses pengujian, persetujuan, dan dokumentasi sesuai ketentuan.	

Tabel 3.3. Penggabungan Temuan Data IT Audit Tahun 2021 - 2025

No	Auditor	Permasalahan	Aplikasi
1	LHA DL (2021)	Kontrol keamanan aplikasi A belum sepenuhnya memenuhi standar ASR dan masih terdapat temuan yang belum ditutup.	Aplikasi A
2	OJK (2022)	Berdasrkan pemeriksaan dokumen Daftar Aplikasi, terdapat 4 aplikasi yang belum dilakukan validasi sesuai versi terkini, yaitu: 1. Aplikasi B 2. Tools C Sesuai dengan SE OJK No 21/SEOJK.03/2017 tentang penerapan	1. Aplikasi B 2. Tools C
3	LHA EP (2023)	Kontrol keamanan Aplikasi X belum sepenuhnya memenuhi standar keamanan aplikasi.	Aplikasi X
4	LHA TSD (2025)	Pengujian DRP pada Aplikasi E belum dilakukan secara berkala	Aplikasi E

Tampilan hasil penggabungan data dapat dilihat pada Tabel 3.3 yang menunjukkan struktur data setelah seluruh sumber digabungkan. Setelah

seluruh data dari berbagai sheet berhasil digabungkan, penulis terlebih dahulu membuat sebuah sheet ringkasan yang memuat tabel berisi informasi inti dari setiap temuan, yaitu nomor temuan, tahun, auditor, permasalahan atau risiko atau solusi, tanggapan, dan nama aplikasi. Sheet ini berfungsi sebagai dasar untuk analisis lanjutan karena seluruh data temuan telah disajikan dalam format yang lebih ringkas dan terstruktur.

Tabel 3.4. Pembersihan Data dan Penggunaan Pivot Tabel

No	Aplikasi		No	Aplikasi (Cleaning)
1	Aplikasi A		1	Aplikasi A
2	Aplikasi B		2	Aplikasi B
3	Aplikasi C		3	Aplikasi C
4	Aplikasi D		4	Aplikasi D
5	Aplikasi E		5	Aplikasi E
6	Aplikasi F		6	Aplikasi F
7	Aplikasi G		7	Aplikasi G
8	Aplikasi H		8	Aplikasi H
9	AplikasiH		9	Aplikasi I
10	Aplikasi J		10	Aplikasi J

Pada tahap berikutnya, sebagaimana ditunjukkan pada Tabel 3.4, penulis melakukan proses pembersihan data, khususnya pada kolom nama aplikasi, mengingat adanya variasi penulisan yang merujuk pada objek aplikasi yang sama. Proses pembersihan ini mencakup penyeragaman penulisan, penghapusan duplikasi, serta penyelarasan nama aplikasi agar setiap aplikasi hanya muncul dalam satu format yang konsisten. Pembersihan data dilakukan dengan memanfaatkan fungsi *TRIM* untuk menghilangkan spasi berlebih dan fungsi *UPPER* untuk menyeragamkan penggunaan huruf kapital, sehingga data menjadi lebih rapi dan siap untuk dianalisis. Setelah data nama aplikasi tersusun secara konsisten, tahap

selanjutnya adalah pembuatan *pivot table* untuk mengidentifikasi pola temuan berdasarkan aplikasi.

Tabel 3.5. Pivot Table melihat jumlah setiap Aplikasi

No	Row Labels (Aplikasi)	Count
1	No Aplikasi	69
2	Aplikasi A	21
3	Aplikasi B	19
4	Aplikasi C	13
5	Aplikasi D	10
6	Aplikasi E	9
7	Aplikasi F	9
8	Aplikasi G	9
9	Aplikasi H	6
10	Aplikasi I	6
11	Aplikasi J	6
12	Aplikasi K	5
13	Aplikasi L	4
14	Aplikasi M	4
15	Aplikasi N	3

Setelah data dinyatakan bersih dan konsisten, penulis melanjutkan ke tahap analisis menggunakan *pivot table* sebagaimana ditampilkan pada Tabel 3.5. *Pivot table* digunakan sebagai alat bantu untuk merangkum dan mengelompokkan data temuan audit berdasarkan nama aplikasi. Melalui fitur ini, penulis dapat menghitung jumlah temuan untuk setiap aplikasi secara otomatis, sehingga memudahkan dalam melihat distribusi dan frekuensi temuan pada periode 2021 hingga 2025. Hasil pengolahan menggunakan *pivot table* memberikan gambaran yang lebih jelas mengenai aplikasi mana yang paling sering menjadi objek temuan audit. Penggunaan

pivot table tidak hanya berfungsi sebagai alat perhitungan, tetapi juga sebagai dasar pengambilan insight awal dalam proses analisis risiko aplikasi.

3.3.1.2 Mengelompokkan temuan berdasarkan kategori risiko untuk mendukung proses analisis dan penilaian efektivitas pengendalian

Setelah aplikasi terdampak dan tingkat *criticality* dipetakan pada tahap sebelumnya, langkah selanjutnya adalah melakukan pengelompokan setiap temuan berdasarkan kategori risiko, yaitu *Important*, *Critical*, *Very Important*, dan *Necessary*. Tahap ini bertujuan untuk memberikan struktur yang lebih jelas terhadap hasil temuan audit sehingga tingkat urgensi dan dampak risiko dari masing-masing temuan dapat dianalisis secara lebih sistematis. Proses pengelompokan dilakukan dengan meninjau kembali isi temuan pada file audit serta mencermati klasifikasi risiko yang telah ditetapkan oleh pihak yang melakukan penilaian. Proses pemetaan kategori risiko tersebut ditunjukkan pada Tabel 3.6 yang menggambarkan hasil *mapping criticality* dari temuan audit yang telah diolah.

Melalui proses penyusunan dan penataan data tersebut, seluruh temuan audit yang sebelumnya tersebar dalam berbagai dokumen dan periode dapat dikelompokkan secara sistematis ke dalam kategori risiko yang seragam. Pengelompokan ini menghasilkan output berupa rekapitulasi jumlah temuan berdasarkan kategori risiko selama periode 2021–2025, yang memberikan gambaran kuantitatif mengenai distribusi tingkat risiko yang dihadapi oleh aplikasi-aplikasi terkait. Selain itu, hasil pengolahan data juga memberikan gambaran awal mengenai jenis risiko yang paling sering muncul, sehingga dapat diidentifikasi kecenderungan risiko dominan dalam pengelolaan aplikasi teknologi informasi.

Tabel 3.6. Pemetaan Risiko Aplikasi

No	Aplikasi	*Count*	No	*Criticality*
1	No Aplikasi	69		N/A
2	Aplikasi A	21	1	Critical
3	Aplikasi B	19	2	Critical
4	Aplikasi C	13	3	Very Important
5	Aplikasi D	10	4	Important
6	Aplikasi E	9	5	Critical
7	Aplikasi F	9	6	Necessary
8	Aplikasi G	9	7	Important
9	Aplikasi H	6	8	Important
10	Aplikasi I	6	9	Critical
11	Aplikasi J	3		N/A
12	Aplikasi K	3	10	Necessary

Pemetaan kategori risiko ini memungkinkan dilakukan analisis awal mengenai keterkaitan antara tingkat risiko dan aplikasi yang terdampak. Dengan demikian, dapat diketahui aplikasi mana yang cenderung memiliki temuan dengan tingkat risiko lebih tinggi dan memerlukan perhatian khusus. Informasi ini menjadi penting sebagai dasar dalam menentukan prioritas tindak lanjut serta penentuan area pengendalian yang perlu diperkuat. Hasil dari tahap ini selanjutnya digunakan sebagai landasan dalam analisis efektivitas pengendalian dan evaluasi risiko pada tahap berikutnya, sehingga proses pengelolaan risiko teknologi informasi dapat dilakukan secara lebih terarah dan berbasis data.

3.3.2 Analisis pengelolaan akses Privileged User ID.

Tugas selanjutnya yang dilakukan penulis adalah pembuatan flowchart proses pengajuan *Privileged User ID* (PUID). Kegiatan ini bertujuan untuk memetakan alur kerja pemberian akses khusus yang

diberikan kepada pengguna tertentu dalam lingkungan sistem internal perusahaan. Akses PUID memiliki tingkat sensitivitas yang tinggi karena memungkinkan pengguna untuk melakukan aktivitas dengan hak istimewa, seperti pengelolaan sistem, perubahan konfigurasi, atau akses terhadap data penting. Oleh karena itu, proses pengajuan dan persetujuan PUID perlu memiliki mekanisme kontrol yang jelas, terdokumentasi, dan dapat dipahami oleh seluruh pihak yang terlibat. Tahapan awal dalam mengerjakan tugas ini adalah dengan membaca *Standard Operational Procedure* terkait Pengelolaan Akses *Privilaged UserID*. Informasi tersebut digunakan untuk memahami peran masing-masing pihak dalam proses pengajuan, mulai dari pengguna yang membutuhkan akses, atasan langsung sebagai pihak yang memberikan persetujuan awal, hingga unit terkait yang bertanggung jawab dalam melakukan evaluasi dan persetujuan lanjutan. Pemahaman terhadap alur kerja ini menjadi penting agar *flowchart* yang disusun dapat merepresentasikan proses yang berjalan secara akurat.

Berdasarkan hasil pengumpulan dan pemahaman tersebut, penulis kemudian menyusun *flowchart* menggunakan aplikasi Draw.io. *Flowchart* dirancang untuk menggambarkan setiap tahapan secara berurutan dan sistematis, dimulai dari pengajuan permohonan akses oleh pengguna, proses validasi oleh atasan langsung, pemeriksaan oleh unit IT Security untuk memastikan kesesuaian dengan kebijakan keamanan, hingga persetujuan akhir oleh pihak yang berwenang. Setiap langkah disusun dengan jelas agar hubungan antarproses dan alur keputusan dapat terlihat dengan mudah. *Flowchart* yang dihasilkan memberikan gambaran visual mengenai proses pengajuan PUID, sehingga memudahkan pihak terkait dalam memahami alur kerja yang harus diikuti. Selain itu, dokumentasi dalam bentuk *flowchart* juga membantu memastikan bahwa pemberian akses khusus dilakukan secara konsisten, terkontrol, dan sesuai dengan kebijakan keamanan yang berlaku. Dengan adanya pemetaan proses ini, potensi

kesalahan prosedur dapat diminimalkan dan transparansi dalam pengelolaan akses istimewa dapat ditingkatkan.

3.3.3 Review tindak lanjut temuan security assessment

Tugas ini berfokus pada verifikasi dan pemantauan tindak lanjut temuan ASR. Proses dimulai dengan mendapatkan data dari memo ASR, yang berisi file ASR dari tiap aplikasi yang digunakan oleh bank. Setiap file ASR diperiksa untuk melihat persentase kepatuhan aplikasi terhadap standar keamanan yang ditetapkan. Aplikasi yang nilai ASR-nya 100% *comply* tidak perlu dimasukkan ke dalam *Excel Summary ASR*, karena tidak memerlukan tindak lanjut. Hanya aplikasi yang belum mencapai 100% yang dicatat ke dalam summary. Untuk setiap temuan, dilakukan pengecekan apakah CIM dan MKK telah dibuat sebagai bentuk remediasi. Apabila dokumen tersebut tersedia, data terkait dicatat ke dalam *Excel*. Jika CIM atau MKK belum tersedia, data dicatat sebagai temuan yang belum lengkap dan menjadi bahan koordinasi lebih lanjut dengan unit terkait.

3.3.3.1 Mengolah data aplikasi temuan dari memo Application Security Requirement ke dalam Microsoft Excel.

Tahap pertama dimulai dengan menerima sejumlah file memo *Application Security Review* (ASR) untuk masing-masing aplikasi yang telah melalui proses *security assessment* oleh tim IT & Cyber Security. Setiap memo ASR berfungsi sebagai dokumen formal yang merekam hasil evaluasi keamanan aplikasi secara menyeluruh. Memo ASR umumnya memuat berbagai informasi penting, antara lain nama aplikasi yang dinilai, tingkat *criticality*, deskripsi temuan keamanan, nilai kepatuhan (*compliance score*), hasil penilaian efektivitas kontrol keamanan, rekomendasi perbaikan yang harus dilakukan, serta target waktu penyelesaian perbaikan yang telah ditetapkan.

Seluruh informasi yang tercantum dalam memo ASR tersebut kemudian dikompilasi dan diolah kembali menggunakan Microsoft Excel

agar proses analisis dapat dilakukan secara lebih terstruktur, sistematis, dan mudah ditelusuri. Pada tahap ini, data yang semula tersebar dalam berbagai dokumen memo dikonversi ke dalam sebuah tabel baru yang berisi ringkasan aplikasi terdampak. Ringkasan ini mencakup skor hasil *security assessment* dalam bentuk persentase pemenuhan kontrol keamanan, jumlah dan jenis temuan yang diidentifikasi, tingkat *criticality* aplikasi, serta target penyelesaian (*target completion date*) untuk masing-masing temuan. Untuk memastikan konsistensi dan kemudahan analisis lanjutan, format tabel diseragamkan sehingga seluruh memo ASR yang berasal dari aplikasi dan periode yang berbeda dapat digabungkan ke dalam satu *dataset* terpadu. Proses standardisasi ini menjadi penting guna meminimalkan perbedaan format data dan menghindari potensi kesalahan interpretasi. Hasil dari tahap pengolahan ini adalah sebuah *summary sheet* yang berperan sebagai dasar dalam proses analisis berikutnya, khususnya untuk melakukan pengecekan kelengkapan dokumen pendukung atas setiap temuan keamanan, seperti *Corrective Improvement Memo* (CIM) dan *Mitigation & Key Action* (MKK).

3.3.3.2 Memeriksa ketersediaan Control Issues Management dan Memo Ketentuan Kewajiban pada masing – masing aplikasi dan mendokumentasikan status penanganan serta rencana tindak lanjut.

Setelah data dari memo ASR dirapikan, tahap berikutnya adalah melakukan pengecekan ketersediaan CIM dan MKK untuk tiap aplikasi, sekaligus mendokumentasikan status penanganan dan rencana tindak lanjut. Proses ini diawali dengan pembuatan *summary Excel* yang memuat seluruh daftar aplikasi dari memo ASR beserta skor ASR masing-masing, sebagai indikator kesiapan pengendalian keamanan. Setiap aplikasi kemudian dicocokkan dengan file CIM dan MKK yang diterima dari mentor atau unit terkait untuk memastikan tindak lanjut terhadap temuan telah tercatat. Pengecekan dilakukan pada beberapa aspek penting, antara lain: ketersediaan CIM sebagai bukti pencatatan temuan, ketersediaan MKK,

target date sebagai batas waktu penyelesaian perbaikan, status penanganan seperti "*Open*", "*On Progress*", atau "*Closed*", serta progres tindak lanjut yang telah dilakukan, seperti update sistem atau perbaikan kontrol keamanan.

Tabel 3.7. Data Control Issue Management

Issue Name	***Desc***	***Date Issues***	***ActionID***
Ketidaksesuaian standar keamanan aplikasi A terhadap ASR	Berdasarkan hasil review ASR, masih terdapat beberapa kontrol keamanan yang belum terpenuhi, antara lain ketentuan panjang dan kompleksitas password serta mekanisme account lockout.	10/01/2024	I-00-ID-2024
Penerapan kontrol keamanan aplikasi B belum sesuai standar ASR.	Dari hasil review ASR, ditemukan pengaturan session timeout dan pencatatan log autentikasi yang belum diterapkan secara optimal.	12/02/2024	I-01-ID-2024
Ketidakpatuhan kontrol akses aplikasi C terhadap ketentuan ASR.	Review ASR menunjukkan masih terdapat kekurangan pada penerapan kontrol akses dan pembatasan hak akses pengguna.	24/02/2024	I-19-ID-2024
Kelemahan penerapan pengamanan data pada aplikasi D.	Berdasarkan hasil ASR, mekanisme enkripsi data sensitif pada aplikasi belum sepenuhnya sesuai standar keamanan.	01/03/2024	I-23-ID-2024
Kekurangan implementasi monitoring keamanan pada aplikasi E.	Hasil review ASR menunjukkan mekanisme monitoring dan logging keamanan aplikasi belum mencakup seluruh aktivitas kritikal.	03/03/2025	I-12-ID-2025

Issue Name	*Desc*	*Date Issues*	*ActionID*
Ketidaksesuaian pengelolaan autentikasi pada aplikasi F.	Berdasarkan hasil review ASR, pengaturan autentikasi aplikasi belum sepenuhnya memenuhi standar, khususnya pada kebijakan password dan pengamanan akses pengguna.	19/03/2025	I-19-ID-2025
Kelemahan pengendalian keamanan akses pada aplikasi G	Hasil review ASR menunjukkan penerapan kontrol keamanan akses aplikasi belum optimal, termasuk mekanisme pembatasan akses dan pencatatan aktivitas pengguna.	21/04/2025	I-30-ID-2025

Data *Control Issues Management* (CIM) pada Tabel 3.7 digunakan untuk mengidentifikasi dan memonitor tindak lanjut atas hasil *Application Security Requirement* (ASR) yang dinyatakan tidak *comply* atau belum mencapai tingkat kepatuhan 100%. Aplikasi dengan hasil ASR yang tidak 100% wajib dibuatkan CIM atau MKK sebagai bentuk remediasi atas temuan keamanan yang teridentifikasi. Dalam pelaksanaan tugas ini, penulis mengacu pada beberapa sumber data utama, yaitu folder memo ASR untuk memperoleh informasi detail terkait nama aplikasi dan persentase tingkat kepatuhan hasil *review*, dan laporan CIM yang digunakan untuk menelusuri detail isu yang berasal dari temuan ASR.

Pada laporan CIM, kolom *Issue Name* digunakan untuk memastikan bahwa isu yang dicatat merupakan hasil temuan ASR, yang umumnya ditandai dengan penamaan "Finding ASR". Kolom *Date Issue Identified* digunakan sebagai acuan dalam pengisian tanggal pada *Exception* M*emo as of,* sedangkan kolom *Action ID* digunakan untuk menelusuri detail temuan ASR yang merujuk langsung pada memo ASR terkait. Informasi mengenai batas waktu penyelesaian tindak lanjut diperoleh dari kolom *Action Due*

Date dan digunakan sebagai referensi dalam pengisian *due date* pada *Exception* Memo. Kolom *Action Status* menunjukkan status penanganan CIM, yaitu apakah temuan telah ditutup (*close*) atau masih dalam proses penyelesaian (*open*).

Data CIM tersebut kemudian dikaitkan dengan hasil review pada Summary Memo ASR untuk memastikan konsistensi antara temuan ASR, *exception* yang diberikan, dan status penyelesaiannya. Melalui proses ini, penulis dapat memastikan bahwa setiap aplikasi dengan hasil ASR yang tidak comply telah memiliki CIM atau MKK yang terdokumentasi dengan baik, lengkap dengan informasi status penanganan dan target penyelesaian yang jelas. Hasil pengolahan data ini menjadi dasar dalam proses monitoring tindak lanjut temuan ASR serta mendukung evaluasi efektivitas pengendalian keamanan aplikasi pada unit IT & Cyber Security.

Gambar 3.3. Output Summary ASR

Gambar 3.3 menampilkan ringkasan hasil pengecekan ASR yang dicatat dalam bentuk *summary memo*. Summary memo ASR digunakan untuk merangkum informasi utama terkait hasil penilaian keamanan aplikasi, termasuk identitas aplikasi, persentase tingkat kepatuhan, serta status apakah aplikasi tersebut telah memenuhi standar yang ditetapkan atau masih memerlukan tindak lanjut. Hasil pengecekan ini menjadi dasar dalam menentukan kebutuhan pembuatan CIM, khususnya untuk aplikasi dengan nilai ASR yang tidak mencapai 100%. *Summary* memo ini juga berfungsi sebagai referensi utama dalam proses verifikasi antara data memo ASR dan

data CIM, sehingga memastikan bahwa setiap temuan keamanan telah tercatat secara konsisten dan ditindaklanjuti melalui mekanisme pengelolaan isu yang berlaku.

3.3.4 Perancangan Dashboard Monitoring Control Issues Management (CIM)

Setiap temuan keamanan yang tercatat dalam *Control Issues Management* (CIM) memerlukan tindak lanjut yang jelas, terdokumentasi, dan dapat dipantau secara berkelanjutan. Pembuatan dashboardnya menggunakan data audit aplikasi tahun 2025. Pemantauan temuan secara manual dinilai kurang efektif karena menyulitkan proses pelacakan progres penyelesaian, identifikasi temuan yang belum ditindaklanjuti, serta pemantauan status temuan secara menyeluruh dan real-time. Kondisi tersebut mendorong perlunya media pemantauan yang lebih terstruktur dan informatif. Oleh karena itu, dilakukan perancangan *dashboard* monitoring CIM menggunakan Power BI dengan memanfaatkan data *Control Issues Management* yang bersumber dari audit aplikasi tahun 2025. *Dashboard* ini dirancang untuk menyajikan informasi temuan secara ringkas dan terintegrasi, termasuk status temuan, target tanggal penyelesaian, PIC, dan unit kerja yang bertanggung jawab. Melalui visualisasi ini, pihak terkait dapat dengan mudah mengidentifikasi temuan yang masih dalam proses, temuan yang belum ditindaklanjuti, serta memantau progres penyelesaian secara lebih efektif. Keberadaan dashboard diharapkan dapat mendukung proses monitoring dan pengambilan keputusan terkait pengelolaan temuan CIM di lingkungan IT & Cyber Security.

3.3.4.1 Pembersihan dan Pengolahan Data *Control Issues Management* (CIM) menggunakan Microsoft Excel

Data Control Issues Management (CIM) yang digunakan dalam perancangan dashboard diperoleh dalam format Microsoft Excel dan berasal dari audit aplikasi tahun 2025. Data tersebut memuat informasi yang cukup lengkap, seperti nomor temuan, auditor, permasalahan atau risiko beserta

rekomendasi, kategori temuan atau prioritas, tanggapan unit terkait, grup dan departemen terkait, PIC, target tanggal penyelesaian, progress status, status action plan, serta status temuan. Struktur data awal masih bersifat kompleks dan belum sepenuhnya siap untuk diolah menggunakan Power BI, terutama karena adanya penggunaan *merged cells* dan format tabel yang tidak konsisten.

Pembuatan sheet baru pada Gambar 3.4, dilakukan dengan memuat kolom-kolom yang relevan sesuai kebutuhan *dashboard* monitoring CIM. Kolom yang digunakan meliputi auditor, tanggapan, PIC, DIC atau unit kerja terkait, target tanggal temuan, status *action plan*, dan status temuan. Pemilihan kolom ini bertujuan untuk menyederhanakan struktur data agar hanya informasi yang dibutuhkan dalam proses pemantauan yang dipertahankan. Data selanjutnya dibersihkan dengan menghilangkan duplikasi, menyeragamkan format tanggal dan teks, serta menyesuaikan penulisan kategori agar konsisten antar entri.

No	Auditor	Permasalahan / Issue Name	Tanggapan	Divisi (DIC)	PIC	Target Date Temuan	Bulan	Tahun	Status Action Plan
1	OJK 2024	Ketidaksesuaian kebijakan kata sandi pada aplikasi utama	Dari hasil review ADK, ditemukan bahwa pengaturan password belum sepenuhnya memenuhi ketentuan minimum panjang dan kompleksitas.	Infrastructure & Operations	Sahat Pasi Simatupang	31-Aug-25	August	2025	Closed
2	OJK 2024	Mekanisme autentikasi pengguna belum diperkuat	Bank sepakat dengan temuan dan akan menerapkan penguatan autentikasi melalui pemisahan kontrol login.	Cyber Defense COE	Rinaldi Parulian Sinaga	30-Sep-25	September	2025	Closed
3	OJK 2024	Penerapan prinsip least privilege belum optimal	Melakukan evaluasi, masih terdapat user dengan hak akses melebihi kebutuhan fungsi tersenut.	Strategic Planning & Architecture	Jeffry Kurniawan	31-Oct-25	October	2025	Closed
4	OJK 2024	Konfigurasi keamanan server belum sesuai standar internal	Bank akan melakukan penyesuaian konfigurasi keamanan server sesuai kebijakan dan hasil ADK.	Cyber Defense COE	Rinaldi Parulian Sinaga	31-Dec-25	December	2025	In Progress
5	Deloitte 2025	Pemantauan log keamanan sistem belum menyeluruh	Bank sepakat dan akan meningkatkan cakupan monitoring dan logging pada sistem kritikal.	Infrastructure & Operations	Darwin H	31-Dec-25	December	2025	In Progress
6	Bank Indonesia 2024	Implementasi enkripsi data sensitif belum konsisten	Berdasarkan hasil pemeriksaan, enkripsi data belum diterapkan secara merata pada seluruh proses bisnis aplikasi.	Cyber Strategy & Resilience	Eric Sutedra	30-Jan-26	January	2026	Open

Gambar 3.4. Struktur Data CIM untuk *Dashboard* Monitoring.

Pengolahan dan pembersihan data tersebut menghasilkan dataset yang rapi, terstruktur, dan kompatibel dengan Power BI. Dataset ini digunakan untuk memvisualisasikan temuan CIM yang berasal dari audit aplikasi tahun 2025 ke dalam *dashboard* monitoring. Visualisasi yang dihasilkan memungkinkan pemantauan status penanganan dan progres penyelesaian temuan dilakukan secara lebih akurat dan terstruktur. Tahapan ini berperan penting dalam memastikan dashboard CIM dapat berfungsi

secara optimal sebagai alat bantu pemantauan temuan dan koordinasi tindak lanjut antarunit kerja.

3.3.4.2 Pembuatan *dashboard* menggunakan Power BI.

Setelah data berhasil dibersihkan dan disusun kembali ke dalam *sheet* baru yang hanya memuat kolom-kolom relevan, tahap selanjutnya adalah pembuatan *dashboard* monitoring menggunakan Power BI. *Dashboard* ini dirancang sebagai sarana visualisasi data untuk membantu proses pemantauan temuan secara lebih terstruktur dan sistematis. Pemanfaatan Power BI dipilih karena mampu menyajikan data dalam bentuk visual interaktif yang mudah dipahami, serta mendukung kebutuhan monitoring temuan secara lebih efisien dibandingkan dengan metode pemantauan manual melalui file *spreadsheet*.

Proses pembuatan dashboard diawali dengan mengimpor dataset yang telah melalui tahap pembersihan di Microsoft Excel ke dalam Power BI. Dataset tersebut kemudian diperiksa kembali untuk memastikan konsistensi format data, terutama pada kolom tanggal, status, dan kategori, agar dapat diolah dengan baik oleh Power BI. Kolom-kolom utama yang digunakan dalam pembuatan visualisasi meliputi auditor, tanggapan unit terkait, *person in charge* (PIC), departemen atau unit kerja terkait (DIC), target tanggal penyelesaian temuan, status *action plan*, dan status temuan. Kolom-kolom ini dipilih karena merepresentasikan informasi inti yang dibutuhkan dalam proses pemantauan dan evaluasi tindak lanjut temuan CIM.

Visualisasi pada *dashboard* disusun untuk memberikan gambaran menyeluruh mengenai kondisi temuan. Informasi auditor ditampilkan dalam bentuk Pie Chart sehingga memudahkan identifikasi sumber temuan, baik yang berasal dari auditor eksternal seperti Bank Indonesia, OJK, Deloitte, maupun dari auditor internal. Penyajian ini membantu dalam memahami distribusi temuan berdasarkan sumber audit serta memberikan konteks

terhadap karakteristik temuan yang muncul. Selain itu, kolom tanggapan, PIC, dan departemen terkait divisualisasikan untuk mempermudah penelusuran tanggung jawab penanganan temuan serta mendukung koordinasi antarunit yang terlibat dalam proses tindak lanjut.

Aspek waktu dan progres penyelesaian temuan juga menjadi fokus utama dalam *dashboard*. Kolom target tanggal penyelesaian, status *action plan*, dan status temuan divisualisasikan dalam bentuk grafik dan indikator status untuk menunjukkan apakah suatu temuan telah diselesaikan, masih dalam proses, atau belum ditindaklanjuti. Penyajian ini memberikan gambaran yang jelas mengenai progres penanganan temuan serta membantu mengidentifikasi temuan yang berpotensi melewati target waktu penyelesaian. Dengan informasi tersebut, pihak yang berkepentingan dapat melakukan pemantauan secara lebih proaktif dan mengambil langkah lanjutan apabila diperlukan.

Dashboard yang dikembangkan juga dilengkapi dengan fitur filter dan *drill-down* yang memungkinkan pengguna untuk melakukan pemantauan secara lebih mendalam berdasarkan kriteria tertentu, seperti auditor, PIC, unit kerja, atau status temuan. Fitur ini memberikan fleksibilitas dalam analisis data, memungkinkan pengguna untuk menelusuri detail temuan tertentu tanpa harus memeriksa data secara manual satu per satu. Selain itu, dashboard dapat digunakan untuk melihat pola dan tren penyelesaian temuan dalam periode tertentu, sehingga mendukung evaluasi efektivitas proses tindak lanjut secara keseluruhan.

Penerapan dashboard monitoring CIM berbasis Power BI membantu meningkatkan keterbacaan dan transparansi informasi terkait unit mana yang sudah membaut CIM. Informasi yang sebelumnya tersebar dalam file Excel dapat disajikan dalam satu tampilan terpadu yang mudah dipahami. Selain sebagai alat pemantauan, dashboard monitoring CIM ini juga berfungsi sebagai media pendukung pelaporan dan evaluasi berkala bagi

Risk Control Unit – Technology. Informasi yang tersaji dalam dashboard dapat digunakan sebagai bahan diskusi dalam koordinasi internal maupun rapat tindak lanjut dengan unit terkait, karena memberikan gambaran kondisi temuan secara ringkas namun komprehensif. Dengan adanya dashboard ini, proses pembaruan status temuan dapat dilakukan secara lebih terkontrol, serta membantu memastikan bahwa setiap temuan memiliki kejelasan penanggung jawab dan rencana tindak lanjut yang terdokumentasi. Penggunaan dashboard monitoring CIM berbasis Power BI juga membuka peluang pengembangan lebih lanjut, seperti penambahan indikator kinerja atau analisis tren penyelesaian temuan lintas periode, sehingga dapat mendukung peningkatan efektivitas pengendalian risiko teknologi informasi secara berkelanjutan.

3.3.5 Kendala yang Ditemukan

Selama menjalani program magang di *Risk Control Unit – Technology*, penulis menghadapi beberapa kendala yang memengaruhi kelancaran pelaksanaan tugas sehari-hari. Kendala tersebut terutama berkaitan dengan keterbatasan perangkat kerja dan dukungan teknologi yang tersedia, yang secara langsung berdampak pada efisiensi proses analisis data dan pengolahan informasi. Kondisi ini menjadi tantangan tersendiri mengingat sebagian besar aktivitas kerja magang berkaitan dengan pengolahan data audit dan security assessment yang membutuhkan perangkat dan sistem pendukung yang memadai. Adapun kendala yang ditemukan antara lain sebagai berikut:

1. Keterbatasan akses internet pada laptop perusahaan

Kendala pertama yang dihadapi adalah keterbatasan akses internet pada laptop perusahaan yang dipinjamkan kepada penulis. Laptop tersebut hanya memiliki akses ke aplikasi internal tertentu, seperti Outlook dan Microsoft 365 (Teams, Excel, Word, dan PowerPoint), dengan akses internet yang sangat terbatas. Keterbatasan ini menyebabkan penulis tidak dapat secara

leluasa mencari referensi tambahan, membuka dokumentasi pendukung, atau mengakses sumber informasi lain yang diperlukan untuk memperdalam pemahaman terhadap temuan audit dan security assessment. Akibatnya, dalam beberapa kondisi penulis harus menggunakan dua perangkat secara bersamaan, yaitu laptop perusahaan untuk pekerjaan resmi dan laptop pribadi untuk mengakses internet atau melakukan pencarian informasi pendukung. Penggunaan dua perangkat ini membutuhkan kehati-hatian agar data yang diolah tetap konsisten dan sesuai dengan standar keamanan informasi yang berlaku di lingkungan perusahaan, sekaligus menambah waktu dan fokus dalam penyelesaian pekerjaan.

2. Versi perangkat lunak yang terbatas

Kendala berikutnya yaitu Microsoft 365 yang tersedia masih menggunakan versi lama, sehingga beberapa fitur terbaru tidak dapat dimanfaatkan secara optimal. Kondisi ini cukup berpengaruh terutama pada saat melakukan pemrosesan data dan integrasi dengan Power BI, di mana beberapa fungsi berjalan kurang stabil dan terkadang mengalami error atau keterlambatan (lag). Situasi tersebut menyebabkan proses pengolahan data membutuhkan waktu yang lebih lama dibandingkan dengan kondisi ideal, serta menuntut penulis untuk melakukan penyesuaian dalam metode kerja agar hasil yang diharapkan tetap dapat tercapai.

3.3.6 Solusi atas Kendala yang Ditemukan

Menghadapi berbagai kendala tersebut, penulis berupaya untuk tetap menjaga kelancaran pelaksanaan tugas dengan menerapkan beberapa langkah penyesuaian dan solusi yang sesuai dengan kebijakan serta arahan dari unit kerja. Setiap permasalahan yang muncul tidak hanya dipandang sebagai hambatan, tetapi juga sebagai kesempatan untuk melatih kemampuan adaptasi dan pemecahan masalah dalam lingkungan kerja profesional. Untuk mengatasinya, penulis menerapkan solusi sebagai berikut:

1. Pelaporan gangguan perangkat ke mentor.

Ketika terjadi gangguan pada perangkat kerja, penulis secara aktif melaporkannya kepada mentor sebagai pihak yang berwenang untuk memberikan arahan lebih lanjut. Melalui koordinasi dengan mentor, permasalahan teknis pada laptop perusahaan kemudian ditindaklanjuti dengan pembuatan tiket ke tim IT Service agar dapat ditangani secara resmi sesuai prosedur yang berlaku. Langkah ini membantu memastikan bahwa setiap kendala perangkat tercatat dengan baik dan mendapatkan penanganan yang tepat, sekaligus menjaga kepatuhan terhadap aturan penggunaan fasilitas perusahaan.

2. Penggunaan dua perangkat kerja.

Penggunaan dua perangkat kerja menjadi solusi alternatif yang diterapkan penulis untuk menjaga kelancaran pelaksanaan tugas selama program magang. Laptop perusahaan tetap digunakan untuk seluruh aktivitas kerja resmi yang berkaitan langsung dengan data internal, pengolahan file audit, serta koordinasi melalui aplikasi yang telah disediakan perusahaan. Sementara itu, laptop pribadi dimanfaatkan untuk keperluan pendukung, seperti pencarian referensi umum, pemahaman konsep, serta pembuatan data dummy yang tidak mengandung informasi sensitif. Pemisahan penggunaan perangkat ini dilakukan secara hati-hati agar tetap mematuhi kebijakan keamanan informasi dan tidak menimbulkan risiko kebocoran data. Dengan pendekatan tersebut, penulis dapat tetap melanjutkan proses analisis dan penyusunan pekerjaan tanpa harus sepenuhnya bergantung pada keterbatasan akses internet dan spesifikasi perangkat pada laptop perusahaan. Selain membantu efisiensi waktu, penggunaan dua perangkat juga memungkinkan penulis untuk menjaga kualitas hasil pekerjaan agar tetap konsisten dengan kebutuhan unit kerja, meskipun terdapat kendala teknis pada fasilitas yang disediakan.