TESIS

ANALISIS AUDIT MANAJEMEN RISIKO UNTUK MENGELOLA RISIKO IT DENGAN MENGGUNAKAN FRAMEWORK COBIT 2019

(Studi Kasus : Lembaga Amil Zakat Nasional Baitulmaal Muamalat)

disusun oleh

THATA AUTHAR RAZAQ

23.55.2496

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

TESIS

ANALISIS AUDIT MANAJEMEN RISIKO UNTUK MENGELOLA RISIKO IT DENGAN MENGGUNAKAN FRAMEWORK COBIT 2019

(Studi Kasus : Lembaga Amil Zakat Nasional Baitulmaal Muamalat)

RISK MANAGEMENT AUDIT ANALYSIS FOR MANAGING IT RISKS USING THE COBIT 2019 FRAMEWORK

(Case Study : National Zakat Management Institution Baitulmaal Muamalat)

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Pascasarjana
Program Studi PJJ Informatika

disusun oleh

THATA AUTHAR RAZAQ

23.55.2496

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

ANALISIS AUDIT MANAJEMEN RISIKO UNTUK MENGELOLA RISIKO IT DENGAN MENGGUNAKAN FRAMEWORK COBIT 2019
(Studi Kasus : Lembaga Amil Zakat Nasional Baitulmaal Muamalat)

RISK MANAGEMENT AUDIT ANALYSIS FOR MANAGING IT RISKS USING THE COBIT 2019 FRAMEWORK
(Case Study: National Zakat Management Institution Baitulmaal Muamalat)

yang disusun dan diajukan oleh

Thata Authar Razaq

23.55.2496

telah disetujui oleh Dosen Pembimbing Tesis
pada tanggal 10 November 2025

Dosen Pembimbing,

Alva Hendi Muhammad, S.T., M.Eng., Ph.D.
NIK. 190302493

HALAMAN PENGESAHAN

ANALISIS AUDIT MANAJEMEN RISIKO UNTUK MENGELOLA RISIKO IT DENGAN MENGGUNAKAN FRAMEWORK COBIT 2019

(Studi Kasus : Lembaga Amil Zakat Nasional Baitulmaal Muamalat)

RISK MANAGEMENT AUDIT ANALYSIS FOR MANAGING IT RISKS USING THE COBIT 2019 FRAMEWORK

(Case Study: National Zakat Management Institution Baitulmaal Muamalat)

yang disusun dan diajukan oleh

Thata Authar Razaq

23.55.2496

Telah dipertahankan di depan Dewan Penguji
pada tanggal 10 November 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dr. Ferry Wahyu Wibowo, S.Si., M.Cs. **NIK. 190302235**	
Tonny Hidayat, S.Kom., M.Kom., Ph.D. **NIK. 190302182**	
Alva Hendi Muhammad, S.T., M.Eng., Ph.D. **NIK. 190302493**	

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer
Tanggal 10 November 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Thata Authar Razaq
NIM : 23.55.2496

Menyatakan bahwa Tesis dengan judul berikut:

Analisis Audit Manajemen Risiko Untuk Mengelola Risiko IT Dengan Menggunakan Framework COBIT 2019

Dosen Pembimbing : Alva Hendi Muhammad, S.T., M.Eng., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 10 November 2025
Yang Menyatakan,

Thata Authar Razaq

HALAMAN PERSEMBAHAN

Dengan segala puji syukur pada Allah SWT, Tuhan Yang Maha Esa. Atas berkat rahmat dan hidayah-Nya sehingga penelitian ini dapat diselesaikan. Dengan rendah hati penulis persembahkan penelitan ini untuk pihak – pihak yang andil dalam penyelesaiannya.

1. Keluarga tercinta, Bapak, Ibuk, Adik & Mbah, yang selalu memberikan dukungan dan doa yang tiada henti, serta semangat yang tak pernah surut untuk menyelesaikan penelitian.
2. Dosen Pembimbing dan Penguji, yang dengan sabar, penuh perhatian, dan ilmu yang berharga, memberikan bimbingan, arahan, masukan serta koreksi yang sangat membantu bagi penyelesaian dan penyempurnaan penelitian ini.
3. Objek Penelitian, yang memberi akses, meluangkan waktu, tenaga, dan pikiran guna memperoleh data serta informasi yang sangat berharga untuk penyelesaian penelitian.
4. Teman - teman, yang selalu memberikan dukungan moril, membantu dalam proses penelitian, serta berbagi ilmu dan kebahagiaan.
5. Seluruh pihak yang terlibat, baik langsung maupun tidak langsung, yang tidak bisa saya sebut satu per satu yang mana telah memberikan kontribusi dalam penyelesaian penelitian ini.

KATA PENGANTAR

Puji syukur saya panjatkan ke hadirat Allah SWT, Tuhan Yang Maha Esa, atas berkat rahmat dan karunia-Nya, saya dapat menyelesaikan penelitian tesis ini, yang berjudul *"Analisis Audit Manajemen Risiko Untuk Mengelola Risiko IT Dengan Menggunakan Framework COBIT 2019."* Penelitian ini bertujuan untuk memberikan pemahaman mengenai audit manajemen risiko TI menggunakan framework COBIT 2019.

Penelitian ini sulit diselesaikan tanpa dukungan dan bimbingan dari berbagai pihak. Oleh karena itu, saya ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Keluarga tercinta, yaitu Bapak Sundoyo, Ibu Sri Wahyuni, Adik Rhevan Waffir Razaq, Mbah Mainah & Mbah Muh Effendi Rebo, yang selalu memberikan dukungan, semangat dan doa yang tiada henti.
2. Dosen Pembimbing Bapak Alva Hendi Muhammad, S.T., M.Eng., Ph.D. yang telah memberikan arahan, bimbingan, dan waktunya selama proses penyusunan tesis ini.
3. Baitulmaal Muamalat sebagai objek penelitian, yang telah memberikan izin dan data yang sangat berguna untuk kelancaran penelitian tesis ini.
4. Sahabat dan teman-teman, yang selalu memberikan semangat dan ide-ide yang konstruktif.

5. Segenap Dosen dan Civitas Akademika Universitas AMIKOM Yogyakarta yang telah memberikan banyak ilmu dan pengalaman selama menjalani perkuliahan.
6. Peran dari pihak - pihak lain yang tidak dapat disebutkan satu persatu yang juga turut andil membantu sehingga tesis ini dapat selesai.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna, dan oleh karena itu, saran dan kritik yang membangun di harapkan guna penyempurnaan penelitian ini di masa depan. Penulis berharap hasil penelitian ini dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan di bidang Informatika terkhusus dalam pembahasan manajemen risiko TI. Akhir kata, semoga penelitian tesis ini dapat memberikan manfaat dan menjadi referensi yang berguna bagi praktisi TI serta akademisi dalam upayanya meneliti tema yang sama.

Yogyakarta, 10 November 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Analisis pengelolaan risiko Teknologi Informasi (TI) di Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM). Penelitian ini berjudul "Analisis Audit Manajemen Risiko untuk Mengelola Risiko IT dengan Menggunakan *Framework* COBIT 2019" yang berfokus pada pengelolaan risiko teknologi informasi di Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM). Dilakukan dengan menggunakan framework COBIT 2019, khususnya pada domain EDM 03 *(Ensure Risk Optimization)*, APO 12 *(Manage Risk)*, dan APO 13 *(Manage Security)*. Mengingat pentingnya TI dalam mendukung operasional dan pengelolaan dana Zakat, Infak, Sedekah, dan Wakaf (ZISWAF), tujuan utama adalah menilai efektivitas manajemen risiko TI yang diterapkan. Metode yang digunakan adalah pendekatan deskriptif kualitatif melalui studi kasus, dengan pengumpulan data melalui observasi, wawancara, dan kuesioner kepada responden yang terlibat dalam pengelolaan TI.

Hasil penelitian menunjukkan bahwa Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM) telah mencapai tingkat kapabilitas yang memadai pada domain EDM 03 *(Ensure Risk Optimization)*, APO 12 *(Manage Risk)*, dan APO 13 *(Manage Security)*, dengan rata-rata level 3. Terdapat kesenjangan pada domain APO 13, yang memerlukan peningkatan untuk mencapai level 4. Rekomendasi perbaikan meliputi bagian *Governance & Leadership*, *Risk Management Framework*, *Information Security*, *Control Process*, *Technology & Integration*, dan *People & Culture*.

Kesimpulan penelitian ini adalah bahwa penerapan COBIT 2019 dapat membantu Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM) meningkatkan proses pengelolaan risiko TI dan keamanan sistem informasi, sehingga menambah kepercayaan donatur dan patuh terhadap regulasi. Penelitian ini juga membuka peluang pengembangan lebih lanjut, seperti integrasi dengan kerangka kerja lain seperti ISO 27001 atau studi komparatif dengan organisasi filantropi sejenis.

Kata kunci : audit, manajemen risiko TI, keamanan, COBIT 2019, LAZNAS BMM.

ABSTRACT

Analysis of Information Technology (IT) Risk Management at the National Zakat Amil Institution Baitulmaal Muamalat (LAZNAS BMM). This study is titled "Risk Management Audit Analysis for Managing IT Risks Using the COBIT 2019 Framework" and focuses on the management of information technology risks at the National Zakat Amil Institution Baitulmaal Muamalat (LAZNAS BMM). The research is conducted using the COBIT 2019 framework, specifically on the EDM 03 (Ensure Risk Optimization), APO 12 (Manage Risk), and APO 13 (Manage Security) domains. Considering the importance of IT in supporting operations and managing Zakat, Infak, Sedekah, and Wakaf (ZISWAF) funds, the main goal is to assess the effectiveness of the IT risk management applied. The method used is a qualitative descriptive approach through a case study, with data collection through observations, interviews, and questionnaires from respondents involved in IT management.

The research findings show that the National Zakat Amil Institution Baitulmaal Muamalat (LAZNAS BMM) has achieved a sufficient level of capability in the EDM 03 (Ensure Risk Optimization), APO 12 (Manage Risk), and APO 13 (Manage Security) domains, with an average level of 3. There is a gap in the APO 13 domain, which requires improvement to reach level 4. Improvement recommendations cover the areas of Governance & Leadership, Risk Management Framework, Information Security, Control Process, Technology & Integration, and People & Culture.

The conclusion of this study is that the implementation of COBIT 2019 can help LAZNAS BMM improve the process of managing IT risks and information system security, thereby increasing donor trust and compliance with regulations. This study also opens opportunities for further development, such as integration with other frameworks like ISO 27001 or comparative studies with similar philanthropic organizations.

Keywords: audit, IT risk management, security, COBIT 2019, LAZNAS BMM.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam era globalisasi dan digitalisasi yang semakin pesat, Teknologi Informasi (TI) memainkan peran yang sangat penting dalam mendukung operasional dan strategi bisnis organisasi di berbagai sektor. TI bukan hanya sekadar alat untuk mempercepat dan memperbaiki proses bisnis, tetapi juga menjadi katalisator utama dalam menciptakan inovasi, efisiensi, dan transformasi digital. TI memungkinkan organisasi untuk memanfaatkan data secara lebih efektif, mendukung pengambilan keputusan yang lebih cerdas, dan meningkatkan keterhubungan dengan pemangku kepentingan. Dengan memanfaatkan TI secara optimal, organisasi dapat mengintegrasikan proses bisnis mereka, menciptakan layanan yang lebih responsif, serta mempermudah interaksi dengan pelanggan atau pengguna jasa. Hal ini memberikan keunggulan kompetitif yang penting di tengah persaingan global yang semakin ketat.

Namun, adopsi TI yang semakin kompleks juga memperkenalkan berbagai tantangan, terutama dalam hal keamanan dan pengelolaan risiko. Dalam konteks organisasi modern, risiko TI mencakup berbagai ancaman seperti serangan siber, kegagalan sistem, kesalahan manusia, dan ketidakpatuhan terhadap regulasi yang berlaku. Risiko-risiko ini berpotensi mengakibatkan gangguan operasional, kerugian finansial, serta kerusakan reputasi yang dapat berdampak jangka panjang pada keberlangsungan organisasi. Oleh karena itu, pengelolaan risiko TI menjadi

sangat penting untuk memastikan bahwa teknologi yang digunakan dapat mendukung tujuan strategis organisasi tanpa menimbulkan risiko yang signifikan.

Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM) adalah salah satu contoh organisasi filantropi di Indonesia yang sangat bergantung pada TI dalam menjalankan misinya. Mulanya didirikan sebagai entitas sosial didalam organisasi korporasi (Bank Muamalat), namun seiring berjalannya waktu dan tuntutan untuk terus tumbuh, akhirnya berkembang menjadi organisasi yang terpisah serta memiliki struktur sendiri dari pusat hingga daerah. Sebagai lembaga yang berfokus pada pengumpulan dan distribusi Zakat, Infak, Sedekah, dan Wakaf (ZISWAF), BMM mengelola data yang sangat sensitif terkait donatur, penerima manfaat, dan sukarelawan. Kepercayaan donatur bergantung pada transparansi dan keandalan BMM dalam mengelola data dan melaporkan distribusi dana. Namun, risiko terhadap keamanan data dapat merusak kepercayaan ini dan mengancam kelangsungan operasional BMM. Di sinilah audit manajemen risiko TI menjadi esensial, memastikan bahwa BMM memiliki kontrol yang kuat untuk melindungi data dan menjaga kepatuhan terhadap regulasi terkait.

Dalam memahami posisi strategis BMM di industri pengelolaan zakat, analisis *Porter's Five Forces* digunakan untuk mengevaluasi dinamika persaingan yang dihadapi. Pertama *(Threat of New Entrants)*, Ancaman dari Pendatang Baru Baru cukup tinggi, karena semakin mudahnya mendirikan organisasi sosial berbasis teknologi dengan modal rendah. Ini berarti bahwa BMM perlu terus memperkuat posisinya sebagai lembaga yang sudah mapan agar tidak tergerus oleh pemain baru. Kedua *(Supplier Bargaining Power)*, Kekuatan Tawar-menawar Pemasok dalam

konteks ini mencakup sumber daya manusia (SDM) yang terampil di bidang pengelolaan zakat dan TI. Keterbatasan SDM yang ahli memberikan daya tawar yang tinggi bagi tenaga kerja tersebut, yang dapat menjadi tantangan dalam pengelolaan risiko TI. Ketiga *(Customer Bargaining Power)*, Kekuatan Tawar-menawar Pembeli (donatur) cukup tinggi, mengingat mereka memiliki banyak pilihan lembaga zakat lain. BMM harus mampu mempertahankan kepercayaan donatur melalui transparansi yang baik dalam pelaporan dan keamanan data yang terjamin. Keempat *(Threat of Substitutes)*, Ancaman dari Produk Pengganti juga signifikan, terutama dengan adanya alternatif donasi melalui platform crowdfunding dan lembaga amal internasional yang dapat mengalihkan potensi donasi dari BMM. Kelima *(Rivalry Among Existing Competitors)*, Persaingan Antar Pesaing yang Ada sangat ketat di antara lembaga zakat di Indonesia, yang memaksa BMM untuk berinovasi dalam strategi pengelolaan dan distribusi dana agar tetap kompetitif.

Di samping analisis Porter, analisis SWOT juga memberikan pandangan yang lebih rinci mengenai kekuatan, kelemahan, peluang, dan ancaman yang dihadapi BMM. BMM memiliki kekuatan dalam hal reputasi sebagai lembaga amil zakat nasional yang terpercaya karena lahir dari korporasi yang bergerak di bidang perbankan yaitu Bank Muamalat yang merupakan salah satu pelopor bank syariah di Indonesia, ini merupakan modal penting bagi BMM untuk terus mempertahankan dan meningkatkan kepercayaan donatur. Selain itu kepercayaan donatur terhadap lembaga ini juga bergantung pada transparansi dan keandalan BMM dalam mengelola data serta melaporkan distribusi dana secara akurat, pengelolaan data

serta distribusi dana yang sensitif tersebut perlu dibersamai dengan infrastruktur TI yang tidak hanya kuat, tetapi juga aman dan andal. Namun, BMM juga memiliki kelemahan pada aspek integrasi dan keamanan sistem TI. Infrastruktur yang ada terkadang belum sepenuhnya terintegrasi secara holistik, sehingga menciptakan celah dalam sistem keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Celah-celah ini dapat menyebabkan kebocoran data atau gangguan operasional yang dapat merusak kepercayaan para donatur. Selain itu, sistem keamanan yang ada memerlukan pemantauan yang lebih ketat untuk mengantisipasi ancaman siber yang semakin kompleks. Kekurangan dalam integrasi dan pemantauan ini menunjukkan bahwa BMM memerlukan pendekatan yang lebih sistematis dalam mengelola risiko TI, agar dapat memastikan perlindungan data donatur dan operasional berjalan dengan lancar. Di sisi lain, ada peluang besar yang dapat dimanfaatkan oleh BMM, seperti meningkatnya kesadaran masyarakat tentang pentingnya keamanan data dan kebutuhan untuk transparansi dalam pengelolaan donasi. Hal ini membuka peluang bagi BMM untuk membedakan diri dari kompetitor melalui peningkatan standar manajemen risiko TI. Selain itu, perkembangan teknologi juga menawarkan kesempatan untuk mengadopsi solusi yang lebih canggih dalam pengelolaan data dan keamanan TI. Namun, BMM juga harus menghadapi beberapa ancaman, termasuk meningkatnya risiko serangan siber dan persaingan yang semakin ketat dari platform donasi digital lainnya. Ancaman-ancaman ini dapat mengurangi kepercayaan donatur jika tidak ditangani dengan baik.

Untuk menghadapi kelemahan dan memanfaatkan peluang tersebut, BMM dapat menggunakan framework COBIT 2019 dalam mengadaptasi pendekaatan TI & melakukan audit manajemen risiko TI. COBIT 2019 adalah versi terbaru dari kerangka kerja yang dikembangkan oleh ISACA, yang menawarkan pendekatan komprehensif untuk tata kelola TI. Framework ini memastikan bahwa pendekatan TI & manajemen risiko TI menjadi bagian integral dari keseluruhan tata kelola TI, tidak hanya sebagai proses terpisah. Dari sekian domain yang dimiliki, COBIT 2019 memiliki sejumlah domain dan proses yang bisa diadopsi untuk menilai kapabilitas manajemen risiko TI, khususnya pada domain APO12 (*Manage Risk*) dan MEA01 (*Monitor, Evaluate, and Assess Performance and Conformance*). APO12 berfokus pada pengelolaan risiko TI secara komprehensif, yang meliputi identifikasi, evaluasi, dan mitigasi risiko yang bisa berdampak pada operasional organisasi. Sementara itu, MEA01 bertujuan untuk memantau dan mengevaluasi kinerja sistem TI serta kepatuhan terhadap standar yang berlaku. Kedua domain ini bisa diadopsi oleh LAZNAS BMM untuk memastikan manajemen risiko TI yang proaktif dan berkelanjutan. Bila dibandingkan dengan versi sebelum - sebelumnya, COBIT 2019 juga lebih fleksibel dan dapat diintegrasikan dengan kerangka kerja lain, seperti ISO 31000 (Manajemen Risiko) dan ISO 27001 (Manajemen Keamanan Informasi). Dengan menggunakan COBIT 2019, BMM dapat menilai efektivitas kapabilitas mereka dalam mengelola risiko TI dan mengidentifikasi area yang memerlukan perbaikan. Proses audit menggunakan COBIT 2019 memungkinkan BMM untuk tidak hanya mengidentifikasi risiko, tetapi juga mengoptimalkan kontrol yang ada dan memastikan bahwa proses-proses TI

mendukung tujuan strategis organisasi. Framework ini memberikan panduan yang jelas untuk mengukur kapabilitas proses dan mengembangkan kebijakan pengelolaan risiko yang lebih baik. Hal ini akan membantu BMM meningkatkan transparansi dan akuntabilitas, yang pada gilirannya dapat memperkuat kepercayaan donatur dan mitra. Selain itu, dengan pendekatan TI berbasis standar, BMM dapat memastikan bahwa manajemen risiko TI mereka selalu selaras dengan praktik terbaik internasional dan adaptif terhadap perubahan regulasi.

Dari analisis *Porter's Five Force* & SWOT yang telah dilakukan sebelumnya, terlihat bahwa aspek TI memainkan peran yang krusial dalam kesuksesan Baitulmaal Muamalat, namun juga menjadi sumber tantangan dan risiko yang perlu dikelola dengan baik. Implementasi COBIT 2019 sebagai framework audit akan memberikan solusi yang efektif untuk mengatasi kelemahan yang ada tersebut dan mengoptimalkan pengelolaan risiko TI Baitulmaal Muamalat. Membantu BMM memperkuat infrastruktur TI mereka dengan pendekatan terstruktur dan sesuai standar internasional. Audit ini akan memastikan bahwa kelemahan dalam kontrol keamanan TI dapat diatasi, peluang inovasi digital dapat dimanfaatkan, dan ancaman dari risiko TI dapat diminimalisir. Dengan demikian, penggunaan COBIT 2019 memungkinkan BMM untuk mengelola risiko TI secara efektif dan selaras dengan tujuan strategis organisasi, menjaga kepercayaan donatur, mendukung kelancaran operasional organisasi dalam jangka panjang.

Pada penelitian ini terdapat beberapa penelitian yang relevan dengan bahasan tema audit manajemen risiko terhadap pengelolaan risiko TI menggunakan

framework COBIT. Didasarkan pada berbagai referensi jurnal yang kredibel agar menghasilkan rekomendasi yang tepat serta dapat bermanfaat dalam pengembangan penelitian bertema sama dimasa mendatang.

Penelitian pertama, berjudul "*Measuring the Performance of Information System Governance using Framework COBIT 2019*". Penelitian ini memfokuskan pada evaluasi kinerja tata kelola sistem informasi dengan memanfaatkan kerangka kerja COBIT 2019. Fokus utama adalah pada identifikasi proses-proses penting yang memerlukan perbaikan dan peningkatan di Dinas Perumahan dan Kawasan Permukiman Kota Salatiga, dengan mempertimbangkan kebutuhan dan tujuan strategis instansi tersebut. Selain itu, penelitian ini juga berfokus pada pemetaan domain dari faktor desain COBIT 2019 untuk memberikan rekomendasi yang spesifik dan relevan. Tujuan dari penelitian ini adalah untuk mengukur kinerja tata kelola sistem informasi di Dinas Perumahan dan Kawasan Permukiman Kota Salatiga menggunakan kerangka kerja COBIT 2019. Penelitian ini juga bertujuan untuk memberikan rekomendasi proses yang penting untuk perbaikan tata kelola TI di instansi tersebut. Penelitian kedua, berjudul *"Simplified IT Risk Management Maturity Audit System based on COBIT 5 for Risk"* berfokus pada pengembangan sistem audit kematangan manajemen risiko TI yang disederhanakan menggunakan kerangka kerja COBIT 5 untuk Risiko. Tujuan utamanya adalah untuk mengevaluasi kematangan manajemen risiko TI dalam organisasi, mengidentifikasi kesenjangan, dan menyusun rencana tindakan untuk mengimplementasikan atau memperbarui manajemen risiko TI. Penelitian ketiga berjudul *"Risk Management Analysis of Bus Transportation Application Using COBIT 4.1"*. Penelitian ini

berfokus pada analisis manajemen risiko aplikasi transportasi bus menggunakan kerangka kerja COBIT 4.1 pada domain Plan and Organize (PO), khususnya PO9 *(Assess and Manage IT risk)*. Tujuan dari penelitian ini adalah untuk menganalisis manajemen risiko pada aplikasi angkutan bus dan mengukur tingkat kematangan manajemen risiko TI menggunakan kerangka kerja COBIT 4.1 pada domain PO9.

Penelitian keempat berjudul *"Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO 12"*. Penelitian ini berfokus pada analisis manajemen risiko teknologi informasi (TI) di Perguruan Tinggi XYZ menggunakan framework COBIT 2019, khususnya domain APO 12 yang berkaitan dengan "Manage Risk." Tujuan utama penelitian ini adalah untuk mengukur dan mengevaluasi tingkat kapabilitas manajemen risiko TI di perguruan tinggi tersebut. Penelitian ini menganalisis bagaimana risiko TI diidentifikasi, dikelola, dan diantisipasi untuk memastikan tata kelola TI yang efektif, dengan harapan dapat memberikan rekomendasi yang dapat meningkatkan manajemen risiko TI di Perguruan Tinggi XYZ.

Penelitian kelima *"Enhancing Risk Management in an IT Service Company: A COBIT 2019 Framework Approach"*. Penelitian ini berfokus pada evaluasi tata kelola teknologi informasi di perusahaan layanan TI menggunakan kerangka kerja COBIT 2019. Evaluasi dilakukan untuk mengukur dan meningkatkan manajemen risiko, manajemen konfigurasi, dan manajemen kelangsungan layanan perusahaan. Tujuan penelitian ini adalah untuk meningkatkan tingkat kapabilitas tata kelola teknologi informasi di perusahaan layanan TI dengan mengidentifikasi kesenjangan dalam manajemen risiko, manajemen konfigurasi, dan manajemen kelangsungan

layanan, serta memberikan rekomendasi perbaikan berdasarkan kerangka kerja COBIT 2019. Penelitian keenam berjudul "*Capability Assessment of IT Governance Using the 2019 COBIT Framework for the IT Business Consultant Industry*". Fokus dari penelitian ini adalah menilai tata kelola teknologi informasi dan tingkat kapabilitas di PT Kwadran Lima, Indonesia, menggunakan kerangka kerja COBIT 2019. Penilaian ini dilakukan dengan mengidentifikasi domain proses yang relevan dan melakukan wawancara untuk mengumpulkan data yang diperlukan. Tujuan dari penelitian ini adalah untuk mengevaluasi tingkat keberhasilan tata kelola risiko TI dan untuk memberikan rekomendasi yang bertujuan meningkatkan efisiensi dan efektivitas sistem serta manajemen risiko di PT Kwadran Lima Indonesia sehingga perusahaan dapat mencapai target yang diinginkan. Penelitian ketujuh berjudul "*Capability Level Measurement Using COBIT 5 (Case Study: PT. Jasa Cendekia Indonesia*". Penelitian ini berfokus pada pengukuran tingkat kapabilitas manajemen operasional teknologi informasi (TI) di PT. Jasa Cendekia Indonesia menggunakan kerangka kerja COBIT 5 dengan domain DSS01 (Manage Operations). Tujuan dari penelitian ini adalah untuk mengidentifikasi kondisi manajemen operasional TI di PT. Jasa Cendekia Indonesia dan mengukur tingkat kapabilitasnya sebagai bahan evaluasi untuk memberikan rekomendasi yang mendukung optimalisasi kinerja TI perusahaan. Penelitian kedelaapan berjudul *"Analisis Efisiensi dan Efektivitas Pengelolaan Dana ZIS pada Laznas Baitulmaal Muamalat"*. Penelitian ini berfokus pada analisis efisiensi dan efektivitas pengelolaan dana Zakat, Infak, dan Sedekah (ZIS) di Laznas Baitulmaal Muamalat, yang merupakan Lembaga Amil Zakat Nasional. Analisis ini

dilakukan dengan menggunakan *Data Envelopment Analysis (DEA)* untuk mengukur efisiensi dan *Allocation to Collection Ratio (ACR)* untuk mengukur efektivitas. Tujuan dari penelitian ini adalah untuk menganalisis efisiensi dan efektivitas pengelolaan dana Zakat, Infak, dan Sedekah (ZIS) di Laznas Baitulmaal Muamalat selama periode 2016-2021. Penelitian ini menggunakan pendekatan kuantitatif dengan metode *Data Envelopment Analysis (DEA)* untuk mengukur efisiensi, dan *Allocation to Collection Ratio (ACR)* untuk mengukur efektivitas. Dengan menganalisis kedua aspek ini, diharapkan dapat memberikan gambaran yang jelas mengenai bagaimana Laznas Baitulmaal Muamalat mengelola dana ZIS-nya dan mengidentifikasi area-area yang memerlukan perbaikan untuk meningkatkan efisiensi dan efektivitas pengelolaan dana tersebut.

Dengan demikian, penelitian ini menerangkan akan pentingnya audit manajemen risiko pengelolaan risiko TI dalam organisasi. Setelah menjalani audit manajemen risiko yang komprehensif, Lembaga Amil Zakat Nasional Baitulmaal Muamalat dapat meningkatkan keamanan, efisiensi operasional, dan meminimalisir kesalahan-kesalahan yang disebabkan oleh manusia. Sehingga membuat *stake holder* lebih yakin bahwa informasi mereka aman dan dana yang mereka sumbangkan dikelola dengan baik. Selain itu, organisasi dapat menghindari potensi denda dan kerugian finansial akibat ketidakpatuhan terhadap regulasi. Dengan demikian, audit manajemen risiko tidak hanya membantu dalam mengidentifikasi dan mengelola risiko, tetapi juga berkontribusi terhadap peningkatan kepercayaan dan transparansi, yang sangat penting bagi keberhasilan dan keberlanjutan organisasi filantropi. Kemudian aspek kebaruan di penelitian ini terletak pada

adaptasi dan penerapan framework COBIT 2019 di sektor filantropi, yaitu Lembaga Amil Zakat. Pada umumnya, COBIT 2019 sering digunakan pada organisasi yang bergerak di sektor komersial atau pemerintahan. Namun, penelitian ini mengimplementasikan framework tersebut dalam konteks pengelolaan risiko di LAZNAS BMM. Pendekatan ini memberikan kontribusi pengetahuan baru tentang bagaimana manajemen risiko TI dapat diterapkan di sektor filantropi, serta menyajikan rekomendasi yang lebih relevan bagi organisasi nirlaba yang memiliki kebutuhan manajemen risiko yang unik.

Penelitian ini juga secara jelas berada dalam ranah informatika, bagian utama yang menempatkan penelitian ini dalam ranah informatika terletak pada fokus audit dan rekomendasi yang akan dilakukan terhadap aspek-aspek yang berkaitan langsung dengan penggunaan dan pengelolaan Teknologi Informasi di dalam organisasi. Audit dalam penelitian ini tidak menilai proses operasional umum, tetapi diarahkan untuk mengkaji bagaimana risiko yang terkait dengan penggunaan TI diidentifikasi, dikendalikan dan diantisipasi, serta bagaimana mekanisme pengelolaan dan keamanan TI dipersiapkan agar organisasi terhindar dari ancaman - ancaman TI yang mengintai. Dengan fokus tersebut, rekomendasi yang akan disusun juga bertujuan untuk memperbaiki dan meningkatkan pengelolaan serta pengamanan TI pada organisasi. Oleh karena itu, baik audit maupun rekomendasi yang dirumuskan dalam penelitian ini berada dalam ranah TI secara umum, sehingga menempatkan penelitian ini sebagai bagian dari bidang informatika. Selain itu penting juga untuk mengetahui perbedaan antara penelitian di bidang informatika dan non informatika yang mana dapat dilihat dari pendekatan

audit dan rekomendasinya. Dalam ranah informatika, audit diarahkan pada penilaian terhadap bagaimana Teknologi Informasi dikelola dan dimanfaatkan, sehingga ruang lingkup audit berfokus pada proses, kebijakan dan mekanisme yang berkaitan dengan TI. Rekomendasi yang dihasilkan pun ditujukan untuk memperbaiki dan menigkatkan pengelolaan TI agar penggunaan Teknologi Informasi dapat lebih mendukung tujuan organisasi. Sedangkan audit pada bidang non informatika lebih diarahkan pada penilaian terhadap proses bisnis, operasional dan administrasi organisasi. Rekomendasinya berfokus pada peningkatan terhadap kepatuhan regulasi dan operasional manajemen secara umum, bukan pada pengelolaan TI. Dengan demikian, penelitian dalam bidang informatika memiliki perbedaan yang jelas dengan penelitian non informatika.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, peneliti merumuskan beberapa rumusan masalah diantaranya sebagai berikut :

a. Bagaimana hasil audit manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM) menggunakan framework COBIT 2019 pada domain EDM03, APO12, dan APO13?
b. Berapa *capability level* pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat berdasarkan hasil audit menggunakan COBIT 2019, dan gap apa saja yang muncul antara kondisi saat ini dengan target yang ditetapkan?

c. Apa rekomendasi yang dapat diberikan untuk meningkatkan kapabilitas dan memperkuat pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat berdasarkan temuan hasil audit?

1.3. Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut :

a. Penelitian ini hanya diberlakukan pada Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM).
b. Pengumpulan data penelitian diperoleh dari *stakeholder* yang terlibat di pengelolaan teknologi informasi Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM).
c. Penelitian ini hanya menggunakan COBIT 2019 sebagai framework audit dengan domain yang ditentukan dari hasil penggunaan *Design Factor*.
d. Temuan dan rekomendasi yang ada merupakan hasil dari audit manajemen risiko terhadap pengelolaan risiko teknologi informasi Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM).

1.4. Tujuan Penelitian

Berdasarkan uraian penelitian di atas, penelitian ini memiliki tujuan sebagai berikut:

a. Melakukan audit manajemen risiko TI pada Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM).

b. Mengadaptasi pendekatan TI di dalam COBIT 2019 untuk memperkuat manejeman risiko.
c. Menghasilkan rekomendasi untuk mengoptimalkan pengelolaan teknologi informasi dan meminimalisir ancaman risiko berdasar temuan yang diperoleh.
d. Menyelesaikan studi program Pascasarjana Pembelajaran Jarak Jauh Informatika di Universitas AMIKOM Yogyakarta.

1.5. Manfaat Penelitian

Manfaat yang diharapkan diperoleh dari penelitian ini adalah sebagai berikut ini :

a. Memberikan wawasan baru mengenai pendekatan TI & audit manajemen risiko TI menggunakan COBIT 2019 di lembaga Filantropi.
b. Memberikan rekomendasi sebagai bahan kajian dalam rangka evaluasi terhadap pengelolaan risiko TI dan adopsi teknologi informasi untuk memeperkuat manjemen risiko TI di Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM)
c. Menjadi rujukan bagi penelitian informatika yang berfokus pada audit manajemen risiko TI.

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Penelitian ini akan berfokus pada upaya untuk mengetahui, menjabarkan, menilai, dan menyusun rekomendasi teknis terkait manajemen risiko di Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM). Tujuannya adalah untuk mengoptimasi pengelolaan risiko teknologi informasi dengan temuan yang ada. Diharapkan penilaian dan rekomendasi teknis yang dihasilkan dapat mengatasi risiko yang ada serta risiko yang mungkin muncul di masa depan.

Penelitian pertama, berjudul "*Measuring the Performance of Information System Governance using Framework COBIT 2019*". Penelitian ini memfokuskan pada evaluasi kinerja tata kelola sistem informasi dengan memanfaatkan kerangka kerja COBIT 2019. Fokus utama adalah pada identifikasi proses-proses penting yang memerlukan perbaikan dan peningkatan di Dinas Perumahan dan Kawasan Permukiman Kota Salatiga, dengan mempertimbangkan kebutuhan dan tujuan strategis instansi tersebut. Selain itu, penelitian ini juga berfokus pada pemetaan domain dari faktor desain COBIT 2019 untuk memberikan rekomendasi yang spesifik dan relevan. Tujuan dari penelitian ini adalah untuk mengukur kinerja tata kelola sistem informasi di Dinas Perumahan dan Kawasan Permukiman Kota Salatiga menggunakan kerangka kerja COBIT 2019. Penelitian ini juga bertujuan untuk memberikan rekomendasi proses yang penting untuk perbaikan tata kelola TI di instansi tersebut.

Penelitian kedua, berjudul *"Simplified IT Risk Management Maturity Audit System based on COBIT 5 for Risk"* berfokus pada pengembangan sistem audit kematangan manajemen risiko TI yang disederhanakan menggunakan kerangka kerja COBIT 5 untuk Risiko. Tujuan utamanya adalah untuk mengevaluasi kematangan manajemen risiko TI dalam organisasi, mengidentifikasi kesenjangan, dan menyusun rencana tindakan untuk mengimplementasikan atau memperbarui manajemen risiko TI.

Penelitian ketiga berjudul *"Risk Management Analysis of Bus Transportation Application Using* COBIT 4.1". Penelitian ini berfokus pada analisis manajemen risiko aplikasi transportasi bus menggunakan kerangka kerja COBIT 4.1 pada domain *Plan and Organize (PO),* khususnya PO9 (*Assess and Manage IT risk*). Tujuan dari penelitian ini adalah untuk menganalisis manajemen risiko pada aplikasi angkutan bus dan mengukur tingkat kematangan manajemen risiko TI menggunakan kerangka kerja COBIT 4.1 pada domain PO9.

Penelitian keempat berjudul *"Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO 12"*. Penelitian ini berfokus pada analisis manajemen risiko teknologi informasi (TI) di Perguruan Tinggi XYZ menggunakan *framework* COBIT 2019, khususnya domain APO 12 yang berkaitan dengan "Manage Risk." Tujuan utama penelitian ini adalah untuk mengukur dan mengevaluasi tingkat kapabilitas manajemen risiko TI di perguruan tinggi tersebut. Penelitian ini menganalisis bagaimana risiko TI diidentifikasi, dikelola, dan diantisipasi untuk memastikan tata kelola TI yang

efektif, dengan harapan dapat memberikan rekomendasi yang dapat meningkatkan manajemen risiko TI di Perguruan Tinggi XYZ.

Penelitian kelima berjudul *"Enhancing Risk Management in an IT Service Company: A COBIT 2019 Framework Approach"*. Penelitian ini berfokus pada evaluasi tata kelola teknologi informasi di perusahaan layanan TI menggunakan kerangka kerja COBIT 2019. Evaluasi dilakukan untuk mengukur dan meningkatkan manajemen risiko, manajemen konfigurasi, dan manajemen kelangsungan layanan perusahaan. Tujuan penelitian ini adalah untuk meningkatkan tingkat kapabilitas tata kelola teknologi informasi di perusahaan layanan TI dengan mengidentifikasi kesenjangan dalam manajemen risiko, manajemen konfigurasi, dan manajemen kelangsungan layanan, serta memberikan rekomendasi perbaikan berdasarkan kerangka kerja COBIT 2019.

Penelitian keenam berjudul *"Capability Assessment of IT Governance Using the 2019 COBIT Framework for the IT Business Consultant Industry"*. Fokus dari penelitian ini adalah menilai tata kelola teknologi informasi dan tingkat kapabilitas di PT Kwadran Lima, Indonesia, menggunakan kerangka kerja COBIT 2019. Penilaian ini dilakukan dengan mengidentifikasi domain proses yang relevan dan melakukan wawancara untuk mengumpulkan data yang diperlukan. Tujuan dari penelitian ini adalah untuk mengevaluasi tingkat keberhasilan tata kelola risiko TI dan untuk memberikan rekomendasi yang bertujuan meningkatkan efisiensi dan efektivitas sistem serta manajemen risiko di PT Kwadran Lima Indonesia sehingga perusahaan dapat mencapai target yang diinginkan.

Penelitian ketujuh berjudul "*Capability Level Measurement Using COBIT 5 (Case Study: PT. Jasa Cendekia Indonesia"*. Penelitian ini berfokus pada pengukuran tingkat kapabilitas manajemen operasional teknologi informasi (TI) di PT. Jasa Cendekia Indonesia menggunakan kerangka kerja COBIT 5 dengan domain DSS01 (Manage Operations). Tujuan dari penelitian ini adalah untuk mengidentifikasi kondisi manajemen operasional TI di PT. Jasa Cendekia Indonesia dan mengukur tingkat kapabilitasnya sebagai bahan evaluasi untuk memberikan rekomendasi yang mendukung optimalisasi kinerja TI perusahaan.

Penelitian kedelapan berjudul *"Analisis Efisiensi dan Efektivitas Pengelolaan Dana ZIS pada Laznas Baitulmaal Muamalat"*. Penelitian ini berfokus pada analisis efisiensi dan efektivitas pengelolaan dana Zakat, Infak, dan Sedekah (ZIS) di Laznas Baitulmaal Muamalat, yang merupakan Lembaga Amil Zakat Nasional. Analisis ini dilakukan dengan menggunakan *Data Envelopment Analysis (DEA)* untuk mengukur efisiensi dan Allocation to Collection Ratio (ACR) untuk mengukur efektivitas. Tujuan dari penelitian ini adalah untuk menganalisis efisiensi dan efektivitas pengelolaan dana Zakat, Infak, dan Sedekah (ZIS) di Laznas Baitulmaal Muamalat selama periode 2016-2021. Penelitian ini menggunakan pendekatan kuantitatif dengan metode *Data Envelopment Analysis (DEA)* untuk mengukur efisiensi, dan *Allocation to Collection Ratio (ACR)* untuk mengukur efektivitas. Dengan menganalisis kedua aspek ini, diharapkan dapat memberikan gambaran yang jelas mengenai bagaimana Laznas Baitulmaal Muamalat mengelola dana ZIS-nya dan mengidentifikasi area-area yang

memerlukan perbaikan untuk meningkatkan efisiensi dan efektivitas pengelolaan dana tersebut.

2.2. Keaslian Penelitian

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian

Analisis Audit Manajemen Risiko Untuk Mengelola Risiko IT Dengan Menggunakan Framework COBIT 2019

(Studi Kasus : Lembaga Amil Zakat Nasional Baitulmaal Muamalat)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Kelemahan & Saran	Perbandingan
1	Measuring the Performance of Information System Governance using Framework COBIT 2019	• Peneliti: Adila Safitri, Imam Syafii, Kusworo Adi • Media Publikasi: International Journal of Computer Applications • Tahun: April 2021	Tujuan dari penelitian ini adalah untuk mengukur kinerja tata kelola sistem informasi di Dinas Perumahan dan Kawasan Permukiman menggunakan kerangka kerja COBIT 2019. Penelitian ini juga bertujuan untuk memberikan rekomendasi proses yang penting untuk perbaikan tata kelola TI di instansi tersebut.	Kesimpulan dari penelitian ini adalah desain tata kelola teknologi informasi perusahaan dan rekomendasi proses penting bagi Dinas Perumahan dan Kawasan Permukiman Kota. Proses-proses yang direkomendasikan meliputi APO 09 (Manage Service Agreements), APO 12 (Managed Risk), APO 13 (Managed Security), DSS02 (Manage Service Requests and Incidents), dan DSS03 (Managed Problems). Penelitian ini menyarankan bahwa desain tata kelola TI yang dihasilkan mampu meningkatkan kinerja dan mitigasi risiko yang lebih baik.	• Kelemahan : Penelitian ini hanya sampai pada tahap pemberian rekomendasi berdasarkan pemetaan domain dari faktor desain COBIT 2019 dan belum dilakukan evaluasi proses kapabilitas secara mendalam. • Saran : Penelitian lanjutan disarankan untuk melakukan evaluasi lebih mendalam terhadap proses kapabilitas pada kerangka kerja COBIT 2019, sehingga dapat memberikan gambaran yang lebih komprehensif mengenai tingkat kapabilitas tata kelola TI di Dinas Perumahan dan Kawasan Permukiman.	Penelitian akan mengukur sejauh mana adaptasi pendekatan TI & manajemen risiko yang telah di lakukan menggunakan framework COBIT 2019 terhadap lembaga filantropi. Yang mana dalam penelitian review dilakukan pada lembaga pemerintahan.

2.	Simplified IT Risk Management Maturity Audit System based on "COBIT 5 for Risk"	• Peneliti: Hasnaa Berrada, Jaouad Boutahar, Souhail El Ghazi El Houssaïni • Media Publikasi: International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 12, No. 8 • Tahun: 2021	Tujuan penelitian ini adalah untuk mendeskripsikan sistem audit kematangan manajemen risiko TI yang disederhanakan dalam suatu organisasi berdasarkan "COBIT 5 for Risk". Sistem ini bertujuan untuk mengevaluasi kematangan manajemen risiko TI, mengidentifikasi kesenjangan, dan menentukan rencana aksi yang diperlukan untuk mengimplementasikan atau memperbarui manajemen risiko TI dalam organisasi.	Penelitian ini menyimpulkan bahwa sistem audit kematangan manajemen risiko TI yang disederhanakan lalu diusulkan dapat digunakan untuk mengevaluasi tingkat kematangan manajemen risiko TI dalam suatu organisasi. Sistem ini dibangun berdasarkan praktik terbaik dari "COBIT 5 for Risk" dan mencakup tujuh enabler COBIT 5 yang dibagi menjadi tujuh makro-fase. Laporan akhir dari audit ini adalah laporan kematangan dalam hal manajemen risiko TI yang mencakup tujuh enabler yang ditentukan oleh COBIT 5.	• Kelemahan : Penelitian ini hanya mencakup fase pertama dari pengembangan sistem manajemen risiko TI yang disederhanakan. Implementasi penuh dan pengujian sistem belum dilakukan dalam penelitian ini. • Saran : Penelitian lebih lanjut diperlukan untuk merancang sistem dan mengembangkan solusi TI yang akan mendukung pelaksanaan langkah-langkah audit. Selain itu, penelitian lebih lanjut dapat mencakup uji coba sistem dalam berbagai jenis organisasi untuk mengevaluasi keefektifan dan efisiensi sistem yang diusulkan.	Penelitian akan menggunakan framework COBIT 2019 untuk melihat penerapan TI & menganalisa manajemen risiko. (Update framework dari yang sebelumnya didasarakan dari COBIT 5 ke COBIT 2019)
3.	Risk Management Analysis of Bus Transportation Application Using COBIT 4.1	• Peneliti: Resad Setyadi dan Handy Nur Prabowo • Media Publikasi: JURTEKSI (Jurnal Teknologi dan Sistem Informasi) • Tahun: April 2021	Tujuan dari penelitian ini adalah untuk menganalisis manajemen risiko pada aplikasi angkutan bus dan mengukur tingkat kematangan manajemen risiko TI menggunakan kerangka kerja COBIT 4.1 pada domain PO9.	Kesimpulan penelitian menunjukkan bahwa tingkat kematangan manajemen risiko aplikasi angkutan bus berada pada level 2 (Repeatable but Intuitive). Ini berarti perusahaan menyadari bahwa ada masalah yang perlu diselesaikan, namun pendekatan manajemen risiko masih bersifat individu dan belum pada tahap penyelesaian terintegrasi. Secara keseluruhan, manajemen aplikasi	• Kelemahan : Penelitian menunjukkan bahwa manajemen risiko TI masih berada pada tahap prosedural dan belum ada pelatihan khusus mengenai risiko TI untuk semua anggota dalam setiap unit proses. • Saran : Disarankan untuk mulai menerapkan pelatihan	Penelitian akan menganalisa manajemen risiko TI secara mendalam menggunakan framework COBIT 2019 pada lembaga filantropi yang sebelumnya COBIT 4.1, pada aplikasi bus.

				memerlukan peningkatan dalam manajemen teknologi informasi.	risiko TI khusus untuk semua anggota dalam setiap unit proses untuk memberikan gambaran mengenai bagaimana mengurangi risiko TI.	
4.	Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO 12	• Peneliti: Rifqi Anugrah, Ema Utami, Alva Hendi Muhammad • Media Publikasi: Jurnal Ilmiah Universitas Batanghari Jambi, Volume 22, Issue 2 • Tahun: 2022	Melakukan analisis manajemen risiko berdasarkan standar framework COBIT 2019 dengan fokus pada domain APO 12 untuk menghasilkan nilai dari capability level sebagai acuan untuk menganalisis manajemen risiko pada Perguruan Tinggi XYZ.	Menunjukkan bahwa teknologi informasi (TI) telah diterapkan dan dikelola sesuai dengan target yang ditentukan. Namun, nilai rata-rata capability level test sebesar 2,88 menunjukkan bahwa tata kelola TI belum maksimal dan masih memerlukan beberapa peningkatan. Analisis GAP lebih lanjut mengindikasikan bahwa belum ada domain yang mencapai nilai indeks 4, yang berarti ada kesenjangan yang perlu diatasi untuk mencapai tata kelola TI yang optimal. Secara keseluruhan, manajemen risiko TI di Perguruan Tinggi XYZ dianggap seimbang tetapi memerlukan peningkatan khususnya dalam aspek "Managed Risk" sesuai dengan domain APO 12.	• Kelemahan : Masih terdapat GAP antara nilai capability level test yang diperoleh dengan nilai yang diharapkan. Perguruan Tinggi XYZ belum mencapai nilai indeks 4, menunjukkan bahwa tata kelola TI belum sepenuhnya optimal. • Saran : Sebagai saran untuk meningkatkan manajemen risiko, Perguruan Tinggi XYZ disarankan untuk melakukan pencatatan data terkait risiko TI secara sistematis dan relevan, serta melakukan proses identifikasi risiko yang dituangkan dalam laporan akhir. Selain itu, penting untuk melakukan analisis mendalam terhadap data hasil evaluasi risiko guna menghasilkan informasi terkait risiko yang mungkin terjadi di masa depan.	Penelitian akan menganalisa manajemen risiko pada pengelolaan risiko TI di Lembaga filantropi Baitulmaal Muamalat (BMM) yang sebelumya di penelitian review di lakukan pada Lembaga Pendidikan.
5.	Enhancing Risk Management in	• Peneliti: Emmanuel Enrique, Melissa Indah Fianty	Tujuan penelitian ini adalah untuk meningkatkan tingkat kapabilitas	Penelitian menemukan bahwa perusahaan berada pada tingkat kapabilitas level 3 untuk manajemen	• Kelemahan : Penelitian ini menunjukkan beberapa kelemahan, termasuk	Penelitian akan menganalisa manajemen risiko pada

	an IT Service Company: A COBIT 2019 Framework Approach	• Media Publikasi: Jurnal Riset Informatika, Universitas Multimedia Nusantara • Tahun: September 2023	tata kelola teknologi informasi di perusahaan layanan TI dengan mengidentifikasi kesenjangan dalam manajemen risiko, manajemen konfigurasi, dan manajemen kelangsungan layanan, serta memberikan rekomendasi perbaikan berdasarkan kerangka kerja COBIT 2019.	risiko (APO 12) dan manajemen konfigurasi (BAI10), serta level 2 untuk manajemen kelangsungan (DSS 04), sementara target yang diharapkan adalah level 4 untuk APO 12 dan BAI 10, dan level 3 untuk DSS 04. Ini menunjukkan adanya kesenjangan satu level di masing-masing proses. Rekomendasi perbaikan meliputi pengelolaan risiko yang lebih baik, manajemen sumber daya TI yang lebih efisien, dan pemeliharaan sistem layanan yang berkelanjutan.	kurangnya adopsi taksonomi risiko yang komprehensif dan identifikasi risiko masa depan secara menyeluruh. Selain itu, manajemen konfigurasi dan baseline data belum terdefinisi dengan jelas. Perusahaan juga belum memiliki rencana pemulihan dan respons insiden yang spesifik dan terstruktur, serta kekurangan dokumentasi dan pelatihan untuk rencana keberlanjutan bisnis dan pemulihan bencana • Saran : Untuk mengatasi kelemahan ini, disarankan agar perusahaan membuat taksonomi risiko yang membantu dalam mengategorikan strategi manajemen risiko dan melakukan estimasi frekuensi serta dampak risiko terkait TI. Perusahaan juga perlu mengidentifikasi serta menyetujui ruang lingkup dan detail manajemen konfigurasi.	pengelolaan risiko TI di Lembaga filantropi Baitulmaal Muamalat (BMM) yang sebelumya di penelitian review di lakukan pada Perusahaan Layanan TI.
6.	Capability Assessment of IT Governance Using the 2019	• Peneliti: Maximillian Brian Hardjadinata, Jansen Wiratama • Media Publikasi: International Journal of	Tujuan dari penelitian ini adalah untuk mengevaluasi tingkat keberhasilan tata kelola risiko IT dan untuk memberikan	Berdasarkan hasil penelitian, PT Kwadran Lima Indonesia masih berada pada level 2 dalam domain APO 12-Managed Risk dan BAI 10-Managed Configuration, sementara DSS 03-	• Kelemahan : Penelitian ini menemukan bahwa meskipun PT Kwadran Lima telah melaksanakan manajemen risiko dengan baik, masih ada	Penelitian akan menganalisa manajemen risiko pada pengelolaan risiko TI di Lembaga filantropi Baitulmaal

	COBIT Framework for the IT Business Consultant Industry	Science, Technology & Management • Tahun : 2023	rekomendasi yang bertujuan meningkatkan efisiensi dan efektivitas sistem serta manajemen risiko di PT Kwadran Lima Indonesia sehingga perusahaan dapat mencapai target yang diinginkan.	Managed Problem sudah mencapai level 3. Penelitian menyarankan pembentukan tim baru dan perbaikan manajemen risiko untuk mencapai level yang lebih tinggi dalam tata kelola IT.	masalah seperti sistem pelacakan dan presensi karyawan yang belum optimal. • Saran : Penelitian merekomendasikan PT Kwadran Lima Indonesia untuk membentuk atau mendesain tim baru yang bertugas untuk merancang dan mengimplementasikan metode pengumpulan dan analisis data terkait risiko TI.	Muamalat (BMM) yang sebelumya di penelitian review di lakukan pada PT Kwadran Lima Industri.
7.	Capability Level Measurement Using COBIT 5 (Case Study: PT. Jasa Cendekia Indonesia)	• Peneliti: Abdurrahman Harits, Gilang Muhamad Noer, Aris Puji Widodo • Media Publikasi: Journal of Information Systems and Informatics • Tahun: 2021	Tujuan dari penelitian ini adalah untuk mengidentifikasi kondisi manajemen operasional TI di PT. Jasa Cendekia Indonesia dan mengukur tingkat kapabilitasnya sebagai bahan evaluasi untuk memberikan rekomendasi yang mendukung optimalisasi kinerja TI perusahaan.	Kesimpulan penelitian ini menunjukkan bahwa tingkat kapabilitas PT. Jasa Cendekia Indonesia dalam mengelola operasi TI umumnya berada pada level 2 (Managed Process). Proses yang ada telah diimplementasikan secara sebagian besar, namun masih terdapat kekurangan yang harus diperbaiki untuk mencapai level 3 (Established Process).	• Kelemahan : Beberapa proses belum sepenuhnya terpenuhi, seperti kurangnya implementasi jadwal kegiatan operasional, audit independen, pemantauan aset infrastruktur, dan kebijakan lingkungan. • Saran : Disarankan untuk membuat jadwal kegiatan operasional, membentuk tim audit independen, melakukan pencatatan peristiwa secara rutin, dan membuat kebijakan lingkungan untuk memastikan keamanan dan keberlanjutan operasional TI.	Menilai kapabilitas tata kelola TI menggunakan COBIT 2019 di Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM). Yang sebelumnya pada penelitian review dilakukan pada PT Jasa Cendekia Indonesia.
8	Analisis Efisiensi dan Efektivitas Pengelolaan	• Peneliti: Hamidatuzzahra Mualo, Ade Nur Rohim	Tujuan dari penelitian ini adalah untuk menganalisis efisiensi dan efektivitas pengelolaan dana Zakat, Infak, dan Sedekah (ZIS)	Penelitian ini menyimpulkan bahwa pengelolaan dana ZIS di Laznas Baitulmaal Muamalat mengalami	• Kelemahan : Pada tahun 2016 dan 2017, ketidakefisienan dalam	Penelitian akan menghasilkan analisa serta rekomendasi taktis untuk Baiutlmaal Muamalat

	Dana ZIS pada Laznas Baitulmaal Muamalat	• Media Publikasi: Islamic Economics and Business Review, Volume 2, No. 1 • Tahun: 2023	di Laznas Baitulmaal Muamalat selama periode 2016-2021. Penelitian ini menggunakan pendekatan kuantitatif dengan metode Data Envelopment Analysis (DEA) untuk mengukur efisiensi, dan Allocation to Collection Ratio (ACR) untuk mengukur efektivitas. Dengan menganalisis kedua aspek ini, diharapkan dapat memberikan gambaran yang jelas mengenai bagaimana Laznas Baitulmaal Muamalat mengelola dana ZIS-nya dan mengidentifikasi area-area yang memerlukan perbaikan untuk meningkatkan efisiensi dan efektivitas pengelolaan dana tersebut.	ketidakefisienan pada tahun 2016 dan 2017, namun menunjukkan peningkatan signifikan pada tahun 2018 hingga 2021 dengan nilai efisiensi mencapai 100%. Pada aspek efektivitas, Laznas Baitulmaal Muamalat mendapatkan predikat "Effective" untuk tahun 2016 dan 2017, sementara pada tahun 2018 hingga 2021, pengelolaan dana ZIS dinilai "Highly Effective." Hal ini menunjukkan bahwa Laznas Baitulmaal Muamalat telah berhasil meningkatkan efisiensi dan efektivitas dalam pengelolaan dana ZIS, meskipun masih ada ruang untuk perbaikan pada beberapa tahun awal penelitian.	pengelolaan dana ZIS disebabkan oleh adanya akumulasi saldo surplus dari tahun sebelumnya, yang menyebabkan total aset dan penerimaan dana ZIS melebihi target efisiensi. Selain itu, penyaluran dana ZIS belum mencapai target yang ditetapkan untuk efisiensi maksimal. • Saran : Untuk meningkatkan efisiensi, Laznas Baitulmaal Muamalat perlu lebih cepat menyalurkan dana ZIS agar tidak terjadi surplus yang berlebihan. Selain itu, perlu adanya peningkatan jumlah total penyaluran dana dan pengurangan biaya operasional amil agar mencapai efisiensi maksimal. Diperlukan juga inovasi dalam teknik penghimpunan dan penyaluran dana ZIS serta peningkatan akuntabilitas dan pelayanan zakat kepada masyarakat	berkaitan dengan manajemen risiko terhadap pengelolaan risiko TI menggunakan COBIT 2019 sebagai framework.

2.3. Landasan Teori

2.3.1. Audit Teknologi Informasi

2.3.1.1. Definisi

Audit Teknologi Informasi (TI) adalah proses evaluasi yang sistematis dan objektif terhadap infrastruktur TI, kebijakan, dan operasi organisasi. Tujuan utama dari audit TI adalah untuk memastikan bahwa sistem informasi dan teknologi yang digunakan oleh organisasi berfungsi dengan efektif, efisien, dan aman. Audit TI mencakup penilaian terhadap kontrol internal, keamanan, manajemen risiko, dan kepatuhan terhadap regulasi serta standar industri.

2.3.1.2. Proses

Proses audit teknologi informasi dimulai dengan perencanaan audit, yang melibatkan penentuan tujuan dan ruang lingkup audit serta identifikasi sumber daya yang dibutuhkan. Dalam tahap ini, rencana audit disusun dengan menetapkan jadwal, metode, dan prosedur yang akan digunakan. Selanjutnya, pelaksanaan audit dilakukan dengan mengumpulkan data melalui wawancara, observasi, dan pemeriksaan dokumen, serta menguji kontrol internal dan sistem informasi untuk memastikan efektivitasnya. Analisis risiko juga dilakukan untuk mengidentifikasi dan mengevaluasi potensi risiko dalam sistem TI.

Setelah pengumpulan data, tahap evaluasi dan analisis dimulai. Ini mencakup penilaian efektivitas kontrol yang ada, identifikasi kelemahan atau celah dalam sistem, dan pengukuran seberapa baik sistem informasi memenuhi standar keamanan dan efisiensi. Hasil dari tahap ini kemudian disusun dalam laporan audit, yang merinci temuan, analisis, dan rekomendasi perbaikan. Temuan audit

dipresentasikan kepada manajemen untuk membahas langkah-langkah perbaikan yang diperlukan.

Langkah terakhir adalah tindak lanjut, yang memastikan bahwa rekomendasi audit diterapkan dengan benar oleh organisasi. Ini mencakup pemantauan implementasi rekomendasi dan, jika perlu, melakukan audit ulang untuk memastikan perbaikan yang dilakukan efektif. Dengan demikian, proses audit TI membantu organisasi dalam meningkatkan keamanan, efisiensi, dan kepatuhan sistem informasi mereka, serta mengelola risiko secara lebih efektif.

2.3.1.3. Tata Kelola

Tata kelola audit teknologi informasi adalah kerangka kerja dan proses yang diterapkan untuk memastikan bahwa audit TI dilakukan secara efektif, efisien, dan sesuai dengan standar serta regulasi yang berlaku. Proses ini dimulai dengan perencanaan dan pengorganisasian yang menetapkan tujuan, ruang lingkup, dan metodologi audit serta mengidentifikasi sumber daya yang diperlukan. Kerangka kerja dan standar internasional seperti COBIT, ISO 27001, dan NIST diadopsi untuk memastikan audit dilakukan sesuai dengan praktik terbaik. Kebijakan dan prosedur yang jelas dan terdokumentasi dirancang untuk mengarahkan kegiatan audit.

Pelaksanaan audit melibatkan pengumpulan data melalui wawancara, observasi, dan pemeriksaan dokumen, serta pengujian kontrol internal dan sistem TI. Laporan audit yang merinci temuan, analisis, dan rekomendasi kemudian disusun dan dibahas dengan manajemen untuk memastikan bahwa rekomendasi diterapkan dengan benar. Pemantauan dan evaluasi dilakukan secara berkala untuk

memastikan perbaikan telah diterapkan dan berfungsi efektif, serta untuk memantau kepatuhan terhadap kebijakan dan prosedur.

Aspek utama dalam tata kelola audit TI termasuk independensi auditor untuk memastikan integritas hasil audit, kompetensi dan pelatihan auditor, manajemen risiko, kualitas dan pengendalian, serta transparansi dan akuntabilitas dalam proses audit. Dengan tata kelola audit TI yang efektif, organisasi dapat memastikan audit dilakukan dengan standar tertinggi, menghasilkan temuan yang dapat diandalkan, dan mendukung perbaikan berkelanjutan dalam pengelolaan TI.

2.3.1.4. Sasaran

Audit Teknologi Informasi (TI) memiliki beberapa sasaran utama yang bertujuan untuk memastikan bahwa sistem informasi dan teknologi yang digunakan oleh organisasi berfungsi secara optimal, aman, dan efisien. Pertama, audit ini bertujuan untuk mengevaluasi efektivitas kontrol internal, memastikan bahwa kontrol yang ada cukup untuk melindungi aset informasi dan mencegah serta mendeteksi pelanggaran. Kedua, audit TI menilai langkah-langkah keamanan yang diterapkan untuk melindungi data dan sistem dari ancaman internal dan eksternal. Selanjutnya, audit TI mengidentifikasi risiko potensial yang dapat mempengaruhi sistem TI dan menilai strategi mitigasi risiko yang ada. Kepatuhan terhadap regulasi dan standar industri juga menjadi fokus, memastikan bahwa organisasi mematuhi peraturan seperti GDPR dan ISO 27001.

Selain itu, audit TI menilai efisiensi dan efektivitas operasional sistem TI dalam mendukung tujuan bisnis, serta memastikan penggunaan sumber daya yang optimal. Integritas dan keandalan data juga diperiksa untuk memastikan bahwa data

yang disimpan dan diproses akurat, lengkap, dan dapat diandalkan. Pengelolaan aset TI, termasuk perangkat keras, perangkat lunak, dan infrastruktur jaringan, menjadi bagian penting dari audit untuk menilai bagaimana aset tersebut dikelola. Terakhir, audit TI menilai kesiapan organisasi dalam menghadapi gangguan operasional dan kemampuannya untuk pulih dari bencana, memastikan adanya rencana kontinuitas bisnis dan pemulihan bencana yang efektif. Dengan mencapai sasaran - sasaran ini, audit TI membantu organisasi meningkatkan tata kelola dan pengelolaan risiko TI mereka, mendukung tujuan bisnis secara efektif dan aman.

2.3.2. Risiko

2.3.2.1. Definisi

Risiko adalah kemungkinan terjadinya suatu peristiwa atau keadaan yang dapat berdampak negatif atau menghambat pencapaian tujuan organisasi. Risiko dapat berasal dari berbagai sumber, baik internal maupun eksternal, dan dapat berdampak pada berbagai aspek operasi organisasi, termasuk keuangan, operasional, strategi, dan reputasi. Risiko mengandung dua elemen utama:

a. Kemungkinan Terjadinya: Seberapa besar peluang atau probabilitas suatu risiko akan terjadi.
b. Dampak: Seberapa besar efek atau konsekuensi yang ditimbulkan oleh risiko tersebut jika terjadi.

2.3.2.2. Klasifiksi

Klasifikasi Risiko dalam organisasi dapat diklasifikasikan ke dalam beberapa kategori berdasarkan sumber, sifat, dan dampaknya. Sedangkan klasifikasi risiko menurut COBIT dikelompokkan berdasarkan dampak risiko

terhadap tiga elemen utama yaitu risiko strategis, risiko operasional, dan risiko kepatuhan.

Risiko strategis adalah risiko yang berkaitan dengan keputusan strategis dan tujuan jangka panjang organisasi, termasuk perubahan pasar, kegagalan inovasi, dan perubahan regulasi. Risiko ini dapat mengakibatkan organisasi gagal mencapai tujuan strategisnya atau kehilangan pangsa pasar. Risiko operasional mencakup risiko yang terkait dengan operasi sehari-hari organisasi, seperti gangguan sistem TI, kesalahan manusia, dan kegagalan proses internal. Gangguan ini dapat menghambat efisiensi operasional dan kualitas layanan yang diberikan. Selanjutnya risiko kepatuhan yang mencakup potensi kegagalan organisasi dalam mematuhi undang-undang, regulasi, atau standar industri yang berlaku. Dalam konteks COBIT, risiko ini dapat terjadi jika sistem informasi dan proses bisnis tidak mematuhi peraturan terkait keamanan, privasi, atau tata kelola data.

2.3.2.3. Manajemen

Manajemen risiko adalah proses sistematis yang digunakan untuk mengidentifikasi, mengevaluasi, dan mengendalikan risiko yang dapat mempengaruhi pencapaian tujuan organisasi. Proses ini terdiri dari beberapa langkah penting :

a. Identifikasi Risiko

Menemukan dan mengenali risiko yang dapat berdampak pada organisasi. Risiko ini dapat berasal dari berbagai sumber, termasuk keuangan, operasional, strategis, dan eksternal.

b. Penilaian Risiko

Menilai kemungkinan terjadinya risiko dan dampaknya terhadap organisasi. Penilaian ini membantu dalam mengukur tingkat keparahan risiko dan menentukan prioritas penanganan.

c. Mitigasi Risiko

Mengembangkan dan menerapkan strategi untuk mengurangi kemungkinan atau dampak dari risiko. Strategi mitigasi dapat mencakup tindakan pencegahan, transfer risiko, atau penerimaan risiko dengan perencanaan kontingensi.

d. Pemantauan dan Pengendalian Risiko

Melakukan pemantauan berkelanjutan terhadap risiko dan efektivitas strategi mitigasi yang diterapkan. Pemantauan ini mencakup pengukuran kinerja dan penyesuaian strategi jika diperlukan berdasarkan perubahan dalam lingkungan risiko.

e. Pelaporan dan Komunikasi Risiko

Menyusun laporan berkala tentang status risiko dan tindakan mitigasi, serta menyampaikan informasi ini kepada pemangku kepentingan. Komunikasi yang efektif memastikan bahwa semua pihak terkait memiliki pemahaman yang sama tentang risiko yang dihadapi dan langkah-langkah yang diambil untuk mengelolanya.

Manajemen risiko yang efektif membantu organisasi untuk mengantisipasi dan mengatasi tantangan yang dapat menghambat pencapaian tujuan strategis. Dengan menerapkan manajemen risiko, organisasi dapat meningkatkan ketahanan, efisiensi operasional, dan kepercayaan pemangku kepentingan, serta memastikan keberlanjutan dan pertumbuhan jangka panjang.

2.3.3. *Control Objectives for Information and Related Technologies*

2.3.3.1. Definisi

COBIT (*Control Objectives for Information and Related Technologies*) adalah kerangka kerja yang dikembangkan oleh ISACA *(Information Systems Audit and Control Association)* untuk membantu organisasi dalam tata kelola dan manajemen teknologi informasi (TI). COBIT menyediakan panduan yang komprehensif untuk memastikan bahwa sistem TI mendukung tujuan bisnis organisasi secara efektif dan efisien. Kerangka kerja ini mencakup prinsip-prinsip, tujuan pengendalian, model referensi proses, dan alat untuk mengukur kinerja dan kepatuhan. Elemen Utama COBIT sebagai berikut :

a. Tata Kelola dan Manajemen TI

Membedakan antara tata kelola (evaluasi, pengarahan, pemantauan) dan manajemen (perencanaan, pembangunan, pelaksanaan, pemantauan).

b. Prinsip-prinsip COBIT

Memenuhi kebutuhan pemangku kepentingan, mengatasi keseluruhan perusahaan, menerapkan kerangka terpadu, memungkinkan pendekatan holistik, memisahkan tata kelola dari manajemen.

c. Tujuan Pengendalian

Menyediakan tujuan pengendalian spesifik untuk berbagai proses TI.

d. Model Referensi Proses

Menggambarkan berbagai proses yang harus ada untuk tata kelola dan manajemen TI yang efektif.

e. Kinerja dan Kepatuhan

Alat untuk mengukur kinerja dan kepatuhan terhadap standar.

2.3.3.2. COBIT 2019

COBIT 2019 adalah versi terbaru dari kerangka kerja COBIT, sebelum COBIT 2019 ada COBIT 5. Pembaruan COBIT 2019 adalah untuk mencerminkan perkembangan terbaru dalam teknologi dan praktik terbaik tata kelola TI. COBIT 2019 menekankan fleksibilitas, memungkinkan organisasi untuk menyesuaikan kerangka kerja dengan kebutuhan spesifik mereka.

COBIT5	COBIT 2019
5 prinsip tata kelola	6 prinsip tata kelola
37 proses	40 proses
Terminologi "Manage" digunakan untuk proses manajemen Terminologi "Ensure" digunakan untuk proses tata kelola	Terminologi "Managed" digunakan untuk proses manajemen Terminologi "Ensured" digunakan untuk proses tata kelola
Prinsip-prinsip kerangka tata kelola tidak tersedia	Prinsip-prinsip kerangka tata kelola ditambahkan
Pengukuran kinerja menggunakan skala 0-5 berdasarkan ISO/IEC 33000	Skema manajemen kinerja CMMI digunakan
Enablers dimasukkan	Enablers diganti namanya menjadi komponen
Faktor desain tidak tersedia	Faktor desain dimasukkan

Gambar 2.1 Perbandingan COBIT 5 dan COBIT 2019

2.3.3.2.1. Elemen Utama

a. Kerangka Kerja yang Diperbarui

COBIT 2019 mengintegrasikan prinsip - prinsip tata kelola terbaru dan memperbarui tujuan pengendalian untuk mencerminkan praktik terbaik saat ini. Kerangka kerja ini dirancang untuk membantu organisasi mencapai tujuan strategis mereka melalui penggunaan teknologi informasi yang lebih baik.

b. Prinsip-prinsip Tata Kelola COBIT 2019 didasarkan pada enam prinsip utama :

1. Memenuhi Kebutuhan Pemangku Kepentingan

Mengarahkan dan mengendalikan TI untuk menciptakan nilai bagi pemangku kepentingan.

2. Mengatasi Keseluruhan Perusahaan

Memastikan bahwa tata kelola TI mencakup seluruh organisasi.

3. Menerapkan Kerangka Terpadu

Mengintegrasikan berbagai standar dan kerangka kerja ke dalam satu model tata kelola.

4. Pendekatan Holistik

Mempertimbangkan semua aspek tata kelola TI, termasuk budaya, etika, dan perilaku.

5. Memisahkan Tata Kelola dari Manajemen

Memisahkan peran tata kelola (evaluasi, pengarahan, pemantauan) dari peran manajemen (perencanaan, pembangunan, pelaksanaan, pemantauan).

6. Pengelolaan Risiko dan Keamanan

Memastikan bahwa risiko TI dan keamanan informasi dikelola secara efektif.

c. Model Referensi Proses

COBIT 2019 mencakup model referensi proses yang menggambarkan berbagai proses yang harus ada dalam organisasi untuk tata kelola dan manajemen TI yang efektif. Model ini mencakup 40 proses yang dibagi menjadi lima domain utama :

1. *Evaluate, Direct, and Monitor (EDM)*

2. *Align, Plan, and Organize (APO)*
3. *Build, Acquire, and Implement (BAI)*
4. *Deliver, Service, and Support (DSS)*
5. *Monitor, Evaluate, and Assess (MEA)*

d. Pendekatan Holistik dan Penyesuaian

COBIT 2019 menekankan pendekatan holistik yang mempertimbangkan semua aspek tata kelola TI. Kerangka kerja ini juga memungkinkan penyesuaian berdasarkan kebutuhan spesifik organisasi, termasuk penyesuaian tingkat kapabilitas dan pencapaian tujuan.

e. Panduan Implementasi dan Alat Tambahan

COBIT 2019 menyediakan panduan yang lebih rinci dan praktis untuk implementasi, termasuk contoh - contoh nyata dan studi kasus. Versi ini juga dilengkapi dengan alat dan sumber daya tambahan untuk mendukung pengukuran kinerja, audit, dan pemantauan.

f. Kinerja dan Kepatuhan

Alat untuk mengukur kinerja dan kepatuhan terhadap standar, membantu organisasi dalam memastikan bahwa praktik TI mereka sesuai dengan regulasi dan standar industri.

2.3.3.2.2. Keuntungan

a. Meningkatkan Efektivitas dan Efisiensi TI

Dengan panduan yang komprehensif dan standar yang jelas, organisasi dapat meningkatkan efektivitas dan efisiensi penggunaan teknologi informasi.

b. Memastikan Kepatuhan

COBIT 2019 membantu organisasi memastikan kepatuhan terhadap berbagai regulasi dan standar industri, seperti GDPR, ISO 27001, dan lainnya.

c. Meningkatkan Pengelolaan Risiko

Dengan mengadopsi prinsip-prinsip tata kelola terbaru, organisasi dapat lebih baik mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan teknologi informasi.

d. Mendukung Pengambilan Keputusan yang Lebih Baik

Informasi yang lebih baik tentang kinerja dan risiko TI memungkinkan manajemen untuk membuat keputusan yang lebih informasional dan strategis.

e. Meningkatkan Transparansi dan Akuntabilitas

Dengan kebijakan dan prosedur yang jelas, serta alat pengukuran kinerja yang efektif, COBIT 2019 meningkatkan transparansi dan akuntabilitas dalam pengelolaan TI.

Dengan semua fitur dan manfaat ini, COBIT 2019 memberikan kerangka kerja yang relevan dan dapat disesuaikan dengan kebutuhan organisasi modern, memastikan bahwa TI dapat mendukung tujuan bisnis dengan lebih baik dan memberikan nilai maksimal bagi pemangku kepentingan.

2.3.3.2.3. Domain

COBIT 2019, sebagai kerangka kerja untuk tata kelola dan manajemen teknologi informasi (TI), mengelompokkan tujuan tata kelola dan manajemen ke dalam lima domain utama. Setiap domain mencakup berbagai proses yang mendukung tata kelola dan pengelolaan TI yang efektif. Berikut adalah penjelasan masing-masing domain dan proses yang termasuk di dalamnya :

a. *Evaluate, Direct, and Monitor (EDM)*

Domain ini berfokus pada tanggung jawab tata kelola yang harus dipegang oleh dewan direksi dan manajemen senior untuk memastikan bahwa TI mendukung tujuan bisnis dan memberikan nilai maksimal. Proses dalam domain EDM meliputi :

1. EDM 01 *Ensure Governance Framework Setting and Maintenance* (Memastikan Pengaturan dan Pemeliharaan Kerangka Tata Kelola)
2. EDM 02 *Ensure Benefits Delivery* (Memastikan Pencapaian Manfaat)
3. EDM 03 *Ensure Risk Optimization* (Memastikan Optimisasi Risiko)
4. EDM 04 *Ensure Resource Optimization* (Memastikan Optimisasi Sumber Daya)
5. EDM 05 *Ensure Stakeholder Transparency* (Memastikan Transparansi Pemangku Kepentingan)

b. *Align, Plan, and Organize (APO)*

Domain ini mencakup perencanaan strategis dan pengorganisasian sumber daya TI untuk memastikan keselarasan dengan tujuan bisnis. Proses dalam domain APO meliputi :

1. APO 01 *Manage the IT Management Framework* (Mengelola Kerangka Kerja Manajemen TI)
2. APO 02 *Manage Strategy* (Mengelola Strategi)
3. APO 03 *Manage Enterprise Architecture* (Mengelola Arsitektur Perusahaan)
4. APO 04 *Manage Innovation* (Mengelola Inovasi)

5. APO 05 *Manage Portfolio* (Mengelola Portofolio)
6. APO 06 *Manage Budget and Costs* (Mengelola Anggaran dan Biaya)
7. APO 07 *Manage Human Resources* (Mengelola Sumber Daya Manusia)
8. APO 08 *Manage Relationships* (Mengelola Hubungan)
9. APO 09 *Manage Service Agreements* (Mengelola Perjanjian Layanan)
10. APO 10 *Manage Suppliers* (Mengelola Pemasok)
11. APO 11 *Manage Quality* (Mengelola Kualitas)
12. APO 12 *Manage Risk* (Mengelola Risiko)
13. APO 13 *Manage Security* (Mengelola Keamanan)

c. *Build, Acquire, and Implement (BAI)*

Domain ini mencakup proses untuk membangun, mengakuisisi, dan mengimplementasikan solusi TI yang mendukung strategi bisnis dan operasional. Proses dalam domain BAI meliputi :

1. BAI 01 *Manage Programs and Projects* (Mengelola Program dan Proyek)
2. BAI 02 *Manage Requirements Definition* (Mengelola Definisi Kebutuhan)
3. BAI 03 *Manage Solutions Identification and Build* (Mengelola Identifikasi dan Pembangunan Solusi)
4. BAI 04 *Manage Availability and Capacity* (Mengelola Ketersediaan dan Kapasitas)
5. BAI 05 *Manage Organizational Change Enablement* (Mengelola Pemberdayaan Perubahan Organisasi)
6. BAI 06 *Manage Changes* (Mengelola Perubahan)

7. BAI 07 *Manage Change Acceptance and Transitioning* (Mengelola Penerimaan dan Transisi Perubahan)
8. BAI 08 *Manage Knowledge* (Mengelola Pengetahuan)
9. BAI 09 *Manage Assets* (Mengelola Aset)
10. BAI 10 *Manage Configuration* (Mengelola Konfigurasi)

d. *Deliver, Service, and Support (DSS)*

Domain ini mencakup proses yang diperlukan untuk memberikan layanan TI yang efektif dan mendukung operasi bisnis. Proses dalam domain DSS meliputi :

1. DSS 01 *Manage Operations* (Mengelola Operasi)
2. DSS 02 *Manage Service Requests and Incidents* (Mengelola Permintaan Layanan dan Insiden)
3. DSS 03 *Manage Problems* (Mengelola Masalah)
4. DSS 04 *Manage Continuity* (Mengelola Kelangsungan)
5. DSS 05 *Manage Security Services* (Mengelola Layanan Keamanan)
6. DSS 06 *Manage Business Process Controls* (Mengelola Kontrol Proses Bisnis)

e. *Monitor, Evaluate, and Assess (MEA)*

Domain ini berfokus pada pemantauan, evaluasi, dan penilaian kinerja serta kepatuhan terhadap tujuan tata kelola dan manajemen TI. Proses dalam domain MEA meliputi :

1. MEA 01 *Monitor, Evaluate, and Assess Performance and Conformance* (Memantau, Mengevaluasi, dan Menilai Kinerja dan Kepatuhan).

2. MEA 02 *Monitor, Evaluate, and Assess the System of Internal Control* (Memantau, Mengevaluasi, dan Menilai Sistem Kontrol Internal).
3. MEA 03 *Monitor, Evaluate, and Assess Compliance with External Requirements* (Memantau, Mengevaluasi, dan Menilai Kepatuhan terhadap Persyaratan Eksternal).

Gambar 2.2. Domain COBIT 2019

Kelima domain dalam COBIT 2019 mencakup seluruh spektrum aktivitas yang diperlukan untuk tata kelola dan manajemen TI yang efektif. Dengan mengadopsi dan mengimplementasikan proses-proses dalam domain ini, organisasi dapat memastikan bahwa teknologi informasi mereka dikelola dengan cara yang mendukung tujuan bisnis, mengoptimalkan penggunaan sumber daya, dan meminimalkan risiko.

2.3.3.2.4. *Implementation Guide*

a. *Where are the drivers?*

Mengidentifikasi "change drivers" dan menciptakan keinginan untuk berubah di tingkat manajemen eksekutif, yang kemudian dinyatakan dalam garis besar kasus bisnis. *"Change drivers"* adalah peristiwa, kondisi, atau masalah utama yang berfungsi sebagai stimulus untuk perubahan, seperti peristiwa, tren industri, kekurangan kinerja, perangkat lunak implementasi, dan tujuan perusahaan. Risiko terkait implementasi program dijelaskan dalam kasus bisnis dan dikelola sepanjang siklus hidupnya.

b. *Where are we now?*

Menyelaraskan tujuan TI dengan strategi dan risiko perusahaan, memprioritaskan tujuan, dan penyelarasan tata kelola serta manajemen. Panduan desain COBIT 2019 menyediakan beberapa faktor desain untuk membantu pemilihan. Berdasarkan tujuan perusahaan dan faktor desain lainnya, perusahaan harus mengidentifikasi tujuan tata kelola dan manajemen kritis serta proses dasar yang memadai. Manajemen perlu mengetahui kemampuan dan kelemahan melalui penilaian proses kemampuan dari proses yang dipilih sebelumnya.

c. *Where do we want to be?*

Menetapkan target perbaikan dan melakukan analisis kesenjangan untuk mengidentifikasi solusi potensial. Beberapa solusi akan mengatasi risiko yang ada. Prioritas diberikan pada proyek yang lebih mudah dicapai dan diselesaikan. Penyelesaian jangka panjang dipecah menjadi beberapa bagian agar dapat dikelola dengan baik.

d. *What needs to be done?*

Merencanakan solusi yang layak dan praktis dengan mendefinisikan proyek yang didukung oleh bisnis yang sesuai dengan kasus bisnis dan rencana perubahan. Kasus bisnis yang dikembangkan dengan baik membantu memastikan proyek bermanfaat dan memantau perkembangannya.

e. *How do we get there?*

Mengimplementasikan solusi yang diusulkan melalui fase - fase sebelumnya dan menetapkan langkah-langkah serta sistem pemantauan untuk memastikan keselarasan bisnis tercapai dan kinerja dapat diukur.

f. *Did we get there?*

Berfokus pada transisi berkelanjutan dari praktik tata kelola dan manajemen yang lebih baik menjadi operasi bisnis normal. Pemantauan pencapaian peningkatan dilakukan menggunakan metrik kinerja dan manfaat yang dihasilkan dari fase sebelumnya.

g. *How do we keep the momentum going?*

Meninjau keberhasilan inisiatif secara keseluruhan, mengidentifikasi kebutuhan tata kelola atau manajemen lebih lanjut, dan memperkuat kebutuhan untuk perbaikan terus-menerus. Memprioritaskan peluang lebih lanjut untuk meningkatkan tata kelola sistem.

2.3.3.2.5. *Design Factor*

COBIT 2019 memperkenalkan konsep faktor desain yang membantu organisasi menyesuaikan tata kelola TI dengan kebutuhan spesifik mereka. Faktor desain ini memungkinkan organisasi untuk menyesuaikan kerangka kerja COBIT

2019 agar lebih relevan dan efektif dalam mendukung tujuan bisnis mereka. Berikut adalah beberapa faktor desain utama dalam COBIT 2019:

a. Strategi Perusahaan

Menentukan arah dan tujuan strategis perusahaan, serta bagaimana teknologi informasi dapat mendukung pencapaian tujuan tersebut. Strategi perusahaan mempengaruhi fokus dan prioritas tata kelola TI.

b. Model Bisnis

Struktur organisasi dan cara perusahaan beroperasi. Model bisnis mencakup aspek seperti centralization versus *decentralization*, *outsourcing versus insourcing*, dan sebagainya. Ini mempengaruhi bagaimana proses TI harus dirancang dan dikelola.

c. Profil Risiko

Tingkat risiko yang dihadapi oleh perusahaan dan bagaimana risiko tersebut dikelola. Profil risiko mencakup risiko operasional, strategis, kepatuhan, dan lainnya. Memahami profil risiko membantu dalam menentukan kontrol dan proses yang diperlukan untuk mitigasi risiko.

d. Ukuran Perusahaan

Besar atau kecilnya perusahaan yang mempengaruhi kompleksitas tata kelola TI. Perusahaan besar mungkin memerlukan proses yang lebih formal dan terstruktur dibandingkan dengan perusahaan kecil.

e. Model Sumber Daya TI

Bagaimana sumber daya TI dikelola dan diatur dalam organisasi, termasuk penggunaan *outsourcing*, *shared services*, dan pengelolaan sumber daya internal. Model ini mempengaruhi struktur dan tanggung jawab tata kelola TI.

f. Strategi Pengadaan TI

Pendekatan perusahaan terhadap pengadaan teknologi informasi, seperti penggunaan vendor, solusi berbasis *cloud*, atau pengembangan internal. Strategi pengadaan mempengaruhi proses manajemen vendor dan integrasi teknologi.

g. Kepatuhan terhadap Regulasi

Tingkat kepatuhan yang diperlukan terhadap regulasi industri, standar keamanan, dan hukum. Kepatuhan ini menentukan kebutuhan untuk kontrol dan audit yang lebih ketat.

h. Adopsi Teknologi

Tingkat adopsi teknologi baru dan inovatif oleh perusahaan. Ini mencakup penerapan teknologi seperti AI, IoT, big data, dan lain-lain, yang memerlukan tata kelola khusus untuk mengelola risiko dan memaksimalkan manfaat.

i. Kebutuhan Pemangku Kepentingan

Harapan dan kebutuhan pemangku kepentingan, termasuk pelanggan, mitra bisnis, karyawan, dan regulator. Memahami kebutuhan ini membantu dalam merancang proses TI yang dapat memenuhi atau melampaui ekspektasi pemangku kepentingan.

j. Model Pengiriman Layanan

Cara layanan TI disampaikan kepada pengguna akhir, seperti penggunaan layanan internal atau eksternal, model *hybrid*, *atau managed services*. Model ini

mempengaruhi pengelolaan kontrak layanan dan hubungan dengan penyedia layanan.

Dengan mempertimbangkan faktor-faktor desain ini, organisasi dapat menyesuaikan kerangka kerja COBIT 2019 untuk memastikan bahwa tata kelola TI mereka relevan dengan kebutuhan unik mereka, serta mendukung pencapaian tujuan bisnis secara efektif dan efisien. Faktor desain ini membantu dalam membuat keputusan yang lebih tepat terkait pengelolaan dan pengendalian TI, sehingga meningkatkan kinerja dan mitigasi risiko.

2.3.3.2.6. *Capability Level Test*

COBIT 2019 menggunakan model kapabilitas proses untuk menilai tingkat kapabilitas *(capability level)* dari berbagai proses tata kelola dan manajemen TI. Model ini membantu organisasi dalam mengevaluasi sejauh mana proses mereka memenuhi standar yang ditetapkan dan seberapa efektif proses tersebut dalam mendukung tujuan bisnis. Berikut adalah tingkatan uji kapabilitas dalam COBIT 2019 :

Level 0 Tidak Lengkap *(Incomplete)*

a. Definisi

Proses pada tingkat ini tidak ada atau gagal mencapai tujuan prosesnya.

b. Karakteristik

Tidak ada bukti atau dokumentasi yang menunjukkan bahwa proses tersebut diimplementasikan.

Level 1 Dilakukan *(Performed)*

a. Definisi

Proses pada tingkat ini dilakukan, tetapi tidak ada dokumentasi atau standar yang jelas.

b. Karakteristik

Aktivitas dan tugas dilaksanakan, namun masih bergantung pada individu, dan hasilnya mungkin tidak dapat diprediksi atau berulang.

Level 2 Dikelola *(Managed)*

a. Definisi

Proses pada tingkat ini didokumentasikan dan dipantau untuk konsistensi dan kepatuhan.

b. Karakteristik

Ada perencanaan dan pelacakan, serta hasil yang lebih dapat diprediksi dibandingkan dengan level sebelumnya.

Level 3 Ditetapkan *(Established)*

a. Definisi

Proses pada tingkat ini distandarisasi dan diatur dalam kebijakan formal.

b. Karakteristik

Proses ini secara konsisten dijalankan sesuai dengan kebijakan dan prosedur yang telah ditetapkan di seluruh organisasi.

Level 4 Dapat Diprediksi *(Predictable)*

a. Definisi

Proses pada tingkat ini dipantau dan diukur secara kuantitatif.

b. Karakteristik

Ada pengukuran kinerja yang jelas, dan proses dapat diprediksi serta dikelola berdasarkan data.

Level 5 Dioptimalkan *(Optimizing)*

a. Definisi

Proses pada tingkat ini terus-menerus ditingkatkan berdasarkan umpan balik dan inovasi.

b. Karakteristik

Ada praktik terbaik yang diterapkan, dan organisasi melakukan peningkatan berkelanjutan untuk mencapai efisiensi dan efektivitas yang lebih tinggi.

Penerapan Uji Kapabilitas

1. Penilaian Awal

Lakukan penilaian awal untuk mengidentifikasi tingkat kapabilitas saat ini dari berbagai proses TI. Ini melibatkan pengumpulan data melalui wawancara, observasi, dan analisis dokumentasi.

2. Analisis Kesenjangan

Bandingkan tingkat kapabilitas saat ini dengan tingkat kapabilitas yang diinginkan. Identifikasi kesenjangan dan area yang memerlukan perbaikan.

3. Pengembangan Rencana Peningkatan

Buat rencana peningkatan untuk mengatasi kesenjangan yang teridentifikasi. Rencana ini harus mencakup langkah-langkah spesifik, sumber daya yang diperlukan, dan jadwal untuk mencapai tingkat kapabilitas yang diinginkan.

4. Implementasi Rencana Peningkatan

Terapkan rencana peningkatan dan lakukan pemantauan berkelanjutan untuk memastikan bahwa perubahan yang diimplementasikan efektif dalam meningkatkan kapabilitas proses.

5. Evaluasi Berkala

Lakukan evaluasi berkala untuk menilai kemajuan yang telah dicapai dan memastikan bahwa proses terus ditingkatkan. Ini juga melibatkan pengukuran kinerja dan penyesuaian rencana sesuai kebutuhan.

Model kapabilitas dalam COBIT 2019 memberikan kerangka kerja yang jelas dan terstruktur untuk mengevaluasi dan meningkatkan proses tata kelola dan manajemen TI. Dengan menggunakan tingkat kapabilitas ini, organisasi dapat mengidentifikasi kekuatan dan kelemahan dalam proses mereka, mengembangkan rencana peningkatan, dan memastikan bahwa proses mereka memenuhi standar yang diperlukan untuk mendukung tujuan bisnis secara efektif.

BAB III

METODE PENELITIAN

3.1. Jenis, Sifat dan Pendekatan Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif kualitatif. Penelitian deskriptif kualitatif dipilih untuk mendapatkan gambaran yang mendalam mengenai audit manajemen risiko TI dengan menggunakan *framework* COBIT 2019. Pendekatan kualitatif memungkinkan peneliti untuk mengeksplorasi, memahami, dan menggambarkan fenomena yang terjadi secara detail dan mendalam.

Sifat penelitian ini adalah eksploratif. Penelitian eksploratif bertujuan untuk menggali informasi, mengidentifikasi masalah, dan memahami fenomena yang belum banyak diteliti sebelumnya. Dalam konteks ini, penelitian akan mengeksplorasi bagaimana *framework* COBIT 2019 dapat digunakan dalam audit manajemen risiko TI untuk mengelola risiko TI secara efektif.

Pendekatan penelitian yang digunakan adalah pendekatan studi kasus. Pendekatan studi kasus memungkinkan peneliti untuk melakukan analisis mendalam terhadap satu kasus tertentu yang relevan dengan topik penelitian. Dalam penelitian ini, studi kasus akan dilakukan pada organisasi tertentu yang menerapkan *framework* COBIT 2019 dalam manajemen risiko TI nya. Data akan dikumpulkan melalui wawancara, observasi, dan analisis dokumen untuk memahami bagaimana *framework* ini diimplementasikan dan digunakan dalam praktik. Berikut langkah-langkah penelitian pemilihan kasus :

a. Memilih organisasi yang relevan untuk diaudit menggunakan *framework* COBIT 2019 terkhusus dalam hal sisi manajemen risiko TI.

b. Mengumpulkan data melalui wawancara dengan pihak-pihak yang terlibat dalam manajemen risiko TI, observasi langsung terhadap proses yang berjalan, serta analisis dokumen terkait.

c. Menganalisis data yang telah dikumpulkan untuk mengidentifikasi pola, tema, dan temuan utama terkait penggunaan *framework* COBIT 2019 dalam manajemen risiko TI.

d. Menginterpretasikan hasil analisis untuk memahami efektivitas *framework* COBIT 2019 dalam mengelola risiko TI.

e. Menyusun laporan penelitian yang mencakup deskripsi kasus, temua penelitian, dan rekomendasi untuk praktik manajemen risiko TI yang lebih baik.

Dengan metode penelitian ini, diharapkan dapat diperoleh pemahaman yang komprehensif mengenai penerapan audit manajemen risiko TI dengan *framework* COBIT 2019 dan bagaimana *framework* tersebut dapat digunakan untuk mengelola risiko TI secara efektif.

3.2. Metode Pengumpulan Data

Dalam penelitian ini metode pengumpulan data yang digunakan adalah sebagai berikut :

a. Wawancara

Wawancara mendalam dilakukan dengan pihak yang terlibat dalam bagian manajemen risiko TI pada organisasi yang menjadi objek studi kasus. Tujuan

wawancara adalah untuk mendapatkan informasi yang mendetail mengenai pengalaman, pandangan, dan praktik terbaik yang mereka terapkan dalam mengelola risiko. Wawancara dilakukan setelah responden mengisi kuesioner, guna memperdalam jawaban yang telah diberikan dalam kuesioner. Dalam proses ini, peneliti memperdalam jawaban responden dan memastikan kembali kepada responden apakah keterangan yang diberikan sudah benar. Dengan cara tersebut, data yang didapat menjadi lebih bisa dipercaya dan valid. Langkah ini sejalan dengan penelitian *Ensuring validity and reliability in qualitative research* yang menjelaskan bahwa kepercayaan pada data dapat dijaga dengan memastikan bahwa data valid serta akuratnya informasi yang diberikan. Hal ini juga didukung oleh penelitian *What Is Qualitative Research? An Overview and Guidelines* yang menekankan pentingnya keterlibatan aktif peneliti melalui wawancara dalam memahami konteks agar data yang diperoleh bisa dipahami dengan lebih tepat dan utuh. Selain itu, penelitian *Principles, Scope, and Limitations of the Methodological Triangulation* menegaskan bahwa memeriksa data dari sumber atau responden akan membantu meningkatkan keabsahan temuan penelitian.

b. Observasi

Observasi dilakukan untuk melihat dan mencatat secara langsung proses manajemen risiko TI yang sedang berlangsung di organisasi yang menjadi studi kasus. Observasi ini membantu peneliti memahami bagaimana *framework* COBIT 2019 diimplementasikan dalam praktik sehari-hari dan bagaimana proses audit manajemen risiko dilakukan. Observasi akan mencakup pengamatan terhadap kegiatan rutin, penggunaan alat dan teknik tertentu, serta interaksi antar tim.

c. Studi Dokumen

Analisis dokumen dilakukan terhadap berbagai dokumen yang relevan dengan manajemen risiko TI dan penggunaan *framework* COBIT 2019. Dokumen yang dianalisis meliputi :

1. Kebijakan dan prosedur manajemen risiko TI
2. Laporan audit manajemen risiko TI
3. Dokumentasi *framework* COBIT 2019 yang digunakan
4. Catatan dan laporan hasil evaluasi risiko TI
5. Dokumentasi proses dan hasil implementasi COBIT 2019

Analisis dokumen bertujuan untuk mendapatkan informasi yang objektif dan komprehensif mengenai struktur, proses, dan hasil dari manajemen risiko TI dengan menggunakan *framework* COBIT 2019.

d. Kuesioner

Kuesioner diberikan kepada sejumlah pegawai yang terlibat dalam manajemen risiko TI di organisasi yang menjadi studi kasus. Kuesioner ini dirancang untuk mengumpulkan data kuantitatif dan kualitatif mengenai persepsi, pemahaman, dan pengalaman mereka terkait dengan penggunaan *framework* COBIT 2019. Pertanyaan dalam kuesioner mencakup aspek - aspek seperti efektivitas framework, tingkat kepuasan, dan tantangan yang dihadapi dalam implementasi. Kuesioner ini difungsikan sebagai salah satu instrumen untuk mendapat informasi secara terstruktur, sekaligus menjadi dasar dalam pelaksanaan wawancara pendalaman nantinya. Dalam pelaksanaannya, peneliti menyusun pernyataan dalam kuesioner yang berkaitan atau sesuai dengan bagain yang diteliti,

serta menjaga konsistensi jawaban responden agar jawaban tervalidasi dan dapat diandalkan. Langkah ini sejalan dengan penelitian *Reliability and validity of a questionnaire measuring knowledge, attitude and practice regarding "oil, salt and sugar" among canteen staff* yang menegaskan bahwa kesesuaian butir pertanyaan dalam kuesioner penelitian menjadi syarat penting untuk memperoleh data yang valid. Selain itu, penelitian *Validity and Reliability of Survey Data: Key to Empowering Chemical Health and Safety Research* juga menekankan bahwa konsistensi jawaban diperlukan agar jawaban responden dapat diandalkan.

e. Studi Literatur

Studi literatur dilakukan untuk mengumpulkan data dan informasi dari berbagai sumber tertulis yang relevan dengan topik penelitian. Literatur yang dikaji meliputi buku, jurnal, artikel, dan publikasi lainnya yang membahas tentang manajemen risiko TI, audit manajemen risiko, dan *framework* COBIT 2019. Studi literatur membantu peneliti dalam memahami konsep-konsep dasar, metodologi, dan temuan-temuan penelitian sebelumnya yang dapat menjadi landasan teori dan referensi bagi penelitian ini.

Dengan menggunakan metode pengumpulan data yang beragam ini, diharapkan dapat diperoleh data yang kaya dan mendalam untuk menganalisis audit manajemen risiko IT dengan menggunakan *framework* COBIT 2019 secara komprehensif.

3.3. Metode Analisis Data

Dalam penelitian ini menerapkan metode analisis data untuk mendapatkan kesimpulan yang berdasar dari hasil pengolahan data yang didapatkan. Berikut beberapa tahapan analisis risiko yang dilakukan :

1. *Risk Analysis*

Tahap pertama analisis risiko dilakukan untuk mengidentifikasi potensi risiko yang mungkin terjadi dalam konteks penelitian yang dilakukan. Proses ini melibatkan pengumpulan data dari berbagai sumber terkait dengan aktivitas atau domain yang sedang dianalisis. Setelah data terkumpul, RACI Chart digunakan sebagai alat bantu untuk menilai peran dan tanggung jawab dari setiap individu atau tim yang terlibat. RACI Chart memungkinkan peneliti untuk menentukan siapa yang *Responsible* (bertanggung jawab langsung), *Accountable* (bertanggung jawab secara keseluruhan), *Consulted* (dilibatkan untuk memberikan masukan), dan *Informed* (harus diberi tahu terkait perkembangan). Hasil dari proses ini menghasilkan pandangan yang lebih jelas mengenai distribusi tanggung jawab dan memungkinkan identifikasi area-area yang memerlukan perhatian lebih dalam manajemen risiko.

2. *Risk Profile*

Pada tahap ini, penelitian mengembangkan *risk profile* atau profil risiko dengan menggunakan hasil pengumpulan data yang didapatkan sebelumnya. Proses ini berfokus pada perhitungan CMMI *(Capability Maturity Model Integration)* yang spesfiki terhadap *Capability Level Test* untuk mengukur berbagai proses tata kelola dan manajemen TI dan sejauh mana kemampuan atau kapabilitas dari tim atau

individu dalam menghadapi risiko yang mungkin terjadi. *Capability Level Test* merupakan alat ukur penting untuk menilai tingkat kesiapan serta kematangan proses dalam merespons risiko, sehingga dapat mengidentifikasi kesenjangan antara kapabilitas yang ada dan kebutuhan nyata di lapangan. Di samping itu, skala Guttman digunakan sebagai tolak ukur pemberian nilai dari jawaban responden serta untuk menganalisis konsistensi responden, guna memperkuat pemahaman terkait tingkat kesiapan dan komitmen organisasi dalam mengelola risiko. Profil risiko ini membantu peneliti dalam menggambarkan risiko-risiko potensial dan dampaknya terhadap kegiatan atau sistem yang sedang diteliti.

3. *Risk Evaluation*

Evaluasi risiko merupakan tahap di mana hasil dari analisis risiko dibandingkan dengan standar atau ekspektasi yang telah ditetapkan dalam penelitian. Dalam konteks ini, dilakukan penilaian gap untuk melihat perbedaan antara level risiko aktual yang ditemukan dengan level risiko yang ideal atau diharapkan. Penilaian gap ini penting karena memungkinkan peneliti untuk memahami apakah risiko yang ada berada dalam batas toleransi atau membutuhkan perhatian khusus. Evaluasi risiko ini juga mempertimbangkan domain spesifik yang digunakan dalam penelitian ini, sehingga hasil evaluasi lebih relevan dan terfokus pada aspek-aspek yang menjadi perhatian utama.

4. *Risk Treatment*

Setelah melalui proses identifikasi, profil, dan evaluasi risiko, langkah selanjutnya adalah merumuskan strategi penanganan risiko atau risk treatment. Dalam skenario ini, peneliti menyusun rekomendasi untuk perencanaan mitigasi

risiko berdasarkan rangkuman dari berbagai skenario risiko yang telah dievaluasi. Penanganan risiko tidak hanya mencakup mitigasi risiko yang sudah ada, tetapi juga perencanaan untuk risiko yang berpotensi muncul di masa depan. Strategi *risk treatment* dapat mencakup langkah-langkah preventif, persiapan tindakan korektif, atau pembentukan kebijakan yang lebih kuat untuk meminimalkan dampak risiko yang mungkin terjadi. Proses ini bertujuan untuk memastikan bahwa organisasi atau tim dapat beradaptasi dan mengelola risiko secara proaktif, baik dalam jangka pendek maupun jangka panjang.

Gambar 3.1. Alur Analisis Data

3.4. Alur Penelitian

Penelitian akan mengikuti alur penelitian sebagai berikut, yang di bagi dalam 4 tahapan :

a. Tahap 1

1. Identifikasi Masalah

   a. Mengidentifikasi masalah yang berkaitan dengan manajemen risiko TI dan pentingnya audit manajemen risiko.

b. Menentukan relevansi dan kebutuhan akan *framework* COBIT 2019 dalam manajemen risiko TI.

2. Studi Literatur

a. Melakukan studi literatur untuk memahami konsep - konsep dasar manajemen risiko TI, audit manajemen risiko, dan *framework* COBIT 2019.

b. Mengkaji penelitian terdahulu yang relevan untuk mendapatkan wawasan dan landasan teori yang kuat.

3. Studi Pustaka

a. Mengumpulkan sumber-sumber pustaka yang relevan dengan manajemen risiko IT, audit manajemen risiko, serta framework COBIT 2019 dari jurnal - jurnal akademis, buku, dan artikel ilmiah.

b. Mengevaluasi hasil penelitian sebelumnya yang membahas penerapan audit manajemen risiko IT dan *framework* COBIT 2019 dalam industri yang relevan.

c. Membandingkan pendekatan dan hasil penelitian untuk menemukan kesenjangan pengetahuan dan peluang pengembangan dalam studi manajemen risiko IT.

4. Studi Dokumen

a. Mengidentifikasi dan menganalisis dokumen internal perusahaan terkait kebijakan, prosedur, dan praktik manajemen risiko IT yang telah diterapkan

b. Mengevaluasi audit internal sebelumnya untuk memahami kekuatan dan kelemahan dalam penerapan manajemen risiko IT.

c. Mengumpulkan data dari laporan audit, kebijakan IT, dan panduan internal lainnya untuk menilai kesesuaian dengan *framework* COBIT 2019.

b. Tahap 2

5. *Design Factor*

a. Mengidentifikasi faktor-faktor spesifik yang mempengaruhi desain sistem tata kelola TI.

b. Faktor - faktor ini meliputi ukuran perusahaan, industri, strategi bisnis, profil risiko, dan kematangan tata kelola TI.

c. Menentukan bagaimana framework COBIT 2019 harus disesuaikan untuk memenuhi kebutuhan spesifik perusahaan.

6. Domain Terpilih

a. Memilih domain COBIT 2019 yang paling relevan berdasarkan hasil identifikasi *design factor*.

b. Domain ini akan digunakan sebagai dasar untuk evaluasi dan audit manajemen risiko TI.

c. Menetapkan domain - domain utama yang akan dijadikan fokus utama dalam tata kelola risiko TI perusahaan.

7. Pengumpulan Data

a. Mengumpulkan informasi yang lengkap, valid, dan relevan dari berbagai sumber untuk mendukung pengambilan keputusan dan perbaikan sistem tata kelola TI

8. Pemetaan Raci

a. Menentukan peran dan tanggung jawab masing-masing pihak dalam manajemen risiko TI.

b. Menetapkan siapa yang bertanggung jawab *(Responsible)*, siapa yang harus mengambil keputusan *(Accountable)*, siapa yang perlu dikonsultasikan *(Consulted)*, dan siapa yang harus diinformasikan *(Informed)*.

9. Wawancara

a. Membuat kuesioner untuk mendapatkan data tambahan dari berbagai pihak yang terlibat.

b. Mengumpulkan pandangan langsung terkait pelaksanaan manajemen risiko TI dan implementasi COBIT 2019.

10. Kuesioner

a. Membuat kuesioner untuk mendapatkan data tambahan dari berbagai pihak yang terlibat.

b. Menyebarkan kuesioner kepada pihak-pihak yang tidak terlibat langsung dalam wawancara.

11. Data Terkumpul

a. Mengumpulkan semua data dari wawancara, kuesioner, dan dokumen yang relevan.

b. Mengorganisir data untuk memudahkan proses analisis selanjutnya.

c. Tahap 3

12. Analisis

a. Mengolah dan mengevaluasi untuk memahami situasi yang ada serta menentukan efektivitas manajemen risiko TI. Analisis ini melibatkan beberapa langkah penting untuk mendapatkan pemahaman yang komprehensif tentang bagaimana sistem tata kelola TI beroperasi, apakah sesuai dengan standar COBIT 2019, dan di mana perbaikan diperlukan.

13. Penilaian

a. Melakukan penilaian berdasarkan CMMI *(Capability Maturity Model Integration)* terhadap data yang telah dikumpulkan untuk menilai sejauh mana manajemen risiko TI yang di terapkan.

b. Menggunakan metode Guttman sebagai tolak ukur pemberian nilai dari jawaban responden yang hanya memiliki dua interval pilihan yaitu ya dan tidak.

14. GAP

a. Membandingkan hasil penilaian terhadap standar ideal yang ditetapkan oleh COBIT 2019.

b. Mengidentifikasi celah (GAP) antara kondisi saat ini dengan kondisi yang diinginkan.

15. Hasil

a. Menyusun laporan hasil yang mencakup area yang sudah sesuai dan area yang membutuhkan perbaikan.

b. Merumuskan poin-poin kunci yang menjadi fokus untuk tindakan lebih lanjut.

d. Tahap 4

16. Rekomendasi

a. Memberikan rekomendasi perbaikan untuk mengurangi GAP yang ditemukan dalam analisis.

b. Menyusun langkah-langkah strategis untuk meningkatkan tata kelola manajemen risiko TI.

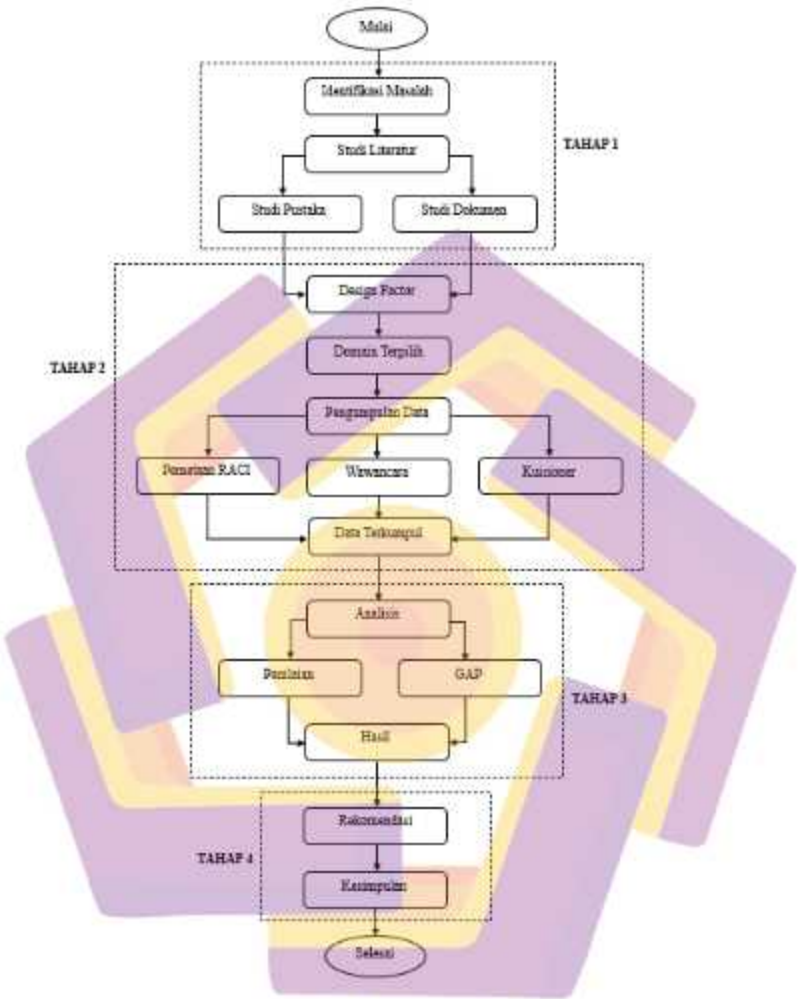
c. Rekomendasi dapat mencakup pelatihan, pengembangan sistem, perubahan kebijakan, atau peningkatan kontrol internal.

17. Kesimpulan

a. Merangkum keseluruhan proses dari identifikasi masalah hingga hasil analisis dan rekomendasi.

b. Menyimpulkan kesesuaian manajemen risiko TI dengan *framework* COBIT 2019

c. Menyusun arah tindakan berikutnya yang harus diambil oleh perusahaan untuk mengoptimalkan manajemen risiko TI.



Gambar 3.2. Alur Penelitian

Dengan mengikuti alur penelitian ini, diharapkan penelitian dapat dilaksanakan secara sistematis dan menghasilkan temuan yang bermanfaat untuk memahami dan meningkatkan manajemen risiko TI dengan menggunakan *framework* COBIT 2019.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Profil LAZNAS BMM

Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM) atau yang lebih dikenal dengan Baitulmaal Muamalat (BMM) adalah lembaga amil zakat nasional yang berbadan hukum, didirikan pada tahun 2000. BMM bertujuan untuk menghimpun dan menyalurkan dana Zakat, Infak, Sedekah, dan Wakaf (ZISWAF) dari umat kepada para mustahik atau penerima yang berhak. Berkantor pusat di Jakarta Timur, BMM berkomitmen untuk menjadi amil zakat yang independen, profesional, dan unggul dalam pengelolaan dana sosial keagamaan. BMM memiliki misi untuk memberdayakan ekonomi umat melalui pengelolaan dana zakat yang efektif dan transparan.

BMM menjalankan berbagai program sosial, pendidikan, kesehatan, dan pemberdayaan ekonomi. Program-program ini dirancang untuk memberikan manfaat maksimal bagi penerima zakat dan meningkatkan kesejahteraan masyarakat. Contoh program yang dijalankan antara lain bantuan beasiswa pendidikan, layanan kesehatan gratis, pembangunan infrastruktur sosial, dan program pemberdayaan ekonomi bagi kaum dhuafa. BMM menggunakan teknologi informasi dalam pengelolaan dana dan operasionalnya untuk memastikan transparansi dan akuntabilitas. Penggunaan TI juga memungkinkan BMM untuk menjangkau lebih banyak donatur dan penerima manfaat dengan efisien. Selain itu,

BMM secara rutin menjalani audit untuk memastikan kepatuhan terhadap regulasi dan standar pengelolaan dana yang berlaku.

4.1.1. Visi & Misi

Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM) memiliki Visi dan Misi sebagai berikut :

a. Visi

Menjadi amil zakat nasional yang independen, profesional dan unggul dalam memberikan kemudahan muzakki berzakat sesuai syariah serta melayani dan meningkatkan kesejahteraan mustahik.

b. Misi

1. Mengembangkan tata kelola yang baik berbasis teknologi dalam pengelolaan zakat dan wakaf.
2. Mengembangkan sumber daya manusia yang kompeten untuk kesinambungan tumbuh kembang lembaga.
3. Membangun aliansi strategis dengan berbagai pemangku kepentingan untuk kemandirian dan kemanfaatan lembaga.
4. Memberikan layanan bagi muzakki untuk menunaikan zakat dengan mudah dan benar sesuai syariah. Mengembangkan layanan dan program pemberdayaan untuk meningkatkan kesejahteraan mustahik.

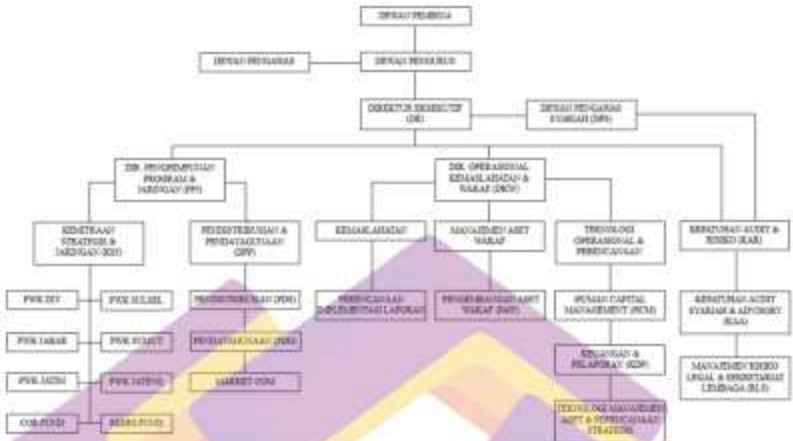
4.1.2. Nilai

Lembaga Amil Zakat Nasional Baitulmaal Muamalat (LAZNAS BMM) memiliki Nilai sebagai berikut :

1. Amanah, menjaga kepercayaan dengan sungguh - sungguh sebagai suatu kehormatan.
2. Manfaat, selalu memberi manfaat dalam setiap pemikiran, ucapan, dan perbuatan.
3. Inklusif, memberikan layanan terbaik kepada muzakki, mustahik, dan pemangku kepentingan lainnya dari berbagai kalangan.
4. Lurus, menempuh jalan lurus yaitu jalannya para Nabi, orang-orang yang mati syahid, orang-orang yang siddiq, dan orang-orang sholih.
5. Islami, menjaga integritas dalam setiap aktivitas sesuai ajaran islam, etika, dan aturan yang berlaku.
6. Modern, tanggap dan inovatif dalam memberikan solusi serta berfikir positif dan terbuka terhadap perubahan.
7. Professional, berorientasi pada proses dan layanan prima serta kompeten dan bertenggung jawab terhadap tugas dan kewajiban.

4.1.3. Struktur

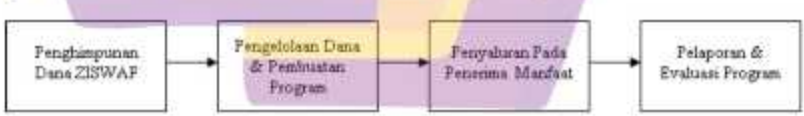
Struktur organisasi LAZNAS Baitulmaal Muamalat (BMM) berdasarkan yang tertera pada website www.bmm.or.id :



Gambar 4.1. Struktur Organisasi LAZNAS BMM

4.1.4. Proses Bisnis

Proses bisnis di LAZNAS Baitulmaal Muamalat (BMM) mencakup serangkaian langkah dasar yang berfokus pada tujuan utama lembaga, yaitu penghimpunan dan pendistribusian dana zakat, infaq, sedekah, dan wakaf. Proses ini menggambarkan alur sederhana, guna memperlihatkan bahwa kegiatan filantropi berjalan dengan jelas. Berikut gambar bagan yang menggambarkan proses bisnis di LAZNAS Baitulmaal Muamalat (BMM).



Gambar 4.2. Alur Proses Bisnis Level 0 di LAZNAS BMM

Gambar alur proses bisnis level 0 diatas menggambarkan 4 tahap proses bisnis di LAZNAS Baitulmaal Muamalat (BMM), setiap tahapan memiliki peran penting dalam membangun satu kesatuan proses bisnis, berikut penjelasan lebih rincinya.

1. Penghimpunan Dana ZISWAF

   Pada tahap ini, LAZNAS Baitulmaal Muamalat (BMM) mengumpulkan dana Zakat, Infak, Sedekah, dan Wakaf (ZISWAF) dari masyarakat baik individu ataupun kelompok melalui berbagai kanal, seperti donasi langsung, platform digital, maupun acara atau kegiatan penggalangan dana. Dana yang terkumpul akan diverifikasi dan dicatat guna memastikan kejelasan serta transparansi dana yang didapat.

2. Pengelolaan Dana & Pembuatan Program

   Setelah dana terkumpul, tahap berikutnya adalah pengelolaan dana, yaitu mengatur dana secara efektif dan efisien sehingga dapat termanfaatkan secara maksimal. Pada tahap ini, bentuk nyatanya adalah LAZNAS Baitulmaal Muamalat (BMM) membuat perencanaan dan pengembangan program-program sosial baru ataupun yang sudah ada untuk dibiayai, seperti program pemberdayaan ekonomi berupa modal usaha, program pendidikan berupa beasiswa, program pembangunan berupa pembangunan tempat ibadah atau tempat tinggal, serta program - program lainnya yang dibutuhkan oleh masyarakat.

3. Penyaluran Pada Penerima Manfaat

   Setelah dikelola dan dibentuk program, dana disalurkan kepada pihak - pihak yang berhak, yaitu penerima manfaat. Penyaluran ini dapat berupa uang atau barang, menyeluruh atau subsidi, langsung atau kemitraan, serta berkelanjutan atau satu kali.

4. Pelaporan & Evaluasi Program

Setelah penyaluran, Baitulmaal Muamalat akan melakukan pelaporan mengenai penggunaan dana dan hasil dari program yang telah dilaksanakan, pelaporan baik pada pemberi dana juga pada regulator. Setelah itu evaluasi dilakukan untuk menilai sejauh mana program tersebut berhasil mencapai tujuannya Hasil evaluasi ini digunakan sebagai umpan balik untuk memperbaiki dan meningkatkan kualitas program di masa depan.

4.2. Penilaian Status Terkini

Penilaian status terkini dilakukan untuk memberikan gambaran objektif dan jelas mengenai kondisi aktual manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Penilaian ini terbagi dalam dua bagian, bagian pertama yaitu kelengkapan penilaian, yang meliputi penentuan peran, domain, dan responden berdasarkan keselarasan antara struktur organisasi di LAZNAS Baitulmaal Muamalat (BMM) dengan kerangka RACI di *framework* COBIT 2019 dan yang kedua adalah hasil penilaian domain terpilih, yang terdiri dari hasil penilaian domain EDM 03 *(Ensure Risk Optimization)*, APO 12 *(Manage Risk)*, dan APO 13 *(Manage Security)*. Hasil yang diperoleh dari penilaian ini digunakan untuk mengetahui tingkat kapabilitas *(capability level)* proses manajemen risiko TI serta untuk mengidentifikasi kesenjangan *(gap)* antara kondisi nyata dan standar yang diharapkan.

4.2.1. Kebutuhan Penilaian

Kebutuhan penilaian merupakan tahap persiapan yang fundamental sebelum pelaksanaan audit manajemen risiko TI. Tahap ini bertujuan untuk

memastikan bahwa seluruh perangkat penilaian telah ditetapkan dengan tepat sesuai dengan konteks organisasi dan kerangka kerja COBIT 2019. Kelengkapan penilaian mencakup tiga bagian, yaitu bagian pertama adalah penentuan peran, yang dilakukan melalui sinkronisasi antara peran dalam struktur organisasi di LAZNAS Baitulmaal Muamalat (BMM) dengan dengan peran yang didefinisikan dalam RACI *chart framework* COBIT 2019, yang kedua adalah penentuan domain, domain ditentukan atau dipilih berdasarkan penggunaan *Design Factor*, guna memfokuskan audit pada area yang paling relevan dengan kebutuhan organisasi, dan yang ketiga adalah penentuan responden, responden ditentukan berdasarkan pihak - pihak yang tercantum dalam domain yang terpilih dan mereka atau pihak yang memiliki kompetensi serta tanggung jawab terkait dengan pengelolaan risiko dan keamanan TI di LAZNAS Baitulmaal Muamalat (BMM).

4.2.1.1. Peran

Penentuan peran melalui sinkronisasi peran yang tercantum di kerangka kerja COBIT 2019 dan yang tercantum di struktur organisasi LAZNAS Baitulmaal Muamalat (BMM), menghasilkan 5 peran yang relevan. Meskipun COBIT 2019 mendefinisikan 33 peran secara keseluruhan, dalam konteks Lembaga Amil Zakat Nasional Baitulmaal Muamalat, hanya 5 peran yang sesuai dengan struktur organisasi yang ada. Proses sinkronisasi ini dilakukan berdasarkan dengan RACI COBIT 2019 yang mencakup siapa yang bertanggung jawab langsung *(Responsible)*, siapa yang memiliki wewenang pengambilan keputusan *(Accountable)*, siapa yang perlu dikonsultasikan *(Consulted)*, dan siapa yang perlu

diinformasikan *(Informed)*. Berikut dapat dilihat pada Tabel 4.1. peran yang telah di sinkronisasi.

Tabel 4.1. Penentuan Peran

Peran di COBIT 2019 (RACI)	Peran di Baitulmaal Muamalat
Chief Risk Officer	Kepatuhan, Risiko dan Audit (KRA)
Chief Information Officer	Direktur Operasional
Chief Digital Officer	Marketing Communication, CRM & Digital (MCD)
Head IT Operations	Teknologi
Head IT Administration	Teknologi, Legal & General Affairs (TLG)

Peran yang terlibat dalam aktivitas audit ini terdiri dari *Chief Risk Officer* dalam COBIT yaitu Kepatuhan, Risiko dan Audit (KAR) dalam LAZNAS Baitulmaal Muamalat, *Chief Information Officer* yaitu Direktur Operasional, *Chief Digital Officer* yaitu Marketing Communication, CRM & Digital (MCD), *Head IT Operations* yaitu Teknologi, dan *Head IT Administration* yaitu Teknologi, Legal & General Affairs (TLG). Kelima peran tersebut memiliki tanggung jawab langsung maupun tidak langsung dalam pengelolaan risiko dan teknologi informasi di LAZNAS Baitulmaal Muamalat.

Setelah peran diketahui, tahap selanjutnya akan berfokus pada penentuan domain COBIT yang relevan dengan kebutuhan audit manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Kemudian saat domain telah diketahui, selanjutnya adalah penentuan responden, dilakukan berdasarkan peran-peran yang telah disinkronkan tersebut. Dalam hal ini, 5 peran yang relevan dengan pengelolaan TI di LAZNAS Baitulmaal Muamalat (BMM) akan menjadi 5 responden yang terlibat dalam audit. Penelitian berjudul *"Sample Size for Survey Research: Review and Recommendations"* menunjukkan bahwa jumlah yang kecil,

seperti 5 responden, cukup digunakan sebagai responden dalam penelitian, asalkan responden yang dipilih memiliki pemahaman yang mendalam dan relevan terhadap bagian yang diteliti. Pendapat ini diperkuat oleh penelitian *"Effectiveness of Cybersecurity Audit"*, yang menekankan bahwa efektivitas audit tidak bergantung pada jumlah responden, tetapi pada pemilihan responden yang kompeten dan memiliki pemahaman yang baik tentang bagian yang diaudit.

Agar lebih jelas mengenai peran masing-masing responden yang terlibat dalam audit ini, berikut disajikan uraian mengenai tugas dan wewenang mereka di dalam organisasi. Penjabaran ini penting untuk memastikan bahwa responden yang dipilih benar-benar selaras dengan peran serta tanggung jawabnya pada ketentuan dalam RACI COBIT 2019, dan memiliki keterkaitan langsung dengan aktivitas pengelolaan manajemen risiko TI serta kewenangan yang cukup untuk mewakili proses audit. Tabel 4.2. berikut menunjukkan tugas responden dalam organisasi.

Tabel 4.2. Tugas & Wewenang Responden

Responden	Tugas & Wewenang
Kepatuhan, Risiko dan Audit (KAR)	a. Bertanggung jawab atas pengelolaan terkait kepatuhan, risiko dan audit dalam organisasi. b. Menetapkan kebijakan, standar, dan prosedur terkait kepatuhan, risiko dan audit. c. Memastikan aktivitas audit risiko yang didalamnya termasuk audit risiko TI selaras dengan kebijakan organisasi. d. Menjadi penghubung utama antara manajemen puncak dengan tim audit internal maupun eksternal.
Direktur Operasional	a. Memiliki kewenangan penuh dalam pengelolaan operasional organisasi. b. Memastikan semua kegiatan termasuk proses audit risiko TI berjalan lancar dan tidak menghambat kegiatan operasional lainnya. c. Mengkomunikasikan terkait hasil audit yang berdampak pada kebijakan operasional kepada Direktur Eksekutif sebagai pucuk pimpinan eksekutif.
Marketing Communication, CRM & Digital (MCD)	a. Memasarkan program dengan memanfaatkan media digital serta sistem CRM (Customer Relationship Management). b. Memberikan perspektif strategis terkait transformasi digital dalam organisasi yang berkaitan dengan, baik pemasaran serta risiko dan keamanan digital.

	c. Memberikan masukan teknis dan bisnis dalam audit risiko TI, terutama yang berkaitan dengan sistem digital. d. Menyelaraskan hasil audit dengan strategi komunikasi dan layanan digital organisasi.
Teknologi	a. Menjalankan operasional dan mengontorl keseharian sistem TI. b. Memastikan infrastruktur TI termasuk jaringan internet, aplikasi, perangkat dan lainnya yang berkaitan dengan TI berfungsi dengan baik dan aman. c. Mendukung proses audit terkhusus dalam penyedian informasi berupa informasi kejadian, bukti, dan respon yang dilakuakn guna dimanfaatkan sebagai informasi dalam proses audit manajemen risiko TI. d. Melakukan implementasi teknis berdasar rekomendasi yang dihasilkan dari proses audit manajemn risiko TI.
Teknologi, Legal & General Affairs (TLG)	a. Bertugas mengelola aspek teknologi, legal dan urusan umum dalam organisasi termasuk pada TI. b. Mendukung proses audit dari sisi administratif berupa perjanjian dengan mitra, kepatuhan hukum, dan hal administratif lainnya yang berkaitan dengan TI c. Memberikan masukan mengenai regulasi yang memengaruhi kebijakan TI. d. Menjadi penghubung antara bagian teknis TI dengan manajemen atas dalam hal ini adalah Direktur Operasional.

Dengan penjabaran tugas dan wewenang dalam Tabel 4.2. diatas, dapat dikatakan bahwa tugas dan wewenang masing-masing peran atau responden sudah cukup mewakili seluruh proses audit sesuai prinsip RACI *(Responsible, Accountable, Consulted, Informed)*. Artinya, tidak ada tumpang tindih peran yang signifikan, dan setiap fungsi organisasi yang relevan terwakili dalam proses tugas dan wewenang peran – peran tersebut.

4.2.1.2. Domain

Pada tahap ini, penelitian berfokus pada penentuan domain COBIT yang relevan dengan kebutuhan audit yang dilakukan. Penentuan domain COBIT yang tepat merupakan langkah awal dan penting dalam audit, karena akan menentukan area-area mana saja yang perlu menjadi perhatian dalam proses audit. Agar pemilihan domain bersifat objektif dan metodologis, penelitian ini menggunakan metode pemilihan domain berdasarkan *Design Factor (DF)* yang ada dalam *Design*

Toolkit COBIT 2019 yang merupakan mekanisme yang disediakan oleh *framework* COBIT 2019 untuk menentukan area yang paling sesuai dengan konteks dan karakteristik organisasi serta tema penelitian. Metode ini dilakukan melalui wawancara dengan pihak - pihak yang memiliki peran dalam pengelolaan risiko TI dan keamanan informasi. Data hasil wawancara ini digunakan untuk memetakan kondisi organisasi ke dalam *Design Factor* (DF), yang meliputi :

a. *Enterprise Strategy (DF1)* untuk memahami strategi dan arah organisasi.
b. *Enterprise Goal (DF2)* untuk mengidentifikasi tujuan-tujuan utama yang didukung oleh TI.
c. *Risk Profile (DF3)* untuk mengidentifikasi risiko-risiko utama yang dihadapi organisasi.
d. IT *Related Issues (DF4)* untuk mengetahui permasalahan TI yang sedang berlangsung.

Keempat *Design Factor* tersebut diisi berdasarkan data dan temuan yang diperoleh melalui wawancara. Setelah *Design Factor* 1 hingga 4 disii selanjutnya menghasilkan nilai atau bobot pada masing - masing domain COBIT 2019 yang dapat dilihat pada *sheet Initial Design*, *sheet Initial Design* memberikan gambaran mengenai domain – domain yang relevan terhadap keadaan dan kebutuhan organisasi akan tata kelola TI khususnya pada pengelolaan risiko TI. Dengan demikian penentuan domain tidak dilakukan secara subjektif oleh peneliti, melainkan dihasilkan dari penekanan dan relevansi yang ditunjukkan oleh *Initial Design* berdasarkan pemetaan pada *Design Factor*. Selain itu penentuan domain bisa juga ditentukan secara langsung pada domain yang memiliki keterkaitan

dengan fokus penelitian, yaitu manajemen risiko TI dan keamanan, dengan pertimbangan berbasis kesesuaian konseptual dengan tema penelitian dan keterhubungannya dengan domain lain yang digunakan. Dengan cara ini, seluruh domain yang digunakan tetap berada dalam koridor metodologis dan sesuai dengan *framework* COBIT 2019. Berikut *Design Factor* yang digunakan :

1. *Design Factor 1 Enterprise Strategy*

Enterprise Strategy atau strategi perusahaan merupakan faktor penting dalam menentukan arah dan tujuan organisasi, serta peran teknologi informasi (TI) di dalamnya. Untuk memastikan bahwa TI dapat mendukung tujuan strategis organisasi, penting bagi perusahaan untuk menyelaraskan strategi TI dengan strategi perusahaan secara keseluruhan. Dalam konteks LAZNAS Baitulmaal Muamalat (BMM), strategi perusahaan berfokus pada pengelolaan ZISWAF (Zakat, Infak, Sedekah, dan Wakaf) yang transparan, efisien, dan aman. Oleh karena itu, TI harus memainkan peran kunci dalam mendukung kegiatan operasional dan meningkatkan layanan bagi donatur serta penerima manfaat.

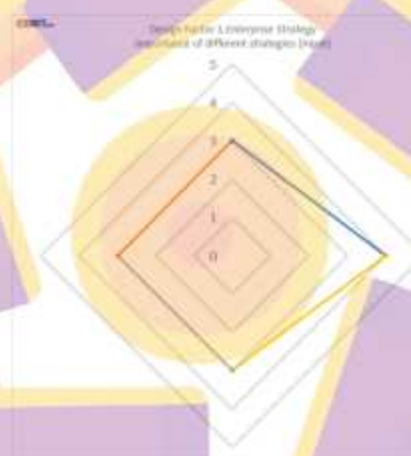
Dalam rangka memahami lebih dalam bagaimana strategi perusahaan diintegrasikan dengan TI, wawancara telah dilakukan dengan pihak terkait di LAZNAS Baitulmaal Muamalat (BMM). Hasil wawancara ini kemudian menghasilkan angka yang mengukur tingkat kepentingan dalam setiap value pada *Design Factor 1 Enterprise Strategy*, seperti yang terlihat pada Tabel 4.3. dibawah.

Tabel 4.3. *Design Factor 1*

Value	Importance (1-5)	Baseline
Growth/Acquisition	3	3
Innovation/Differentiation	3	3
Cost Leadership	3	3

Client Service/Stability	4	3

Dari Tabel 4.3. diatas dapat dilihat bahwa meskipun semua *value* memiliki bobot yang seimbang, terdapat fokus yang lebih *pada Client Service/Stability*, yang menunjukkan prioritas utama pada pelayanan yang stabil dan memuaskan bagi para klien dalam konteks LAZNAS Baitulmaal Muamalat (BMM) adalah donatur serta penerima manfaat. Berikut jika ditampilkan dalam bentuk lain yaitu dalam bentuk gambar grafik dapat dilihat pada Gambar 4.3.



Gambar 4.3. Grafik *Design Factor 1*

2. *Design Factor 2 Enterprise Goal*

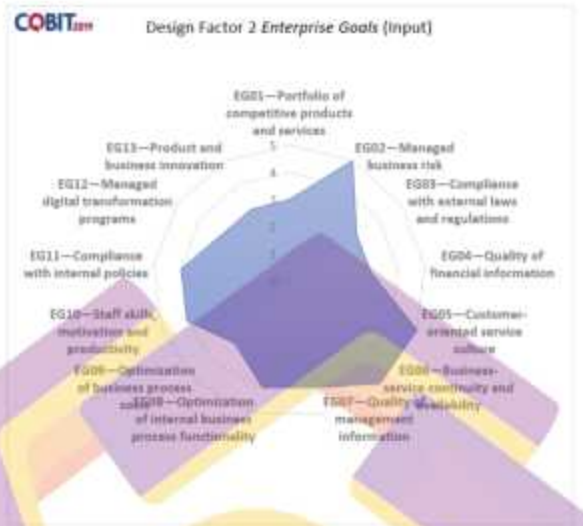
Enterprise Goal berfokus pada pencapaian tujuan organisasi yang lebih spesifik dan terukur. Dalam konteks Baitulmaal Muamalat (BMM), tujuan perusahaan tersemat jelas di visi yaitu "Menjadi amil zakat nasional yang independen, profesional dan unggul dalam memberikan kemudahan muzakki berzakat sesuai syariah serta melayani dan meningkatkan kesejahteraan mustahik". Melalui wawancara yang

dilakukan dengan pihak terkait di LAZNAS Baitulmaal Muamalat (BMM), guna penyelarasan dengan visi telah diperoleh angka yang merepresentasi tingkat kepentingan dari berbagai nilai yang ada pada *Enterprise Goal*. Hasil dapat dilihat pada Tabel 4.4. *Design Factor* 2 di bawah.

Tabel 4.4. *Design Factor 2*

Value	Importance (1-5)	Baseline
EG01—Portfolio of competitive products and services	3	3
EG02—Managed business risk	5	3
EG03—Compliance with external laws and regulations	3	3
EG04—Quality of financial information	3	3
EG05—Customer-oriented service culture	5	3
EG06—Business-service continuity and availability	5	3
EG07—Quality of management information	4	3
EG08—Optimization of internal business process functionality	4	3
EG09—Optimization of business process costs	3	3
EG10—Staff skills, motivation and productivity	4	3
EG11—Compliance with internal policies	4	3
EG12—Managed digital transformation programs	3	3
EG13—Product and business innovation	3	3

Tabel 4.4. *Design Factor* 2 menunjukkan nilai-nilai yang penting untuk LAZNAS Baitulmaal Muamalat (BMM). Nilai EG02 manajemen risiko bisnis yang terkendali, EG05 budaya layanan yang berorientasi pada pelanggan, dan EG06 kelangsungan layanan bisnis masing-masing mendapat nilai 5, menunjukkan prioritas utama pada pengelolaan risiko, layanan pelanggan, dan kelangsungan operasional. Selanjutnya dalam bentuk grafik dapat dilihat perolehan nilai pada setiap value dalam gambar grafik Gambar 4.4. di bawah.



Gambar 4.4. Grafik *Design Factor 2*

3. *Design Factor 3 Risk Profile*

Risk Profile menggambarkan risiko-risiko yang mungkin terjadi dalam operasional organisasi, serta dampak dan kemungkinan terjadinya risiko tersebut. Dalam konteks Baitulmaal Muamalat (BMM), *risk profile* mencakup berbagai kategori risiko TI yang relevan, yang dapat memengaruhi kelancaran operasional dan pencapaian tujuan organisasi. Dalam mengelola *risk profile*, risiko dibagi menjadi beberapa kategori berdasarkan tingkat dampak dan kemungkinan terjadinya yang dapat di lihat pada gambar 4.5. dibawah.

	Very High Risk
	High Risk
	Normal Risk
	Low Risk

Gambar 4.5. *Risk Rating*

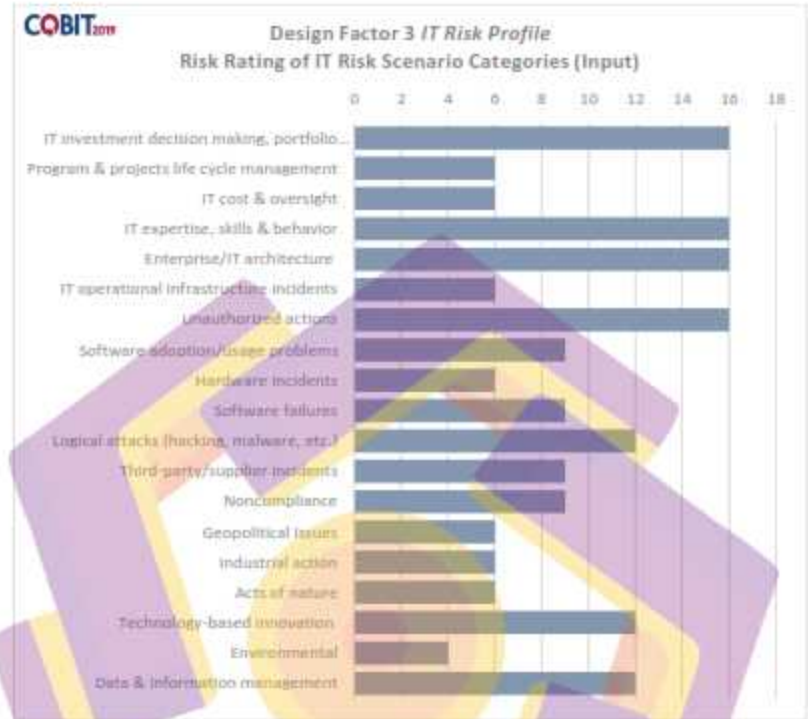
Tingkatan risiko ini membantu dalam pengelolaan dan pengambilan keputusan terkait langkah mitigasi yang harus diambil untuk mengurangi atau mengelola risiko sesuai dengan tingkat urgensi dan dampaknya. Untuk memperoleh gambaran yang lebih jelas mengenai profil risiko yang dihadapi, telah dilakukan wawancara dengan pihak terkait, dan hasilnya dituangkan dalam Tabel 4.5. yang menggambarkan penilaian terhadap berbagai skenario risiko.

Tabel 4.5. *Design Factor 3*

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating	Baseline
IT investment decision making, portfolio definition & maintenance	4	4	●	9
Program & projects life cycle management	3	2	●	9
IT cost & oversight	3	2	●	9
IT expertise, skills & behavior	4	4	●	9
Enterprise/IT architecture	4	4	●	9
IT operational infrastructure incidents	3	2	●	9
Unauthorized actions	4	4	●	9
Software adoption/usage problems	3	3	●	9
Hardware incidents	3	2	●	9
Software failures	3	3	●	9
Logical attacks (hacking, malware, etc.)	4	3	●	9
Third-party/supplier incidents	3	3	●	9
Noncompliance	3	3	●	9
Geopolitical Issues	3	2	●	9
Industrial action	3	2	●	9

Acts of nature	3	2	●	9
Technology-based innovation	4	3	●	9
Environmental	2	2	●	9
Data & information management	4	3	●	9

Tabel 4.5. diatas menunjukkan kategori skenario risiko yang diidentifikasi, beserta dampaknya *(impact)*, kemungkinan terjadinya *(likelihood)*, dan penilaian risiko *(risk rating)* untuk masing-masing kategori. Sebagai contoh, pada IT investment decision making, portfolio definition & maintenance, dampak dan kemungkinan terjadinya masing-masing diberi nilai 4. Begitu juga dengan kategori Program & *projects life cycle management*, *IT cost* & *oversight*, serta berbagai kategori risiko lainnya yang menunjukkan bagaimana setiap elemen risiko dihadapi dan dinilai. Selanjutnya dapat dilihat dalam bentuk grafik seperti yang terlihat pada gambar grafik dibawah. Grafik di bawah memperlihatkan visualisasi dari penilaian risiko yang telah dilakukan. Dari grafik ini, bisa dilihat bahwa kategori-kategori risiko dengan penilaian tinggi, memiliki nilai risiko yang lebih tinggi dibandingkan dengan kategori lainnya.



Gambar 4.6. Grafik *Design Factor 3*

Dengan melihat Tabel 4.5. dan Gambar 4.6. diatas, LAZNAS Baitulmaal Muamalat (BMM), dapat lebih memahami profil risiko yang dihadapi, serta mengidentifikasi area yang memerlukan perhatian khusus dalam upaya mitigasi risiko. Hal ini juga membantu dalam perencanaan dan pengelolaan risiko TI yang lebih efektif, sesuai dengan strategi yang telah ditetapkan.

4. *Design Factor 4 IT Related Issues*

IT Related Issues berfokus pada masalah terkait Teknologi Informasi (TI) yang dapat memengaruhi operasional dan keberhasilan organisasi. Di bagian ini, sejumlah isu yang berhubungan dengan pengelolaan TI diidentifikasi sebagai faktor

kritis yang harus mendapat perhatian khusus. Sebelum melihat tabel yang menggambarkan tingkat keparahan isu-isu terkait Teknologi Informasi (TI), penting untuk memahami bagaimana setiap masalah dikategorikan berdasarkan statusnya. Gambar 4.7. dibawah memperlihatkan bahwa setiap masalah TI akan ditandai berdasarkan seberapa besar dampaknya terhadap organisasi.

Gambar 4.7. *Importance Design Factor 3*

Gambar 4.7. membantu memvisualisasikan pengelompokan isu-isu TI yang tercatat berdasarkan tingkat risikonya, yang akan dijelaskan lebih lanjut dalam tabel selanjutnya. Tabel dibawah akan mengelompokkan setiap masalah TI sesuai dengan kategori status yang telah dijelaskan sebelumnya. diperoleh dari hasil wawancara dengan pihak terkait di LAZNAS Baitulmaal Muamalat (BMM), yang memberikan gambaran mengenai berbagai masalah yang dihadapi oleh organisasi terkait TI. Setiap masalah akan diberikan label berdasarkan tingkat keparahan, yaitu *No Issue, Issue,* atau *Serious Issue*, yang akan membantu dalam mengidentifikasi dan memprioritaskan langkah-langkah mitigasi yang diperlukan.

Tabel 4.6. *Design Factor 4*

IT-Related Issue	Importance (1-3)	Baseline

Frustration between different IT entities across the organization because of a perception of low contribution to business value		2
Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value		2
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT		2
Service delivery problems by the IT outsourcer(s)		2
Failures to meet IT-related regulatory or contractual requirements		2
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems		2
Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets		2
Duplications or overlaps between various initiatives, or other forms of wasted resources		2
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction		2
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget		2
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT		2
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions		2
Excessively high cost of IT		2
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems		2
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages		2
Regular issues with data quality and integration of data across various sources		2
High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation		2
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department (related to end-user computing, which often stems from dissatisfaction with IT solutions and services)		2
Ignorance of and/or noncompliance with privacy regulations		2

Inability to exploit new technologies or innovate using I&T		2

Berdasarkan Tabel 4.6. di atas isu serius mencakup frustrasi antara departemen TI dan bisnis yang dapat menghambat pencapaian tujuan organisasi, serta pengeluaran TI yang tersembunyi atau tidak sah, yang berpotensi menyebabkan pemborosan sumber daya. Selain itu, kegagalan penyedia layanan TI eksternal dalam memenuhi ekspektasi juga menjadi masalah kritis yang dapat mengganggu kelancaran operasional. Semua isu ini memerlukan perhatian segera untuk mencegah dampak negatif yang lebih besar pada organisasi. Selanjutnya, pada gambar grafik yang ada di bawah, dapat dilihat distribusi tingkat keparahan berbagai isu terkait TI yang telah dibahas sebelumnya. Gambar grafik ini menggambarkan bagaimana setiap isu dikategorikan berdasarkan tingkat kepentingannya, dengan sebagian besar isu serius mendapatkan nilai yang lebih tinggi. Isu-isu ini menunjukkan prioritas tinggi dalam pengelolaan dan mitigasi risiko TI.

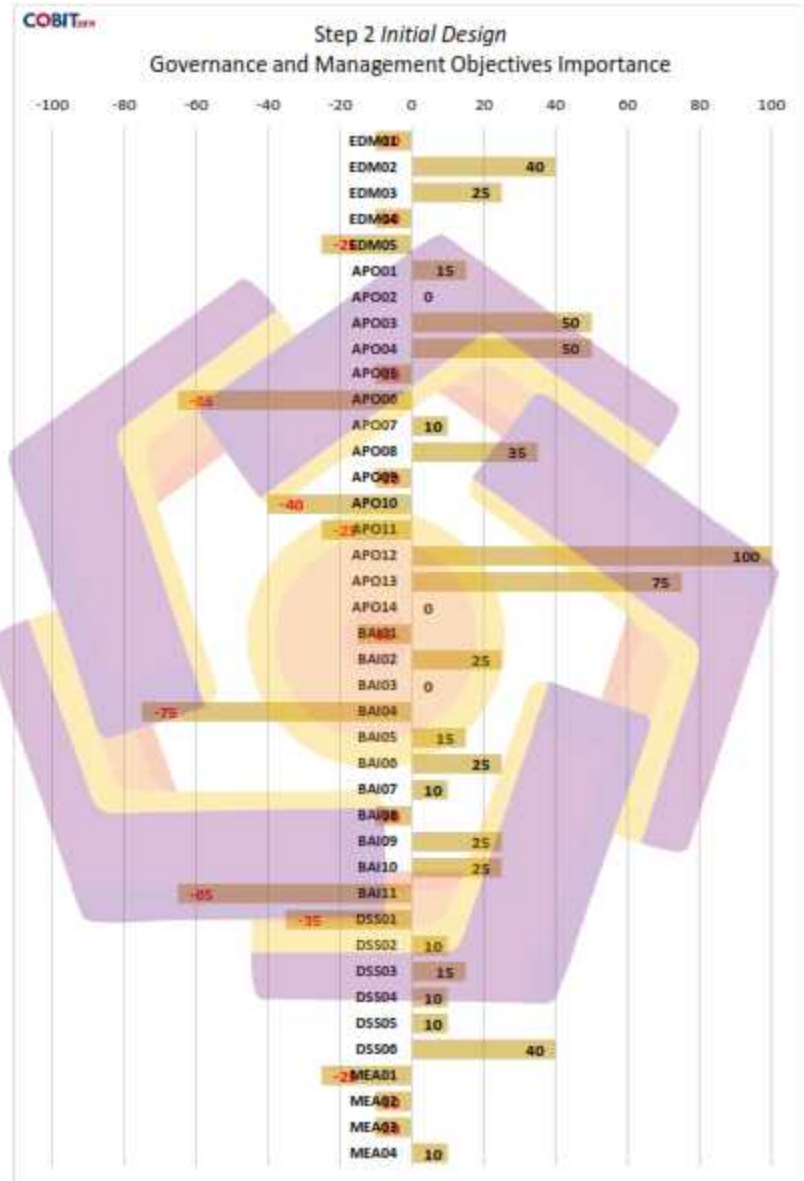
Gambar 4.8. Grafik *Design Factor 4*

Gambar 4.8. diatas menunjukkan bahwa sebagian besar isu yang masuk kategori serius, seperti frustrasi antara TI dan bisnis, serta pengeluaran TI yang tidak sah, mendapat perhatian lebih besar dalam pengelolaan risiko. Hal ini

mencerminkan pentingnya mengatasi masalah internal dan eksternal yang dapat merugikan organisasi jika dibiarkan tanpa penanganan yang tepat.

5. *Design Factor Result*

Design Factor Result, yang berbentuk gambar grafik di bawah menggambarkan hasil dari penilaian terhadap faktor-faktor desain dalam framework COBIT 2019 yang diterapkan pada Baitulmaal Muamalat (BMM). Grafik ini mengilustrasikan prioritas berbagai aspek atau domain yaitu *EDM, APO, BAI, DSS & MEA* dalam pengelolaan risiko TI berdasarkan penilaian terhadap *Design Factor* (DF1 hingga DF4). Hasil penilaian memberikan gambaran tentang seberapa penting masing-masing faktor desain dalam organisasi. Sisi kanan grafik mewakili faktor yang dianggap lebih penting atau lebih mendesak untuk diperhatikan, sementara sisi kiri menunjukkan faktor yang memiliki prioritas lebih rendah beserta juga nilai angkanya.



Gambar 4.9. Grafik Domain Terpilih

Berdasarkan gambar 4.9. di atas, terlihat bahwa nilai tertinggi muncul pada domain *APO 12 (Manage Risk)* dengan nilai 100 dan *APO 13 (Manage Security)* dengan nilai 75, ini menggambarkan pentingnya kedua faktor tersebut dalam manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Nilai yang tinggi pada kedua faktor ini menunjukkan bahwa LAZNAS Baitulmaal Muamalat (BMM) memberikan perhatian besar pada pengelolaan risiko dan keamanan dalam infrastruktur TI mereka. Domain lain yang dianggap penting namun memiliki nilai tingkat kepentingan yang lebih kecil di banding *APO 12 (Manage Risk)* dan *APO 13 (Manage Security)*, yaitu diangka 30 adalah EDM 03 *(Ensure Risk Optimization)*. EDM 03 diikutsertakan karena domain tersebut erat kaitannya juga dengan risiko. Penjelasan lebih lengkap terhadap domain terpilih sebagai berikut :

a. *EDM 03 (Ensure Risk Optimization)* berfokus pada pengoptimalan risiko di tingkat organisasi secara keseluruhan. Pengoptimalan ini tidak hanya berfokus pada pengurangan potensi kerugian akibat risiko, tetapi juga pada cara untuk mengelola risiko dengan cara yang menciptakan manfaat bagi organisasi. Proses dalam EDM 03 melibatkan evaluasi risiko dan memastikan bahwa setiap risiko ditangani dengan cara yang efisien dan menguntungkan. Dengan pendekatan ini, LAZNAS Baitulmaal Muamalat (BMM), dapat mengoptimalkan pengelolaan risiko yang ada, serta menciptakan nilai lebih melalui pengelolaan risiko yang lebih baik, yang pada gilirannya akan meningkatkan efektivitas dan transparansi operasional LAZNAS Baitulmaal Muamalat (BMM).
b. *(APO 12 (Manage Risk)* adalah domain yang berfokus pada pengelolaan risiko TI secara menyeluruh. Tujuan utama dari domain ini adalah untuk memastikan

bahwa risiko yang terkait dengan teknologi informasi dapat diidentifikasi, dievaluasi, dan dikelola dengan cara yang sistematik dan terstruktur. Proses dalam APO 12 mencakup identifikasi risiko, penilaian dampak dan kemungkinan terjadinya risiko, serta pengembangan strategi mitigasi risiko. Dalam konteks Lembaga Amil Zakat Nasional Baitulmaal Muamalat LAZNAS Baitulmaal Muamalat (BMM), pengelolaan risiko TI yang efektif sangat penting untuk mengurangi potensi gangguan operasional.

c. *APO 13 (Manage Security)* berkaitan dengan pengelolaan keamanan TI dalam organisasi. Tujuan dari domain ini adalah untuk memastikan bahwa kebijakan, kontrol, dan prosedur keamanan yang tepat diterapkan untuk melindungi aset informasi organisasi dari ancaman internal maupun eksternal. APO 13 mencakup kebijakan keamanan yang jelas, kontrol akses yang tepat, serta pengelolaan ancaman fisik dan logis terhadap infrastruktur TI. Keamanan data di LAZNAS Baitulmaal Muamalat (BMM) sangat penting karena lembaga ini mengelola dana ZISWAF yang sensitif, sehingga pengelolaan keamanan yang baik akan menjaga kepercayaan stakeholder serta memastikan perlindungan keamanan secara maksimal.

4.2.1.3. Responden

Pada tahap ini, peneliti akan menentukan siapa saja yang akan menjadi responden dalam pelaksanaan audit manajemen risiko TI menggunakan COBIT 2019 di Baitulmaal Muamalat . Proses pemilihan responden akan mengacu pada struktur organisasi di LAZNAS Baitulmaal Muamalat (BMM), yang disesuaikan dengan tabel RACI *Chart* sesuai pedoman COBIT 2019. RACI Chart, yang terdiri

dari empat peran yaitu *Responsible (R), Accountable (A), Consulted (C), dan Informed (I)*, digunakan untuk memetakan tanggung jawab setiap individu atau bagian dalam organisasi terhadap aktivitas audit yang akan dilakukan. Dalam hal ini, RACI *Chart* memastikan bahwa setiap anggota tim memiliki peran yang jelas dalam proses audit manajemen risiko TI. Proses perencanaan ini bertujuan untuk memastikan bahwa kegiatan audit dilaksanakan dengan efektif dan efisien, serta hasil yang diperoleh dapat memberikan rekomendasi yang konkret dalam memperkuat pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Berikut dibawah ini merupakan daftar responden pada masing-masing domain yang terpilih untuk digunakan dalam audit manajemen risiko TI :

1. Responden EDM 03 *(Ensure Risk Optimization)*

Dalam COBIT 2019 telah memilih responden dengan RACI yang telah ditentukan untuk domain *EDM 03 (Ensure Risk Optimization)* adalah dapat dilihat dalam Gambar 4.10. berikut.

B. Component: Organizational Structures									
Key Governance Practice	Board	Executive Committee	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	I&T Governance Board	Enterprise Risk Committee	Chief Information Security Officer	
EDM03.01 Evaluate risk management.	A	R	R	R	R	R	R		
EDM03.02 Direct risk management.	A	R	R	R	R	R	R		
EDM03.03 Monitor risk management.	A	R	R	R	R	R	R	R	

Gambar 4.10. Responden EDM 03

Selanjutnya berdasarkan pilihan responden dari COBIT 2019 dengan RACI yang telah ditentukan untuk domain *EDM 03 (Ensure Risk Optimization)* di

selaraskan dengan responden yang ada dalam struktur organisasi LAZNAS Baitulmaal Muamalat (BMM), dapat dilihat dalam Tabel 4.7 dibawah.

Tabel 4.7. Responden EDM 03

No	Peran di COBIT 2019	Peran di LAZNAS BMM
1	Board	-
2	Executive Committee	-
3	Chief Executive Officer	-
4	Chief Risk Officer	Kepatuhan, Risiko dan Audit (KRA)
5	Chief Information Officer	Direktur Operasional
6	I&T Governance Board	-
7	Enterprise Risk Committee	-
8	Chief Information Security Officer	-

Setelah dilakukan penyelarasan, peran yang terpilih adalah Kepatuhan, Risiko, dan Audit (KRA) yang berfokus pada pengelolaan risiko utama dan memastikan kepatuhan terhadap regulasi, disesuaikan dengan peran *Chief Risk Officer* (CRO) dalam COBIT 2019, yang bertanggung jawab atas mitigasi risiko TI secara menyeluruh. Sementara itu, Direktur Operasional di BMM yang memastikan kelancaran operasional TI diselaraskan dengan peran *Chief Information Officer* (CIO) yang mengelola infrastruktur TI dan mendukung tujuan organisasi. Kedua peran ini adalah bagian penting dalam mengelola dan memitigasi risiko yang berhubungan dengan TI di organisasi, khususnya untuk memastikan bahwa risiko TI yang ada dapat dioptimalkan dan dikelola dengan baik.

2. Responden APO 12 *(Ensure Risk Optimization)*

Pada COBIT 2019 telah memilih responden dengan RACI yang telah ditentukan untuk domain APO 12 *(Ensure Risk Optimization)* adalah dapat dilihat dalam Gambar 4.11. berikut.

B. Component: Organizational Structures																				
Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analyze risk.	A	R			R		R										
APO12.03 Maintain a risk profile.	A	R			R		R										
APO12.04 Articulate risk.	A	R			R		R										
APO12.05 Define a risk management action portfolio.	A	R			R		R										
APO12.06 Respond to risk.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

Gambar 4.11. Responden APO 12

Kemudian berdasarkan pilihan responden dari COBIT 2019 dengan RACI yang telah ditentukan untuk domain APO 12 *(Manage Risk)* diselaraskan dengan responden yang ada dalam struktur organisasi LAZNAS Baitulmaal Muamalat (BMM), dapat dilihat dalam Tabel 4.8. dibawah.

Tabel 4.8. Responden APO 12

No	Peran di COBIT 2019	Peran di LAZNAS BMM
1	Chief Risk Officer	Kepatuhan, Risiko dan Audit (KRA)
2	Chief Information Officer	Direktur Operasional
3	Chief Technology Officer	-
4	Chief Digital Officer	Marketing Communication, CRM & Digital (MCD)
5	Enterprise Risk Committee	-
6	Chief Information Security Officer	-
7	Business Process Owners	-
8	Project Management Office	-
9	Data Management Function	-
10	Head Architect	-
11	Head Development	-
12	Head IT Operations	Teknologi
13	Head IT Administration	Teknologi, Legal & General Affairs (TLG)
14	Service Manajer	-
15	Information Security Manajer	-
16	Business Continuity Manajer	-
17	Privacy Officer	-

Setelah dilakukan penyelarasan, peran yang terpilih meliputi Kepatuhan, Risiko, dan Audit (KRA), Direktur Operasional, *Chief Digital Officer, Head IT Operations*, dan *Head IT Administration*. KRA yang berfokus pada pengelolaan risiko utama disesuaikan dengan peran *Chief Risk Officer* (CRO) dalam COBIT 2019, yang bertanggung jawab atas mitigasi risiko TI secara menyeluruh. Direktur Operasional di BMM diselaraskan dengan *Chief Information Officer* (CIO) yang mengelola infrastruktur TI dan mendukung tujuan organisasi. *Chief Digital Officer* diselaraskan dengan Marketing Communication, CRM & Digital (MCD), sementara *Head IT Operations* dan *Head IT Administration* diselaraskan dengan peran Teknologi serta Teknologi Legal & General Affairs (TLG) untuk mendukung kelancaran operasional TI yang sesuai dengan kepatuhan dan regulasi.

3. Responden APO 13 *(Manage Security)*

Dalam COBIT 2019, domain *APO 13 (Manage Security)* memilih responden dengan RACI yang telah ditentukan, yang dapat dilihat dalam Tabel 4.12. berikut.

B. Component: Organizational Structures Key Management Practice	Chief Information Officer	Chief Technology Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO13.01 Establish and maintain an information security management system (ISMS).	R		R	A						R		R		
APO13.02 Define and manage an information security and privacy risk treatment plan.	R		R	A						R		R		R
APO13.03 Monitor and review the information security management system (ISMS).	R	R		A	R	R	R	R	R	R	R	R	R	R

Gambar 4.12. Responden APO 13

Kemudian, berdasarkan pilihan responden dari COBIT 2019 dengan RACI yang telah ditentukan untuk domain APO 13 *(Manage Security)*, penyelarasan dilakukan dengan responden yang ada dalam struktur organisasi LAZNAS Baitulmaal Muamalat (BMM), yang dapat dilihat dalam Tabel 4.9. di bawah.

Tabel 4.9. Responden APO 13

No	Peran di COBIT 2019	Peran di LAZNAS BMM
1	Chief Information Officer	Direktur Operasional
2	Chief Technology Officer	-
3	Enterprise Risk Committee	-
4	Chief Information Security Officer	-
5	Business Process Owners	-
6	Project Management Office	-
7	Head Architect	-
8	Head Development	-
9	Head IT Operations	Teknologi
10	Head IT Administration	Teknologi, Legal & General Affairs (TLG)
11	Service Manajer	-
12	Information Security Manajer	-
13	Business Continuity Manajer	-
14	Privacy Officer	-

Setelah dilakukan penyelarasan, peran yang terpilih adalah Direktur Operasional yang diselaraskan dengan *Chief Information Officer (CIO)* dalam COBIT 2019, bertanggung jawab untuk memastikan kelancaran operasional TI secara menyeluruh, serta mengelola infrastruktur TI yang mendukung tujuan strategis organisasi. Peran lainnya, *Head IT Operations*, yang disesuaikan dengan Teknologi, juga bertugas untuk mengelola dan mengoptimalkan sistem TI yang ada agar mendukung kelancaran operasional TI yang aman dan efisien. Selain itu, *Head IT Administration*, yang diselaraskan dengan Teknologi, Legal & General Affairs (TLG), juga berperan dalam memastikan bahwa operasional TI yang dilakukan sesuai dengan regulasi dan kebijakan yang berlaku.

4.2.2. Hasil Penilaian EDM 03 *(Ensure Risk Optimization)*

Penilaian pada domain EDM03 *(Ensure Risk Optimization)* bertujuan untuk mengevaluasi sejauh mana organisasi memastikan bahwa risiko terkait TI dikelola secara optimal untuk mendukung pencapaian tujuan strategis. Domain ini menilai efektivitas proses pengawasan manajemen risiko, termasuk bagaimana risiko diidentifikasi, dianalisis, dipantau, serta dilaporkan kepada pemangku kepentingan yang relevan. Penilaian pada domain ini dilakukan melalui kuesioner yang ditujukan kepada responden yang terkait dengan proses manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM) . Hasil penilaian untuk setiap sub domain dalam domain EDM 03 diuraikan sebagai berikut :

a. EDM 03.01 *(Evaluate Risk Management)*

Hasil kuesioner pada domain EDM 03.01 *(Evaluate Risk Management)* yang diberikan kepada 2 responden yaitu manajer Kepatuhan, Risiko, dan Audit (KRA) dan Direktur Operasional adalah sebagai berikut dapat dilihat pada Tabel 4.10. dibawah.

Tabel 4.10. Hasil Penilaian Kuesioner EDM 03.01

No	Aktivitas	*Capability Level*	Skor Responden	
			Responden 1	Responden 2
1	Memahami organisasi dan konteksnya terkait risiko I&T (Informasi dan Teknologi).	2	1	1
2	Menentukan toleransi risiko organisasi, yaitu tingkat risiko terkait I&T yang bersedia diambil oleh perusahaan dalam mengejar tujuan organisasinya.		1	1
3	Menentukan tingkat toleransi risiko terhadap toleransi risiko, yaitu penyimpangan yang dapat diterima sementara dari toleransi risiko.		1	1
4	Menentukan sejauh mana strategi risiko I&T selaras dengan strategi risiko organisasi dan memastikan toleransi risiko berada di bawah kapasitas risiko organisasi.		1	1
5	Secara proaktif mengevaluasi faktor risiko I&T sebelum keputusan strategis organisasi dan memastikan pertimbangan risiko menjadi bagian	3	1	1

	dari proses pengambilan keputusan strategis organisasi.			
6	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas organisasi terhadap potensi kerugian I&T dan toleransi kepemimpinan terhadapnya.		1	1
7	Menarik dan mempertahankan keterampilan dan personel yang diperlukan untuk manajemen risiko I&T.		1	0
Nilai Tertinggi			3	

Tabel 4.10. diatas menunjukkan hasil penilaian kuesioner untuk aktivitas *EDM 03.01 (Evaluate Risk Management)*. Sebagian besar aktivitas sudah dilaksanakan yang mana oleh 2 responden diberikan skor 1. Aktivitas yang sudah dilaksanakan masuk pada *capability level* 3 yaitu sebagai level tertinggi di domain EDM 03.01 *(Evaluate Risk Management)*, yang berarti organisasi sudah mencapai tingkat yang lebih matang dalam melaksanakan evaluasi menejemen risiko. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil dari wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) memahami organisasi dan konteksnya terkait risiko TI yang dituangkan dalam Rencana Strategis (Renstra) 2019-2025, toleransi risiko yang dapat diambil oleh perusahaan serta tingkat toleransi terhadap penyimpangan dalam toleransi risiko.
2. LAZNAS Baitulmaal Muamalat (BMM) mengevaluasi aktivitas dan faktor – faktor yang berpotensi menimbulkan risiko TI, memiliki personel yang terampil dalam mengatasai risiko TI. pelaksanaan aktivitas tersebut dilaksanakan terutama oleh manajer Kepatuhan, Risiko & Audit (KRA) yang bersinergi dengan manajer Tekonologi, Legal dan General Affairs (TLG).

b. EDM 03.02 *(Direct Risk Management)*

Hasil kuesioner pada domain EDM 03.02 *(Direct Risk Management)* diberikan kepada dua responden yaitu manajer Kepatuhan, Risiko, dan Audit (KRA) & Direktur Operasional adalah sebagai berikut yang dapat dilihat pada Tabel 4.11. dibawah.

Tabel 4.11. Hasil Penilaian Kuesioner EDM 03.02

No	Aktivitas	*Capability Level*	Skor Responden	
			Responden 1	Responden 2
1	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan aktivitas operasional.	2	1	1
2	Mengaarahkan pengembangan rencana komunikasi risiko (mencakup semua level dalam organisasi).		1	1
3	Mengarahkan implementasi mekanisme yang sesuai untuk merespons perubahan risiko secara cepat dan segera laporkan kepada tingkat manajemen yang relevan, didukung oleh prinsip-prinsip eskalasi yang telah disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).		1	0
4	Mengarahkan agar risiko, peluang, masalah, dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa saja kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan, serta dieskalasi kepada pengambil keputusan yang relevan.		1	1
5	Mengidentifikasi tujuan utama metrik dari proses tata kelola dan manajemen risiko yang akan dipantau, serta setujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran tersebut.	3	0	0
Nilai Tertinggi			2	

Tabel 4.11. diatas menunjukkan hasil penilaian kuesioner untuk aktivitas *EDM 03.02 (Direct Risk Management)*. Aktivitas yang sudah dilaksanakan oleh kedua responden diberikan skor 1 sedangkan yang belum dilaksanakan di berikan skor 0. Sebagian besar aktivitas yang dilaksanakan oleh kedua responden mencapai *capability level* 2, ini menunjukkan bahwa organisasi sudah memiliki pendekatan

yang terorganisir dan terdokumentasi untuk memanajemen risiko secara langsung, sedangkan aktivitas *capability level* 3 belum dilaksanakan. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil dari wawancara dan penilaian kuesioner yang ada.

1. Penterjemahan strategi risiko TI kedalam praktiknya di LAZNAS Baitulmaal Muamalat (BMM) dilaksanakan langsung oleh manajer Teknologi, lalu komunikasi terkait manajemen risiko termasuk risiko TI kepada struktur atas dan bawah dilakukan oleh manajer Kepatuhan, Risiko & Audit (KRA), sedang implementasi mekanisme apabila terjadi risiko dilakukan oleh manajer Teknologi dengan berlandaskan SOP.
2. Pelaporan terkait manajemen risiko dilakukan oleh manajer Kepatuhan, Risiko & Audit (KRA) ke pengambil keputusan tertinggi dalam jajaran eksekutif organisasi dalam hal ini adalah Direktur Eksekutif.
3. LAZNAS Baitulmaal Muamalat (BMM) belum menentukan pendekatan, metode serta teknik yang mendetail guna mengukur keberhasilan manajemen risiko TI, menimbang tingkat kesulitan risiko TI yang pernah dihadapi dan yang mungkin terjadi kedepan tidak terlalu memerlukan pendekatan, metode serta teknik yang mendetail, berhasil tidaknya manajemen risiko saat ini tertuang dalam *logbook* manajer Teknologi dan terkomunikasi ke pemangku kepentingan.

c. EDM 03.03 *(Monitor Risk Management)*

Hasil kuesioner pada domain EDM 03.03 *(Monitor Risk Management)* yang diberikan kepada dua responden yaitu manajer Kepatuhan, Risiko, dan Audit (KRA) & Direktur Operasional dapat dilihat pada Tabel 4.12. berikut.

Tabel 4.12. Hasil Penilaian Kuesioner EDM 03.03

No	Aktivitas	*Capabilty Level*	Skor Responden	
			Responden 1	Responden 2
1	Melaporkan setiap masalah manajemen risiko kepada dewan direksi atau komite eksekutif.	2	1	1
2	Memantau sejauh mana profil risiko dikelola sesuai dengan toleransi risiko dan ambang batas toleransi organisasi.	3	1	1
3	Memantau tujuan utama metrik dari proses tata kelola dan manajemen risiko terhadap targetnya, analisis penyebab setiap penyimpangan, dan lakukan tindakan perbaikan untuk mengatasi penyebab utamanya.	4	1	0
4	Memfasilitasi peninjauan oleh pemangku kepentingan utama terkait kemajuan organisasi menuju tujuan yang telah diidentifikasi.		1	1
Nilai Tertinggi			4	

Tabel 4.12. di atas menunjukkan hasil penilaian kuesioner untuk aktivitas EDM 03.03 *(Monitor Risk Management)*. Aktivitas yang sudah dilaksanakan oleh kedua responden diberikan skor 1, sedangkan yang belum dilaksanakan diberikan skor 0. Aktivitas yang dilaksanakan oleh kedua responden berada di *capability level* 2, *capability level* 3 dan *capability level* 4, menunjukkan bahwa pengukuran kinerja sudah dilakukan secara terus-menerus, dan keputusan pengelolaan risiko didasarkan pada data yang terkumpul untuk memprediksi dan mengelola proses sehingga lebih efisien. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) memberikan informasi terkait pembahasan manajemen risiko kepada dewan direksi dalam hal ini di BMM adalah Dewan Pengurus & Dewan Pengawas Syariah melalui RKAT (Rapat

Kerja Anggaran Tahunan) dari jajaran eksekutif diwakili oleh Direktur & Senior Manajemen (Kadiv, Manajer & Kepala Perwakilan).

2. Dalam memonitor dan memantau risiko di LAZNAS Baitulmaal Muamalat (BMM) dilaksanakan oleh manajer Teknologi bersinergi dengan manajer Kepatuhan, Risiko & Audit (KRA).
3. Pemantauan risiko TI dilakukan oleh manajer Teknologi namun belum sepenuhnya optimal mengingat SDM yang terbatas hanya 1 orang menyebabkan analisis penyebab penyimpangan, tindakan perbaikan cukup memerlukan waktu.
4. Peninjauan atau pembahasan terkait manajemen risiko dengan dewan direksi atau pemangku kepentingan utama dalam hal ini dilaksanakan saat RKAT (Rapat Kerja Anggaran Tahunan) yang dilaksanakan setahun sekali.

4.2.3. Hasil Penilaian APO 12 *(Manage Risk)*

Penilaian pada domain APO 12 *(Manage Risk)* bertujuan untuk mengetahui proses pengelolaan risiko TI secara menyeluruh, diantaranya mencakup identifikasi, pengumpulan data, analisis, dan respon terhadap risiko TI yang dapat mempengaruhi pencapaian tujuan organisasi. Penilaian dilakukan melalui kuesioner yang diberikan kepada responden yang memiliki keterlibatan langsung maupun tanggung jawab strategis dalam pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Hasil penilaian disajikan berdasarkan sub domain yang terdapat dalam domain APO 12, sehingga memberikan gambaran yang rinci, diuraikan sebagai berikut :

a. APO 12.01 *(Collect Data)*

Hasil kuesioner pada domain APO 12.01 *(Collect Data)* yang diberikan kepada lima responden dengan posisi sebagai berikut, manajer Kepatuhan, Risiko dan Audit (KRA), Direktur Operasional, manajer Marketing Communication, manajer CRM & Digital (MCD), manajer Teknologi, dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.13. berikut.

Tabel 4.13. Hasil Penilaian Kuesioner APO 12.01

No	Aktivitas	*Capabilty Level*	Skor Responden				
			Responden 1	Responden 2	Responden 3	Responden 4	Responden 5
1	Menetapkan dan memelihara metode untuk pengumpulan, pengklasifikasian, dan analisis data terkait risiko I&T	2	1	1	1	1	1
2	Mencatat data terkait dan signifikan yang berkaitan dengan risiko I&T pada lingkungan operasional internal dan eksternal perusahaan		1	1	1	1	1
3	Mengadopsi atau mendefinisikan taksonomi risiko untuk definisi yang konsisten mengenai skenario risiko dan kategori dampak serta kemungkinan.	3	1	1	1	1	1
4	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai dengan kategori dampak yang didefinisikan dalam taksonomi risiko. Menangkap data relevan dari masalah, insiden, masalah, dan penyelidikan terkait.		1	1	1	1	1
5	Menyurvei dan menganalisis data historis risiko I&T dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	4	1	1	0	1	1
6	Untuk kelas peristiwa yang serupa, mengorganisir data yang terkumpul dan menyoroti faktor yang berkontribusi. Menentukan faktor penyebab umum di berbagai peristiwa.		1	1	0	0	0
7	Menentukan kondisi spesifik yang ada atau tidak ada ketika peristiwa		1	1	0	1	1

	risiko terjadi dan bagaimana kondisi tersebut memengaruhi frekuensi peristiwa dan besaran kerugian.						
8	Melakukan analisis peristiwa dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang sedang berkembang dan untuk memahami faktor risiko internal dan eksternal yang terkait.		1	1	0	1	1
Nilai Tertinggi			4				

Tabel 4.13. menunjukkan hasil penilaian kuesioner untuk kegiatan pengumpulan data yang dilakukan oleh organisasi dalam mendukung pengelolaan risiko TI. Sebagian besar aktivitas yang dilaksanakan oleh responden mencapai *capability level* 2, *capability level* 3, dan *capability level* 4, yang menunjukkan bahwa organisasi sudah mengelola data dengan pendekatan yang terorganisir, terstandarisasi, dan dioptimalkan dengan baik. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. Pengumpulan data risiko TI baik dari internal ataupun eksternal LAZNAS Baitulmaal Muamalat (BMM) termasuk survei sederhana dan analisis data historis serta pengalaman kerugian dilakukan oleh manajer Teknologi, dicatatkan pada logbooknya.
2. Analisis penyebab, faktor dan dampak risiko TI bagi bisnis dibuat dan di tuangkan dalam file presentasi oleh manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi serta diketahui oleh Kepatuhan, Risiko dan Audit (KRA) yang nantinya akan dipaparkan kepada Direktur Eksekutif dan pemangku kepentingan lainnya.

b. APO 12.02 *(Analyze Risk)*

Hasil kuesioner pada domain APO 12.02 *(Analyze Risk)* yang diberikan kepada lima responden dengan jabatan sebagai berikut, manajer Kepatuhan, Risiko dan Audit (KRA), Direktur Operasional, manajer Marketing Communication CRM & Digital (MCD), manajer Teknologi, dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.14. berikut.

Tabel 4.14. Hasil Penilaian Kuesioner APO 12.02

No	Aktivitas	*Capability Level*	Skor Responden				
			Responden 1	Responden 2	Responden 3	Responden 4	Responden 5
1	Menentukan cakupan yang tepat untuk upaya analisis risiko, dengan mempertimbangkan semua faktor risiko dan/atau tingkat kepentingan aset bisnis.	3	1	1	1	1	1
2	Membuat dan secara rutin memperbarui skenario risiko I&T; eksposur kerugian yang terkait dengan I&T; serta skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis ancaman dan peristiwa yang saling berhubungan atau berurutan. Mengembangkan ekspektasi untuk aktivitas kontrol tertentu dan kemampuan untuk mendeteksi.		1	1	1	1	1
3	Memperkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan		0	1	1	1	1

	mengevaluasi kontrol operasional yang diketahui.						
4	Membandingkan risiko saat ini (eksposur kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko yang tidak dapat diterima atau meningkat.		1	1	1	1	1
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat selera risiko dan toleransi		1	1	1	1	1
6	Menentukan persyaratan tingkat tinggi untuk proyek atau program yang akan mengimplementasikan respons risiko yang dipilih. Mengidentifikasi persyaratan dan ekspektasi untuk kontrol utama yang sesuai dalam respons mitigasi risiko.		1	1	0	1	1
7	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (Business Impact Analysis, BIA) sebelum menggunakannya dalam pengambilan keputusan. Memastikan bahwa analisis selaras dengan kebutuhan perusahaan dan memverifikasi bahwa estimasi telah dikalibrasi dengan baik dan diuji terhadap bias.	4	1	1	0	1	1
8	Menganalisis biaya/manfaat dari opsi respons risiko potensial seperti	5	1	1	1	1	1

	menghindari, mengurangi/mitigasi, mentransfer/berbagi, dan menerima serta memanfaatkan peluang. Memastikan respons risiko yang optimal.						
Nilai Tertinggi			5				

Sebagian besar aktivitas yang dilaksanakan oleh responden mencapai *capability level* 3, *capability level* 4 dan *capability level* 5 juga sudah di capai artinya organisasi berfokus pada peningkatan berkelanjutan, proses TI terus disempurnakan dengan pembaruan yang didorong oleh evaluasi kinerja dan teknologi baru.. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) melakukan analisis risiko dengan mempertimbangkan semua faktor risiko termasuk kerugian dan keuntungan yang bisa didapatkan. Manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi bersinergi dengan manajer Kepatuhan, Risiko dan Audit (KRA) secara rutin berkomunikasi guna memperbarui, mengidentifikasi dan mengevaluasi skenario terkait risiko TI.
2. Usulan untuk langkah respon risiko TI seringkali berawal dari manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi dengan sepengetahuan Kepatuhan, Risiko dan Audit (KRA) lalu dituangkan dalam bentuk PPT yang akan di paparkan pada pengambil Keputusan utama dalam hal ini adalah Direktur Eksekutif.
3. Analisis dampak bisnis termasuk opsi respon seperti menghindari, mengurangi, memitigasi, dan lainnya di LAZNAS Baitulmaal Muamalat

(BMM) di buat oleh Manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi.

c. APO 12.03 *(Maintain A Risk Profile)*

Hasil kuesioner pada domain APO 12.03 (*Maintain Risk Performance)* yang diberikan kepada lima responden dengan jabatan sebagai berikut, manajer Kepatuhan, Risiko dan Audit (KRA), Direktur Operasional, manajer Marketing Communication, CRM & Digital (MCD), manajer Teknologi, dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.15. berikut.

Tabel 4.15. Hasil Penilaian Kuesioner APO 12.03

No	Aktivitas	*Capabilty Level*	Skor Responden				
			Responden 1	Responden 2	Responden 3	Responden 4	Responden 5
1	Menginventarisasi proses bisnis dan mendokumentasikan ketergantungan mereka pada proses manajemen layanan I&T dan sumber daya infrastruktur TI. Mengidentifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan penyedia layanan alih daya.		1	1	1	1	1
2	Menentukan dan menyepakati layanan I&T dan sumber daya infrastruktur TI yang penting untuk mendukung keberlanjutan operasi proses bisnis. Menganalisis ketergantungan dan mengidentifikasi kelemahan yang ada.	2	1	1	1	1	1
3	Mengelompokkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area		1	1	0	1	1

	fungsional						
4	Secara rutin menangkap semua informasi profil risiko dan mengkonsolidasikannya ke dalam profil risiko yang teragregasi.	3	1	1	1	1	1
5	Mengumpulkan informasi tentang status rencana tindakan risiko untuk dimasukkan ke dalam profil risiko I&T perusahaan.		1	1	1	1	1
6	Berdasarkan semua data profil risiko, mendefinisikan serangkaian indikator risiko yang memungkinkan identifikasi cepat dan pemantauan risiko saat ini serta tren risiko	4	1	1	1	1	1
7	Menangkap informasi tentang peristiwa risiko I&T yang telah terjadi untuk dimasukkan ke dalam profil risiko TI perusahaan.		1	1	1	1	1
Nilai Tertinggi			4				

Aktivitas yang dilaksanakan oleh responden mencapai *capability level* 2 *capability level* 3 dan *capability level* 4, yang menunjukkan bahwa proses TI sudah diukur dan dikelola berdasarkan data dan pengukuran yang lebih terperinci. Pengukuran kinerja dilakukan secara terus-menerus, dan keputusan pengelolaan risiko didasarkan pada data yang terkumpul untuk memprediksi dan mengelola proses lebih efisien.. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) melakukan inventarisasi terhadap layanan TI dan sumber daya TI yang dimiliki guna menambah informasi dalam profil risiko, dilaksanakan oleh manajer Teknologi.

2. LAZNAS Baitulmaal Muamalat (BMM) memiliki perencanaan atau skenario yang digunakan untuk meminimalisir terjadinya risiko yang dituangkan dalam bentuk SOP.
3. LAZNAS Baitulmaal Muamalat (BMM) menangkap perisitiwa risiko yang pernah terjadi di masa lalu kemudian di catatkan dalam profil risiko dalam bentuk logbook milik manajer Teknologi.

d. APO 12.04 *(Articulate Risk)*

Hasil kuesioner pada domain APO 12.04 *(Articulate Risk)* yang diberikan kepada lima responden dengan jabatan sebagai berikut, manajer Kepatuhan, Risiko dan Audit (KAR), Direktur Operasional, manajer Marketing Communication, CRM & Digital (MCD), manajer Teknologi, dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.16. berikut.

Tabel 4.16. Hasil Penilaian Kuesioner APO 12.04

No	Aktivitas	*Capabilty Level*	Skor Responden				
			Responden 1	Responden 2	Responden 3	Responden 4	Responden 5
1	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terdampak dalam istilah dan format yang berguna untuk mendukung pengambilan keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat kepercayaan untuk memungkinkan manajemen	3	1	1	1	1	1

	menyeimbangkan risiko dan pengembalian						
2	Memberikan pemahaman kepada pengambil keputusan mengenai skenario terburuk dan yang paling mungkin terjadi, eksposur kerugian terkait I&T, serta pertimbangan signifikan terkait reputasi, hukum, dan regulasi, atau kategori dampak lainnya sesuai dengan taksonomi risiko.		1	1	1	1	1
3	Melaporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi mengenai efektivitas proses manajemen risiko, efektivitas kontrol, celah, inkonsistensi, redundansi, status remediasi, dan dampaknya pada profil risiko.		1	1	1	1	1
4	Secara berkala, untuk area dengan kesetaraan relatif antara risiko dan kapasitas risiko, mengidentifikasi peluang terkait I&T yang memungkinkan penerimaan risiko yang lebih besar dan pertumbuhan serta pengembalian yang lebih baik.		0	1	1	0	1
5	Meninjau hasil penilaian pihak ketiga yang objektif, audit	4	0	0	0	0	0

	internal, dan tinjauan jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau celah yang teridentifikasi dan eksposur kerugian terkait I&T untuk menentukan kebutuhan akan analisis risiko tambahan						
Nilai Tertinggi			3				

Aktivitas yang dilaksanakan oleh responden mencapai *capability level* 3, yang menunjukkan bahwa organisasi sudah mulai mengelola risiko khususnya dalam mengartikulasikan risiko dengan pendekatan yang terorganisir dan terstandarisasi. Aktivitas dengan *capability level* 4 belum dilaksanakan. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) melaporkan hasil analisis risiko kepada pemangku kepentingan, laporan mencakup potensi kerugian dan keuntungan, serta terkait kategori dampak lainnya. Dilaporkan oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi yang bersinergi dengan manajer Kepatuhan, Risiko & Audit (KRA) kepada pemangku kepentingan dalam hal ini adalah Direktur Eksekutif.
2. Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi memberikan pemahaman mengenai profil risiko yang ada kepada pemangku kepentingan.

3. Dalam melakukan audit LAZNAS Baitulmaal Muamalat (BMM) belum pernah melibatkan pihak ke eksternal.

e. APO 12.05 *(Define a Risk Management Action Portfolio)*

Hasil kuesioner pada domain APO 12.05 *(Define a Risk Management Action Portfolio)* yang diberikan kepada lima responden dengan posisi sebagai berikut, manajer Kepatuhan, Risiko dan Audit (KRA), Direktur Operasional, manajer Marketing Communication, CRM & Digital (MCD), manajer Teknologi, dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.17. berikut.

Tabel 4.17. Hasil Penilaian Kuesioner APO 12.05

No	Aktivitas	*Capabilty Level*	Skor Responden				
			Responden 1	Responden 2	Responden 3	Responden 4	Responden 5
1	Memelihara inventarisasi aktivitas kontrol yang diterapkan untuk mengurangi risiko dan memungkinkan risiko yang diambil sesuai dengan selera risiko dan toleransi. Mengklasifikasikan aktivitas kontrol dan memetakannya ke skenario risiko I&T spesifik serta pengelompokan skenario risiko I&T	2	1	1	1	1	1
2	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima tanggung jawab atas operasinya dalam tingkat toleransi individu dan portofolio.	3	1	1	1	1	1

3	Mendefinisikan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang strategis perusahaan, dengan mempertimbangkan biaya, manfaat, dampaknya pada profil risiko saat ini, serta peraturan,		0	1	1	1	1
Nilai Tertinggi			3				

Aktivitas yang dilaksanakan oleh responden mencapai *capability level* 2 dan *capability level* 3, yang menunjukkan bahwa organisasi sudah mendefinisikan tindakan untuk memanajemen risiko dengan pendekatan yang terorganisir dan terstandarisasi. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) menginventarisasi aktivitas kontrol ke dalam skenario manajemen risiko TI melalui manajer Teknologi & manajer Kepatuhan, Risiko & Audit (KRA).
2. Setiap bagian di LAZNAS Baitulmaal Muamalat (BMM) memiliki peran dalam memantau dan menangani risiko TI sesuai tanggung jawab masing-masing, pengarahan diberikan oleh manajer Teknologi.
3. Proyek atau perencanaan di LAZNAS Baitulmaal Muamalat (BMM) dalam rangka mengatasi risiko TI dirancang oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi, dengan mempertimbangan faktor-faktor yang ada.

f. APO 12.06 *(Respon To Risk)*

Hasil kuesioner pada domain APO 12.06 *(Respond To Risk)* yang diberikan kepada lima responden dengan jabatan sebagai berikut, manajer Kepatuhan, Risiko dan Audit (KAR), Direktur Operasional, manajer Marketing Communication, CRM & Digital (MCD), manajer Teknologi, dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.18. berikut.

Tabel 4.18. Hasil Penilaian Kuesioner APO 12.06

No	Aktivitas	*Capability Level*	Skor Responden				
			Responden 1	Responden 2	Responden 3	Responden 4	Responden 5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik untuk diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak serius terhadap bisnis. Pastikan bahwa rencana mencakup jalur eskalasi di seluruh perusahaan.	3	1	1	1	1	1
2	Menerapkan rencana respons yang sesuai untuk meminimalkan dampak ketika insiden risiko terjadi.		1	1	1	1	1
3	Mengkategorikan insiden dan membandingkan eksposur kerugian terkait I&T dengan ambang toleransi risiko. Mengkomunikasikan dampak bisnis kepada pengambil	4	1	0	1	1	1

	keputusan sebagai bagian dari pelaporan dan memperbarui profil risiko.						
4	Memeriksa kejadian buruk/kerugian masa lalu dan peluang yang terlewatkan untuk menentukan penyebab utamanya.		1	1	1	1	1
5	Mengkomunikasikan penyebab utama, kebutuhan respons risiko tambahan, dan perbaikan proses kepada pengambil keputusan yang tepat. Pastikan bahwa penyebab, kebutuhan respons, dan perbaikan proses dimasukkan ke dalam proses tata kelola risiko.	5	1	1	1	1	1
Nilai Tertinggi			5				

Aktivitas yang dilaksanakan oleh responden mencapai *capability level* 3, *capability level* 4 dan *capability level* 5, yang menunjukkan bahwa organisasi sudah mulai berfokus pada peningkatan berkelanjutan. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. Dalam merespon risiko LAZNAS Baitulmaal Muamalat (BMM) memiliki langkah-langkah dalam bentuk SOP yang dapat dijalankan ketika suatu peristiwa risiko terjadi.
2. LAZNAS Baitulmaal Muamalat (BMM) melalu manajer Teknologi dalam logbook mencatat kerugian akibat risiko yang pernah terjadi di masa lalu untuk mengetahui penyebab utamanya, sehingga bisa dijadikan sebagai bahan pertimbangan menyusun langkah antisipasi risiko di masa mendatang.

3. LAZNAS Baitulmaal Muamalat (BMM) mengkomunikasikan setiap hal yang berkaitan dengan manajemen risiko kepada pemangku kepentingan di level eksekutif yang tertinggi dalam hal ini adalah Direktur Eksekutif.

4.2.4. Hasil Penilaian APO 13 *(Manage Security)*

Penilaian pada domain APO13 *(Manage Security)* bertujuan untuk mengetahui sejauh mana organisasi telah menerapkan pengelolaan keamanan informasi sebagai upaya mendukung keberlangsungan operasional dan perlindungan informasi. Domain ini menitik beratkan pada efektivitas pengembangan, penerapan, dan pemeliharaan sistem manajemen keamanan informasi, termasuk kebijakan, prosedur, serta kontrol yang digunakan untuk mencegah dan memitigasi ancaman terhadap keamanan TI. Penilaian dilakukan melalui penyebaran kuesioner kepada responden yang memiliki tanggung jawab strategis maupun operasional terkait keamanan informasi di LAZNAS BMM. Hasil penilaian kemudian disajikan berdasarkan sub domain pada domain APO 13 guna memberikan gambaran secara lebih rinci, sebagai berikut :

a. APO 13.01 *(Establish and maintain an information security management system (ISMS))*

Hasil kuesioner pada domain APO 13.01 *(Establish and maintain an information security management system (ISMS)* yang diberikan kepada tiga responden dengan jabatan sebagai berikut, Direktur Operasional, manajer Teknologi dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.19. berikut.

Tabel 4.19. Hasil Penilaian Kuesioner APO 13.01

No	Aktivitas	*Capabilty Level*	Skor Responden		
			Responden 1	Responden 2	Responden 3
1	Menentukan ruang lingkup dan batasan sistem manajemen keamanan informasi berdasarkan karakteristik perusahaan, organisasi, lokasi, aset, dan teknologi. Sertakan detail serta alasan untuk setiap pengecualian dari ruang lingkup.	2	1	1	1
2	Mendefinisikan batasan sistem manajemen keamanan informasi sesuai dengan kebijakan perusahaan dan konteks di mana perusahaan beroperasi.		1	1	1
3	Menyelaraskan batasan sistem manajemen keamanan informasi dengan pendekatan keseluruhan perusahaan terhadap pengelolaan keamanan.		1	1	1
4	Mendapatkan otorisasi manajemen untuk mengimplementasikan, mengoperasikan, atau mengubah batasan sistem manajemen keamanan informasi.		1	1	1
5	Mempersiapkan dan memelihara pernyataan penerapan yang menjelaskan ruang lingkup batasan sistem manajemen keamanan informasi.		1	1	1
6	Menentukan dan mengkomunikasikan peran dan tanggung jawab pengelolaan keamanan informasi.		1	1	1
7	Mengkomunikasikan pendekatan batasan sistem manajemen keamanan informasi.		1	1	1
Nilai Tertinggi			2		

Aktivitas yang dilaksanakan oleh responden mencapai *capability level* 2, yang menunjukkan bahwa organisasi sudah mulai mengelola sistem keamanan informasi dengan pendekatan yang terorganisir dan terdokumentasi. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) menentukan ruang lingkup dan batasan sistem manajemen keamanan informasi, serta menyesuaikannya dengan karakteristik perusahaan dan teknologi yang digunakan, tertuang dalam Renstra (Rencana Strategis) 2019-2025.

2. Menyelaraskan batasan sistem keamanan informasi sesuai dengan kebijakan dan kondisi perusahaan, serta menyampaikan batasan tersebut kepada seluruh bagian yang terlibat baik peran, tanggung jawab & batasan dalam pengelolaan keamanan informasi, dalam persoalan keamanan sistem informasi di LAZNAS Baitulmaal Muamalat (BMM) di kelola oleh manajer Teknologi, Legal & General Affairs (TLG).

b. APO 13.02 *(Define and Manage an Information Security and Privacy Risk Treatment Plan)*

Hasil kuesioner pada domain APO 13.02 *(Define and Manage an Information Security and Privacy Risk Treatment Plan)* yang diberikan kepada tiga responden dengan jabatan sebagai berikut, Direktur Operasional, manager Teknologi dan manager Teknologi, Legal & General Affairs (TLG).

Tabel 4.20. Hasil Penilaian Kuesioner APO 13.02

No	Aktivitas	*Capability Level*	Skor Responden		
			Responden 1	Responden 2	Responden 3
1	Merumuskan dan memelihara rencana penanganan risiko keamanan informasi yang selaras dengan tujuan strategis dan arsitektur perusahaan. Pastikan rencana tersebut mengidentifikasi praktik manajemen dan solusi keamanan yang tepat dan optimal, beserta sumber daya, tanggung jawab, dan prioritas yang terkait untuk mengelola risiko keamanan informasi yang telah diidentifikasi.	3	1	1	1
2	Memelihara inventarisasi komponen solusi sebagai bagian dari arsitektur perusahaan untuk mengelola risiko terkait keamanan.		1	1	1
3	Mengembangkan proposal untuk mengimplementasikan rencana penanganan risiko keamanan informasi, didukung oleh studi kelayakan bisnis yang mencakup pertimbangan pendanaan serta pembagian peran dan tanggung jawab.		1	1	1
4	Memberikan masukan untuk desain dan pengembangan praktik manajemen serta solusi yang dipilih dari rencana penanganan risiko		1	1	1

	keamanan informasi.				
5	Melaksanakan program pelatihan dan peningkatan kesadaran terkait keamanan informasi dan privasi.		0	1	1
6	Mengintegrasikan perencanaan, desain, implementasi, dan pemantauan prosedur keamanan informasi dan privasi, serta kontrol lain yang mampu mencegah secara cepat, mendeteksi peristiwa keamanan, dan merespons insiden keamanan.		0	1	1
7	Menentukan cara untuk mengukur efektivitas praktik manajemen yang dipilih. Spesifikasikan bagaimana pengukuran ini digunakan untuk menilai efektivitas guna menghasilkan hasil yang dapat dibandingkan dan direproduksi.	4	0	0	0
Nilai Tertinggi			3		

Aktivitas yang dilaksanakan oleh responden mencapai *capability level* 3, yang menunjukkan bahwa organisasi sudah menetapkan dan mengelola penanganan risiko kemanan informasi dan privasi dengan pendekatan yang terorganisir, terstandarisasi, dan dikelola dengan baik. Namun, aktivitas dengan *capability level* 4 belum dilaksanakan. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) menyusun dan memperbarui rencana penanganan risiko keamanan informasi yang mendukung tujuan perusahaan, serta mencatat komponen-komponen solusi yang diperlukan.
2. Setiap orang di LAZNAS Baitulmaal Muamalat (BMM) berhak memberikan masukan untuk desain dan pengembangan solusi keamanan.
3. LAZNAS Baitulmaal Muamalat (BMM) memilikli program pelatihan untuk meningkatkan kesadaran terkait keamanan dan privasi yang diadakan oleh manajer Teknologi.

4. LAZNAS Baitulmaal Muamalat (BMM) belum merinci bagaimana cara mengukur bahwa sudah sejauh mana praktik manajemen yang dipilih efektif.

c. APO 13.03 *(Monitor and Review the Information Security Management System (ISMS))*

Hasil kuesioner pada domain APO 13.03 *(Monitor and Review the Information Security Management System (ISMS)* yang diberikan kepada tiga responden dengan jabatan sebagai berikut, Direktur Operasional, manajer Teknologi dan manajer Teknologi, Legal & General Affairs (TLG), dapat dilihat pada Tabel 4.21. berikut.

Tabel 4.21. Hasil Penilaian Kuesioner APO 13.03

No	Aktivitas	*Capabilty Level*	Skor Responden		
			Responden 1	Responden 2	Responden 3
1	Melakukan tinjauan rutin terhadap efektivitas sistem manajemen keamanan informasi. Tinjauan ini mencakup pemenuhan kebijakan dan tujuan sistem manajemen keamanan informasi serta peninjauan praktik keamanan dan privasi.	4	1	1	1
2	Melaksanakan audit sistem manajemen keamanan informasi secara berkala sesuai dengan interval yang direncanakan		0	1	1
3	Melakukan tinjauan manajemen terhadap sistem manajemen keamanan informasi secara rutin untuk memastikan bahwa ruang lingkup tetap memadai dan perbaikan dalam proses sistem manajemen keamanan informasi dapat diidentifikasi.		1	1	1
4	Mencatat tindakan dan peristiwa yang dapat memengaruhi efektivitas atau kinerja sistem manajemen keamanan informasi.		0	1	1
5	Memberikan masukan untuk pemeliharaan rencana keamanan dengan mempertimbangkan temuan dari aktivitas pemantauan dan tinjauan.	5	1	1	1
Nilai Tertinggi			5		

Aktivitas yang dilaksanakan oleh responden yaitu pada *capability level* 4 & *capability level* 5 yang menunjukkan bahwa organisasi sudah melaksanakan

penyempurnaan dibarengi pembaruan yang didorong oleh evaluasi kinerja dan teknologi baru. Penggunaan inovasi dan praktik terbaik dilakukan untuk mencapai kinerja optimal dan efisiensi yang lebih tinggi dalam pengelolaan TI.. Berikut adalah kesimpulan yang ditemukan berdasarkan hasil wawancara dan penilaian kuesioner yang ada.

1. LAZNAS Baitulmaal Muamalat (BMM) meninjau secara rutin efektivitas sistem keamanan dan memastikan sistem tersebut berjalan sesuai kebijakan dan tujuan yang ditetapkan.
2. Melakukan audit internal secara berkala yang dilakukan oleh manajer Teknologi dengan mengevaluasi dan memeriksa sistem keamanan guna memastikan bahwa semua aspek kemanan informasi tetap terjaga dan diperbaiki jika ada kekeliruan.
3. LAZNAS Baitulmaal Muamalat (BMM) mencatat peristiwa yang mempengaruhi kinerja sistem keamanan informasi dilakukan oleh manajer Teknologi lalu di catatkan pada *logbook* nya.
4. Setiap orang di LAZNAS Baitulmaal Muamalat (BMM) berhak memberi masukan terkait keamanan sistem termasuk pemeliharaan, rancangan, aktivitas pemantau sistem keamanan yang ada di organisasi.

4.3. Identifikasi Gap & Area Perbaikan

Bagian ini menguraikan proses untuk mengidentifikasi kesenjangan *(gap)* antara tingkat kapabilitas pengelolaan risiko TI yang dicapai saat ini dengan tingkat kapabilitas yang menjadi target organisasi, serta menentukan area-area yang perlu

mendapatkan perhatian khusus untuk perbaikan. Identifikasi ini tidak hanya menyoroti perbedaan tingkat kapabilitas, tetapi juga memetakan aspek-aspek spesifik yang masih memerlukan perbaikan dan peningkatan sehingga bisa memenuhi standar. Dengan memahami *gap* dan area yang perlu ditingkatkan, organisasi dapat menentukan fokus perbaikan secara lebih terarah dan menyusun langkah-langkah penguatan yang relevan. Hasil identifikasi ini menjadi dasar bagi penetapan prioritas perbaikan serta penyusunan strategi peningkatan kapabilitas pada tahap selanjutnya.

4.3.1. Hasil Identifikasi Gap

Pada bagian ini, dilakukan identifikasi terhadap hasil audit dan menilai sejauh mana kapabilitas pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM), serta mengidentifikasi kesenjangan *(gap)* antara kondisi saat ini dengan standar yang diharapkan, dengan mengacu pada model kapabilitas yang terdapat dalam kerangka kerja COBIT 2019. Melalui uji tingkat kapabilitas ini, dapat diketahui area-area yang membutuhkan perbaikan serta langkah-langkah yang dapat diambil untuk meningkatkan efektivitas pengelolaan risiko TI dalam mendukung tujuan organisasi.

Mengetahui nilai gap dilakukan sebagai upaya untuk mengidentifikasi perbedaan antara tingkat kapabilitas yang ada saat ini *(as-is)* dan tingkat kapabilitas yang diinginkan *(to-be)* berdasarkan standar yang ditetapkan dalam COBIT 2019. Tujuan dari analisis ini adalah untuk memahami kesenjangan *(gap)* yang ada dalam proses-proses pengelolaan risiko dan keamanan TI di LAZNAS Baitulmaal Muamalat (BMM). Dengan mengetahui kesenjangan ini, organisasi dapat

merumuskan strategi dan rekomendasi perbaikan yang lebih tepat sasaran, baik dari segi kebijakan, sumber daya, atau prosedur yang perlu diperbaiki agar pengelolaan risiko TI lebih efektif dan efisien. Berikut identifikasi terhadap hasil audit serta analisis *gap* terhadap 3 domain yang terpilih.

1. Domain EDM 03 *(Ensure Risk Optimization)*

Identifikasi pada domain EDM 03 *(Ensure Risk Optimization)* menunjukkan hasil dari *Capability Level Test*, mencakup tiga aktivitas domain EDM 03 yaitu EDM 03.01 *(Evaluate Risk Management)*, EDM 03.02 *(Direct Risk Management)*, EDM 03.03 *(Monitor Risk Management)* dan berikut rekapannya.

Tabel 4.22. *Capability Level Test* EDM 03

No	Sub Domain	*Capability Level (as-is)*
1	EDM 03.01	3
2	EDM 03.02	2
3	EDM 03.03	4
Rata-Rata		3

EDM 03.01 dan EDM 03.03 menunjukkan level kapabilitas 3, yang berarti bahwa proses dalam sub domain ini sudah terdefinisi, jalan dan mapan penerapannya di dalam organisasi. Namun, masih ada ruang untuk perbaikan dalam hal pemantauan, seperti pemantauan tujuan utama matrik manajemen risiko terhadap targetnya. EDM 03.02 berada pada level 2, yang berarti bahwa organisasi sudah mulai langsung mengelola optimalisasi risiko, dengan optimalisasi pengelolaan risiko yang telah terdefinisi dengan baik, sedang untuk EDM 03.03 sudah berapa di level 4 yang mengartikan terkendali dan hasilnya dapat diprediksi dengan, ada kontrol statistik dan pengukuran kinerja. Rata-rata untuk domain ini adalah Level 3, menunjukkan bahwa secara umum, optimalisasi pengelolaan risiko

sudah berjalan dengan baik dan mapan, namun masih ada potensi untuk mencapai tingkat pengelolaan yang lebih maksimal. Selanjutnya perolehan gap EDM 03 *(Ensure Risk Optimization)* dapat dilihat pada Tabel 4.23. di bawah.

Tabel 4.23. Gap EDM 03

No	Sub Domain	*Capability Level (as-is)*	*Target Capability Level (to-be)*	Gap
1	EDM 03.01	3	3	0
2	EDM 03.02	2	3	1
3	EDM 03.03	4	4	0
Rata-Rata		3	3,33 = 3	0

Tabel 4.23. diatas memperlihatkan nilai gap pada sub domain EDM 03.01, EDM 03.02 & EDM 03.03. EDM 03.01 & EDM 03.03 masing – masing memiliki nilai gap 0, sedangkan EDM 02 memiliki nilai gap 1, hasil rata-rata menunjukkan *Capability Level (as-is)* dan *Target Capability Level (to-be)* sama-sama bernilai 3 sehingga nilai gap domain EDM 03 adalah 0, mengartikan tidak ada gap dan saat ini organisasi berada pada keadaan yang mapan. Kemudian dalam bentuk grafik dapat dilihat pada gambar 4.13. dibawah.

Gambar 4.13. Grafik EDM 03

2. Domain APO 12 *(Manage Risk)*

Identifikasi pada domain APO 12 *(Manage Risk)* menunjukkan hasil dari *Capability Level Test*, mencakup enam aktivitas domain APO 12 yaitu APO 12.01 *(Collect Data)*, APO 12.02 *(Analyze Risk)*, APO 12.03 *(Maintain A Risk Profile)*, APO 12.04 *(Articulate Risk)*, APO 12.05 *(Define A Risk Manaegement Action Portofolio)*, APO 12.06 *(Respond To Risk)* dan berikut rekapannya.

Tabel 4.24. *Capability Level Test* APO 12

No	Sub Domain	*Capability Level (as-is)*
1	APO 12.01	4
2	APO 12.02	5
3	APO 12.03	4
4	APO 12.04	3
5	APO 12.05	3
6	APO 12.06	5
Rata-Rata		4

APO 12.04 dan APO 12.05 menunjukkan level kapabilitas 3, yang berarti bahwa organisasi sudah dikelola secara kuantitatif dalam pengelolaan risiko, berdasarkan analisa, pemeliharaan, pengartikulasian pendefinisian yang mapan. APO 12.01 dan APO 12.03 menunjukkan level kapabilitas 4, sedangkan untuk APO 12.02 dan APO 12.06 berada di level 5 yang mengartikan proses dapat terus-menerus ditingkatkan melalui inovasi dan optimalisasi melalui evaluasi kinerja yang sistematis. Rata-rata untuk domain APO 12 ini adalah 4, menunjukkan bahwa pengelolaan risiko di organisasi ini berada pada level yang dapat diprediksi, proses terkendali dan hasilnya dapat diprediksi serta kontrol statistik dan pengukuran kinerja. Meskipun tetap ada area-area yang masih membutuhkan penyempurnaan

demi mencapai tingkat yang lebih baik. Selanjutnya perolehan gap APO 12 *(Manage Risk)* dapat dilihat pada tabel 4.25. di bawah.

Tabel 4.25. Gap APO 12

No	Sub Domain	*Capability Level (as-is)*	*Target Capability Level (to-be)*	Gap
1	APO 12.01	4	4	0
2	APO 12.02	5	5	0
3	APO 12.03	4	4	0
4	APO 12.04	3	4	1
5	APO 12.05	3	3	0
6	APO 12.06	5	5	0
Rata-Rata		4	4,16 = 4	0

Tabel 4.25. diatas memperlihatkan nilai gap pada sub domain APO 12.01, APO 12.02, APO 12.03, APO 12.04, APO 12.05, APO 12.06 . APO 12.01, APO 12.02, APO 12.03, APO 12.05, APO 12.06 memiliki nilai gap 0, sedangkan APO 12.04 memiliki nilai gap 1, hasil rata-rata menunjukkan *Capability Level (as-is)* bernilai 4 sedangkan *Target Capability Level (to-be)* bernilai 4 sehingga nilai gap domain APO 12 adalah 0, mengartikan tidak ada gap dan saat ini organisasi berada pada keadaan yang pengelolaan risiko yang terkontrol dan terukur. Kemudian dalam bentuk grafik dapat dilihat pada gambar 4.14. dibawah.

Gambar 4.14. Grafik APO 12

3. Domain APO 13 (*Manage Security)*

Identifikasi pada domain APO 13 *(Manage Secutiry)* menunjukkan hasil dari *Capability Level Test*, mencakup tiga aktivitas domain APO 13 yaitu APO 13.01 *(Establish and Maintain an Information Security Management System (ISMS))*, APO 13.02 *(Define and Manage an Information Security and Privacy Risk Treatment Plan)*, APO 13.03 *(Monitor and Review The Information Security Management System (ISMS))* dan berikut rekapannya.

Tabel 4.26. *Capability Level Test* APO 13

No	Sub Domain	*Capability Level (as-is)*
1	APO 13.01	2
2	APO 13.02	3
3	APO 13.03	5
Rata-Rata		3,33 = 3

APO 13.01 berada pada Level 2, yang menunjukkan bahwa proses terkait pembangunan dan pemeliharaan manajemen keamanan TI telah dikelola. APO 13.02 berada pada level 3 yang menunjukkan bahwa pendefinisian dan pengelolaan

manajemen keamanan sudah mapan. APO 13.03 berada pada level 5, yang berarti bahwa pemantauan dan peninjauan terkait manajemen keamanan sudah dapat ditingkatkan melalui inovasi dan optimalisasi. Walau masih ada area yang membutuhkan peningkatan seperti penentuan cara mengukur efektivitas praktik manajemen keamanan yang digunakan. Rata-rata untuk domain ini adalah 3, yang menunjukkan bahwa meskipun ada area yang masih perlu peningkatan namun secara umum pengelolaan keamanan sudah dianggap bisa mapan. Selanjutnya perolehan gap APO 13 *(Manage Security)* dapat dilihat pada Tabel 4.27. di bawah.

Tabel 4.27. Gap APO 13

No	Sub Domain	*Capability Level (as-is)*	*Target Capability Level (to-be)*	Gap
1	APO 13.01	2	2	0
2	APO 13.02	3	4	1
3	APO 13.03	5	5	0
Rata-Rata		3,33 = 3	3,66 = 4	1

Tabel 4.27. diatas memperlihatkan nilai gap pada sub domain APO 13.01, APO 13.02 & APO 13.03. APO 13.01 & APO 13.03 memiliki nilai gap 0, sedangkan APO 13.02 memiliki nilai gap 1, dengan *Capability Level (as-is)* bernilai 3 dan *Target Capability Level (to-be)* bernilai 4, menggambarkan adanya gap sebesar 1 sehingga organisasi perlu mengoptimalkan proses manajemen keamanan TI dengan cara yang lebih inovatif dan berkelanjutan.

Gambar 4.15. Grafik APO 13

4.3.2. Rekapitulasi Gap

Rekapitulasi *capability level* EDM 03 *(Ensure Risk Optimization)*, APO 12 *(Manage Risk)* & APO 13 *(Manage Secutiry)* dan nilai gap dapat dilihat pada Tabel 4.28. dibawah.

Tabel 4.28. Gap Domain

No	Domain	*Capability Level (as-is)*	*Capability Level (to-be)*	Gap
1	EDM 03	3	3	0
2	APO 12	4	4	0
3	APO 13	3	4	1
Rata-Rata		3,33 = 3	3,66 = 4	1

Rata - rata gap untuk ketiga domain ini adalah 1, yang menunjukkan bahwa secara keseluruhan LAZNAS Baitulmaal Muamalat (BMM) sudah berada pada tingkat kapabilitas yang baik, tetapi masih memiliki ruang untuk peningkatan agar mencapai tingkat kapabilitas yang lebih tinggi. Gap ini mengindikasikan bahwa langkah-langkah perbaikan yang terencana dan strategis dapat membantu

organisasi untuk mengoptimalkan pengelolaan risiko TI dan keamanan secara lebih efektif.

4.3.3. Area Perbaikan Prioritas

Berdasarkan hasil analisis tingkat kapabilitas pada setiap domain, diketahui bahwa terdapat satu domain yang masih menunjukkan adanya gap, yaitu APO13 *(Manage Security)* dengan gap sebesar 1. Hal ini menunjukkan bahwa pengelolaan keamanan informasi di LAZNAS Baitulmaal Muamalat masih memerlukan peningkatan untuk mencapai level kapabilitas yang ditargetkan. Sementara itu, domain EDM03 *(Ensure Risk Optimization)* dan APO12 *(Manage Risk)* secara keseluruhan telah mencapai tingkat kapabilitas yang ditetapkan. Namun, jika dilihat dari rata-rata keseluruhan domain, masih terdapat gap sebesar 1, yang mengindikasikan perlunya peningkatan lebih lanjut secara umum. Selain itu, berdasarkan evaluasi pada tingkat sub domain, terdapat empat sub domain yang masih memiliki gap sebesar satu tingkat terhadap target kapabilitas yang ditetapkan, yaitu :

a. EDM 03.02 *(Direct Risk Management)*

   Menekankan peran pimpinan dalam mengarahkan dan mengawasi proses manajemen risiko organisasi. Peningkatan diperlukan untuk memastikan pengambilan keputusan risiko dilakukan secara konsisten, terstruktur, dan selaras dengan tujuan strategis.

b. APO 12.01 *(Collect Data)*

Berfokus pada pengumpulan data risiko secara sistematis sebagai dasar analisis. Perbaikan dibutuhkan agar data yang dihimpun lebih akurat dan terdokumentasi dengan baik, sehingga penilaian risiko dapat dilakukan secara lebih tepat.

c. APO 12.04 *(Articulate Risk)*

Berkaitan dengan penyampaian hasil analisis risiko kepada pemangku kepentingan. Peningkatan diperlukan agar informasi risiko dapat dikomunikasikan secara lebih jelas dan informatif untuk mendukung keputusan yang lebih efektif.

d. APO 13.02 *(Define and Manage an Information Security and Privacy Risk Treatment Plan)*

Mencakup penyusunan dan pengelolaan rencana keamanan informasi dan privasi. Penguatan diperlukan agar kontrol keamanan dapat direncanakan dan diterapkan secara lebih terarah dan sesuai kebutuhan.

Keempat sub domain tersebut ditetapkan sebagai prioritas perbaikan karena memiliki kontribusi strategis terhadap efektivitas tata kelola risiko TI dan keamanan informasi. Penetapan ini mempertimbangkan urgensi proses, tingkat dampak terhadap tujuan organisasi, serta keterkaitan dengan proses lainnya dalam kerangka kerja COBIT 2019. Area perbaikan prioritas ini menjadi salah satu dasar dalam penyusunan roadmap peningkatan *capability level* yang akan dibahas pada bagian selanjutnya.

4.4. Roadmap Peningkatan *Capability Level*

Roadmap peningkatan *capability level* sebagai langkah strategis untuk mengarahkan proses perbaikan dan peningkatan pengelolaan risiko TI berdasarkan hasil identifikasi gap dan area perbaikan pada bagian sebelumnya. Roadmap ini dirancang untuk memberikan panduan yang jelas, mulai dari penetapan *milestone*, formulasi rekomendasi, penentuan prioritas implementasi, hingga penyusunan garis waktu pelaksanaan yang terukur. Melalui roadmap ini, proses peningkatan kapabilitas dapat dilaksanakan secara terencana dan bertahap, sehingga sesuai urgensi dan kebutuhan organisasi.

4.4.1. *Milestone*

Sebagai tindak lanjut dari hasil identifikasi gap dan area perbaikan pada bagian sebelumnya, diperlukan arah pengembangan yang berkesinambungan untuk memastikan perbaikan dan peningkatan *capability level* pada pengelolaan risiko TI dapat dilaksanakan dengan benar. Oleh karena itu, dibuatlah *roadmap* peningkatan *capability level* yang berfungsi sebagai petunjuk atau peta jalan dalam proses penguatan level kapabilitas manajemen risiko TI dan keamanan informasi. *Roadmap* ini disajikan dalam bentuk diagram *fishbone*, yang dapat dilihat pada gambar 4.16. Model *fishbone* digunakan untuk menggambarkan hubungan antar elemen yang saling mendukung dalam proses penguatan pengelolaan risiko TI.

Gambar 4.16. *Milestone*

Gambar 4.16. memetakan enam *milestone* utama sebagai faktor penggerak peningkatan *capability level* organisasi. Setiap *milestone* diidentifikasi sebagai elemen kunci yang harus diperkuat untuk mendukung pencapaian target *capability level*. Berikut penjelasan enam *milestone* tersebut :

a. Governance & Leadership

Milestone ini berfokus pada penguatan arah dan struktur tata kelola risiko TI di level strategis organisasi. Penguatan dilakukan melalui penetapan arah strategis pengelolaan risiko TI yang selaras dengan tujuan bisnis, komitmen dan dukungan manajemen puncak, serta mekanisme pengawasan dan evaluasi yang terstandarisasi. Keberadaan kepemimpinan yang kuat merupakan prasyarat fundamental untuk memastikan bahwa risiko TI diperlakukan sebagai bagian dari pengambilan keputusan strategis dan bukan respons insidentil.

b. Risk Management Framework

Menekankan pentingnya kerangka kerja manajemen risiko yang terstruktur dan terdokumentasi. Poin penting dalam area ini meliputi standarisasi metodologi penilaian risiko, implementasi proses identifikasi dan penilaian risiko yang sistematis, serta penyusunan profil risiko yang konsisten dan dapat dijadikan dasar analisis. Kerangka kerja yang komprehensif memastikan bahwa setiap risiko dapat dipetakan, dinilai, dan dikendalikan secara efektif.

c. Information Security

Berfokus pada perlindungan aset informasi dan penerapan kebijakan keamanan informasi yang menyeluruh. Langkah utama mencakup penyusunan dan penerapan kebijakan keamanan informasi yang terpadu, pengaturan kontrol akses berdasarkan peran dan tanggung jawab, serta pengelolaan insiden keamanan secara terkoordinasi. Penguatan pada aspek keamanan informasi tidak hanya mendukung perlindungan data organisasi, tetapi juga menjaga kepercayaan dan integritas operasional.

d. Control Process

Milestone ini menitikberatkan pada penguatan proses operasional dan pengendalian internal agar proses manajemen risiko memiliki struktur dan tolok ukur evaluasi yang jelas. Area penguatan meliputi penyusunan dan penerapan SOP terkait risiko TI, pengukuran efektivitas kontrol secara berkala, serta kepatuhan terhadap standar dan regulasi yang berlaku. Kontrol proses yang kuat membantu memastikan implementasi manajemen risiko berjalan konsisten dan berorientasi perbaikan.

e. Technology & Integration

Mendorong pemanfaatan teknologi untuk mendukung efektivitas pengelolaan risiko. Elemen kunci meliputi integrasi sistem manajemen risiko berbasis teknologi, penggunaan dashboard dan data real-time untuk visualisasi dan pelaporan, serta monitoring otomatis untuk mempercepat respons terhadap risiko. Integrasi digital memungkinkan organisasi berpindah dari pendekatan manual menuju pengambilan keputusan berbasis data (data-driven risk decision).

f. People & Culture

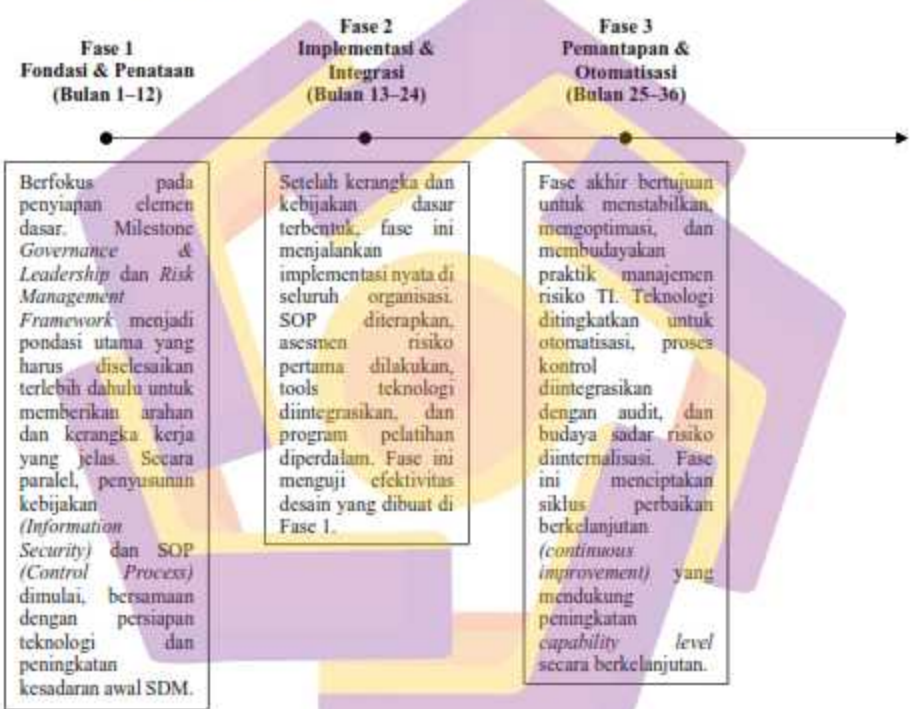
Milestone terakhir menekankan pentingnya kapabilitas SDM dan budaya organisasi dalam keberlanjutan implementasi pengelolaan risiko TI. Elemen penyusun meliputi pembangunan budaya sadar risiko di seluruh level organisasi, peningkatan kompetensi dan pelatihan keamanan informasi secara berkelanjutan, serta kolaborasi lintas unit dalam proses pengelolaan risiko TI. Faktor manusia adalah fondasi keberhasilan jangka panjang dan penentu terbentuknya siklus perbaikan berkelanjutan.

Keenam *milestone* tersebut membentuk rantai strategis yang terintegrasi dan saling melengkapi, sehingga menciptakan perjalanan peningkatan yang terstruktur dan terarah, sehingga menjadi panduan implementasi rekomendasi berbasis prioritas dan orientasi capaian, yang pada akhirnya mendukung pencapaian target *capability level*.

4.4.2. *Timeline*

Berdasarkan penjelasan mengenai enam milestone sebelumnya, bagian selanjutnya adalah menentukan rentang waktu dan tahapan makro untuk mencapai setiap target tersebut. Timeline ini menyajikan garis besar fase-fase pelaksanaan

yang menggambarkan pergeseran fokus strategis dari pembangunan dasar, pelaksanaan, hingga pemantapan budaya. Untuk memberikan gambaran menyeluruh tentang alur waktu ini, disusunlah sebuah *timeline* yang membagi perjalanan peningkatan selama 36 bulan ke dalam tiga fase utama, seperti yang tercantum dalam Gambar 4.17. berikut :



Gambar 4.17. *Timeline*

Dengan struktur tiga fase ini, peningkatan *capability level* tidak dilakukan secara serampangan atau reaktif, melainkan melalui sebuah perjalanan terencana yang memastikan setiap langkah diambil berdasarkan fondasi yang kokoh dari langkah sebelumnya. Pencapaian di setiap fase menjadi prasyarat sekaligus pemicu

bagi fase berikutnya, menciptakan momentum berkelanjutan menuju tingkat yang diharapkan. Berdasarkan peta waktu ini, dapat dirumuskan rekomendasi yang mendetail, memprioritaskan inisiatif-inisiatif sesuai dengan fokus setiap fase, hasil analisis gap dan temuan – temuan, guna memaksimalkan sumber daya dan dampak pencapaian.

4.4.3. Rekomendasi

Tahap selanjutnya adalah menyusun rekomendasi guna memperdalam *milestone* dan *timeline* yang telah ditetapkan, setelah menjabarkan *milestone* dan *timeline* yang dibuat, serta berdasarkan hasil analisis gap kapabilitas level dan temuan penelitian, berikut rekomendasi yang disusun untuk setiap sub domain baik untuk mempertahankan serta meningkatkan nilai kapabilitas level pada manajemen risiko TI dan keamanan di LAZNAS Baitulmaal Muamalat (BMM), yaitu dapat dilihat pada Tabel 4.29 di bawah.

Tabel 4.29. Rekomendasi

No	Domain	Sub Domain	Temuan	Rekomendasi Aktivitas Umum	Rekomendasi Berbasis Penerapan TI
1	EDM 03 (Memastikan Optimalisasi Risiko)	EDM 03.01 (Mengevaluasi Manajemen Risiko)	LAZNAS Baitulmaal Muamalat (BMM) memahami organisasi dan konteksnya terkait risiko TI yang dituangkan dalam Rencana Strategis (Renstra) 2019 - 2025, toleransi risiko yang dapat diambil oleh perusahaan serta tingkat toleransi terhadap penyimpangan dalam toleransi risiko.	LAZNAS Baitulmaal Muamalat (BMM) perlu mempertahankan pemahaman organisasi dan konteksnya mengenai risiko TI dalam Rencana Strategis (Renstra) & secara berkala meninjau dan memperbarui toleransi risiko yang tercantum dalam Renstra 2019-2025 untuk memastikan kebijakan tersebut tetap relevan dengan kondisi dan tantangan yang dihadapi organisasi, serta memastikan bahwa risiko yang dapat diterima sesuai dengan kemampuan dan tujuan strategis BMM.	Mengimplementasikan sistem dashboard digital yang terintegrasi dengan indikator dan target risiko TI dalam Renstra 2019 - 2025 untuk memantau perubahan tingkat risiko dan kesesuaiannya dengan batas toleransi yang ditetapkan, serta penggunaan sistem manajemen dokumen digital untuk mendukung pembaruan kebijakan risiko dan parameter toleransi risiko sesuai peninjauan rutin dalam Renstra.
			LAZNAS Baitulmaal Muamalat (BMM) mengevaluasi aktivitas dan faktor – faktor yang berpotensi menimbulkan risiko TI, memiliki personel yang terampil dalam mengatasai risiko TI. pelaksanaan aktivitas tersebut dilaksanakan terutama oleh manajer Kepatuhan, Risiko & Audit (KRA) yang bersinergi dengan manajer Tekonologi, Legal dan General Affairs (TLG).	LAZNAS Baitulmaal Muamalat (BMM) diharapkan terus konsisten mengevaluasi aktivitas dan faktor – faktor yang berpotensi menimbulkan risiko, serta memastikan bahwa evaluasi terhadap aktivitas dan faktor-faktor yang berpotensi menimbulkan risiko TI dilakukan secara rutin.	Aplikasi evaluasi risiko berbasis web dapat dimanfaatkan untuk mencatat, memantau dan memperbarui daftar risiko TI secara berkala, termasuk status evaluasi dan tindak lanjutnya, sehingga proses evaluasi rutin dapat dilakukan lebih terstruktur, terdokumentasi, dan mudah dikomunikasikan antar unit terkait.

		EDM 03.02 (Manajemen Risiko Langsung)	Penterjemahan strategi risiko TI kedalam praktiknya di LAZNAS Baitulmaal Muamalat (BMM) dilaksanakan langsung oleh manajer Teknologi, lalu komunikasi terkait manajemen risiko termasuk risiko TI kepada struktur atas dan bawah dilakukan oleh manajer Kepatuhan, Risiko & Audit (KRA), sedang implementasi mekanisme apabila terjadi risiko dilakukan oleh manajer Teknologi dengan berlandaskan SOP.	Pemahaman dan penerapan strategi risiko TI diharapakan dapat dipertahankan dengan memastikan komunikasi yang efektif antara pihak yang terlibat langsung yaitu manajer Teknologi dan manajer Kepatuhan, Risiko & Audit (KRA), serta seluruh level karyawan yang dalam hal ini sebagai pihak yang diberi pemahaman. Kemudian penting untuk memastikan bahwa mekanisme pelaksanaan risiko diterapkan secara konsisten, dengan mengikuti prosedur standar operasi (SOP) yang jelas agar setiap risiko yang teridentifikasi serta dapat segera ditangani dengan tepat oleh pihak yang berwenang.	Platform kolaborasi virtual dapat digunakan untuk mendukung komunikasi dan koordinasi penanganan risiko antara manajer Teknologi, manajer KRA, dan unit terkait, serta penerapan sistem pelaporan risiko berbasis TI agar setiap insiden atau potensi risiko dapat dilaporkan, ditindaklanjuti, dan dipantau sesuai SOP secara lebih cepat, terdokumentasi, dan terstruktur.
			Pelaporan terkait manajemen risiko dilakukan oleh manajer Kepatuhan, Risiko & Audit (KRA) ke pengambil keputusan tertinggi dalam jajaran eksekutif organisasi dalam hal ini adalah Direktur Eksekutif.	LAZNAS Baitulmaal Muamalat (BMM) perlu untuk terus memastikan bahwa pelaporan terkait manajemen risiko TI dilakukan secara terstruktur dan tepat waktu oleh manajer Kepatuhan, Risiko & Audit (KRA) kepada pengambil keputusan tertinggi, yaitu Direktur Eksekutif. Hal ini untuk memastikan bahwa keputusan strategis terkait risiko TI dapat diambil dengan cepat dan berdasarkan informasi yang akurat serta *up to date*.	Memanfaatkan sistem dashboard eksekutif dan pelaporan otomatis yang menyajikan informasi risiko TI secara real-time, terstruktur, dan dapat diakses kapan saja oleh Direktur Eksekutif.
			LAZNAS Baitulmaal Muamalat (BMM) belum menentukan pendekatan, metode serta teknik yang mendetail guna mengukur keberhasilan manajemen risiko TI, menimbang tingkat kesulitan risiko TI yang pernah dihadapi dan yang mungkin terjadi kedepan tidak terlalu memerlukan pendekatan, metode serta teknik yang mendetail, berhasil tidaknya manajemen risiko saat ini tertuang dalam *logbook* manajer Teknologi dan terkomunikasi ke pemangku kepentingan.	Diharapkan untuk menentukan dan mengadopsi pendekatan, metode, dan teknik yang terukur dan sistematis guna mengevaluasi keberhasilan manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Hal ini untuk mengidentifikasi tingkat keberhasilan terhadap manajemen risiko yang sudah dibuat.	Penerapan sistem penilaian keberhasilan manajemen risiko TI berbasis digital melalui pengukuran indikator kinerja risiko dan parameter pencapaian yang terdokumentasi dalam platform evaluasi risiko, sehingga hasil pengukuran keberhasilan manajemen risiko dapat dilakukan lebih terstruktur, transparan, serta mudah dilaporkan kepada pemangku kepentingan.
		EDM 03.03 (Memantau	LAZNAS Baitulmaal Muamalat (BMM) memberikan informasi terkait pembahasan manajemen risiko kepada dewan direksi	Informasi yang terkait manajemen risiko TI dapat kontinyu disampaikan secara jelas kepada Dewan Pengurus dan	Platform penyajian data manajemen risiko berbasis dashboard digital dapat digunakan untuk menampilkan perkembangan risiko, status

		Manajemen Risiko)	dalam hal ini di BMM adalah Dewan Pengurus & Dewan Pengawas Syariah melalui RKAT (Rapat Kerja Anggaran Tahunan) dari jajaran eksekutif diwakili oleh Direktur & Senior Manajemen (Kadiv, Manajer & Kepala Perwakilan.	Dewan Pengawas Syariah melalui Rapat Kerja Anggaran Tahunan (RKAT).	mitigasi, dan capaian kinerja risiko secara visual dan real-time sehingga memudahkan penyampaian informasi yang akurat dan komprehensif kepada Dewan Pengurus dan Dewan Pengawas Syariah dalam forum RKAT.
			Dalam memonitor dan memantau risiko di LAZNAS Baitulmaal Muamalat (BMM) dilaksanakan oleh manajer Teknologi bersinergi dengan manajer Kepatuhan, Risiko & Audit (KRA).	Senantiasa memastikan adanya koordinasi yang intens antara manajer Teknologi dan manajer Kepatuhan, Risiko & Audit (KRA) dalam memonitor dan memantau risiko TI.	Memakai platform monitoring risiko berbasis sistem untuk mendukung koordinasi *real-time* antara manajer Teknologi dan manajer Kepatuhan, Risiko & Audit (KRA) melalui pelacakan status risiko, pembaruan tindak lanjut, serta notifikasi otomatis sehingga monitoring risiko dapat dilakukan lebih cepat, transparan, dan terstruktur.
			Pemantauan risiko TI dilakukan oleh manajer Teknologi namun belum sepenuhnya optimal mengingat SDM yang terbatas hanya 1 orang menyebabkan analisis penyebab penyimpangan, tindakan perbaikan cukup memerlukan waktu.	LAZNAS Baitulmaal Muamalat (BMM) perlu mempertimbangkan untuk menambah sumber daya manusia (SDM) yang terlibat dalam pemantauan risiko TI guna meningkatkan efektivitas dan efisiensi proses tersebut. Dengan melibatkan lebih banyak personel yang terlatih, analisis penyebab penyimpangan dan tindakan perbaikan dapat dilakukan dengan lebih cepat dan tepat, sehingga meminimalkan keterlambatan dalam mengatasi risiko.	Penggunaan platform otomatisasi pemantauan risiko TI yang dapat membantu mengidentifikasi penyimpangan secara otomatis, menyediakan rekomendasi tindakan awal, serta memungkinkan kolaborasi lintas unit sehingga proses analisis tidak hanya bergantung pada satu personel serta mempercepat pengambilan keputusan mitigasi risiko, sehingga keterbatasan SDM bisa tutup dengan pemanfaatan platform yang tepat.
			Peninjauan atau pembahasan terkait manajemen risiko dengan dewan direksi atau pemangku kepentingan utama dalam hal ini dilaksanakan saat RKAT (Rapat Kerja Anggaran Tahunan) yang dilaksanakan setahun sekali.	Direkomendasikan mengalokasikan waktu khusus untuk melakukan peninjauan dan pembahasan terkait manajemen risiko dengan dewan direksi atau pemangku kepentingan utama, selain dilakukan pada saat RKAT (Rapat Kerja Anggaran Tahunan), sehingga pembahasan mengenai risiko bisa lebih spesifik tanpa di campur dengan pembahasan persoalan lain.	Memanfaatakan platform rapat virtual dan dashboard risiko untuk mendukung penjadwalan rapat evaluasi risiko secara berkala, serta penyediaan akses visual perkembangan risiko dan status mitigasi secara *real-time*, sehingga keputusan yang berkaitan dengan risiko TI dapat dibuat lebih cepat tanpa menunggu RKAT tahunan.
2	APO 12 (Mengelola Risiko)	APO 12.01 (Mengumpulkan Data)	Pengumpulan data risiko TI baik dari internal ataupun eksternal LAZNAS Baitulmaal Muamalat (BMM) termasuk survei sederhana dan analisis data historis serta pengalaman	Diharapkan LAZNAS Baitulmaal Muamalat (BMM) mempertahankan dan bila memungkinan memperkuat proses pengumpulan data risiko TI dengan memastikan bahwa data yang dikumpulkan, baik dari internal maupun	Memakai platform pengumpulan dan penyimpanan data risiko TI untuk mengelola data secara terstruktur dan terpusat sehingga proses analisis historis, identifikasi tren risiko, serta

			kerugian dilakukan oleh manajer Teknologi, dicatatkan pada *logbook* nya.	eksternal, dilakukan secara menyeluruh dan lengkap, kemudian manajer Teknologi perlu terus mendalami serta menganalisis data historis dan mencatat semua informasi yang relevan guna memudahkan pemantauan dan pengambilan keputusan yang lebih akurat dalam mengelola risiko TI.	dokumentasi penyebab risiko dapat dilakukan lebih cepat, akurat, dan tidak bergantung pada pencatatan manual.
			Analisis penyebab, faktor dan dampak risiko TI bagi bisnis dibuat dan di tuangkan dalam file presentasi oleh manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi serta diketahui oleh Kepatuhan, Risiko dan Audit (KRA) yang nantinya akan dipaparkan kepada Direktur Eksekutif dan pemangku kepentingan lainnya.	LAZNAS Baitulmaal Muamalat (BMM) perlu terus mempertahankan dan memastikan bahwa analisis mengenai penyebab, faktor, dan dampak risiko TI bagi bisnis dilakukan secara tepat dan didokumentasikan dengan jelas. Agar dapat mendukung pengambilan keputusan yang lebih baik dalam pengelolaan risiko TI oleh pemangku kepentingan utama.	Platform dokumentasi dan visualisasi analisis risiko dapat dimanfaatkan untuk menstandarisasi format penyajian penyebab, faktor, dan dampak risiko agar informasi yang dipaparkan lebih lengkap, komprehensif, dan mudah dipahami oleh pemangku kepentingan selama proses presentasi dan pengambilan keputusan.
		APO 12.02 (Analisis Risiko)	LAZNAS Baitulmaal Muamalat (BMM) melakukan analisis risiko dengan mempertimbangkan semua faktor risiko termasuk kerugian dan keuntungan yang bisa didapatkan. Manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi bersinergi dengan manajer Kepatuhan, Risiko dan Audit (KRA) secara rutin berkomunikasi guna memperbarui, mengidentifikasi dan mengevaluasi skenario terkait risiko TI.	Komunikasi antara manajer Teknologi, Legal & General Affairs (TLG), dan manajer Kepatuhan, Risiko, dan Audit (KRA) di LAZNAS Baitulmaal Muamalat guna memperbarui dan mengidentifikasi faktor-faktor risiko TI yang berkembang perlu terus dipertahankan dan penting untuk memastikan bahwa analisis risiko mencakup semua faktor.	Menggunakan platform kolaborasi digital untuk memfasilitasi pembaruan analisis risiko secara berkala, dan dashboard evaluasi risiko untuk mendukung penilaian faktor risiko serta dampaknya terhadap proses bisnis secara lebih sistematis dan transparan.
			Usulan untuk langkah respon risiko TI seringkali berawal dari manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi dengan sepengetahuan Kepatuhan, Risiko dan Audit (KRA) lalu dituangkan dalam bentuk PPT yang akan di paparkan pada pengambil keputusan utama dalam hal ini adalah Direktur Eksekutif.	Usulan untuk langkah respon risiko TI yang telah dibuat, disusun dan dipastikan bahwa setiap usulan dapat dipertimbangkan oleh Direktur Eksekutif, sebagai upaya memperkecil peluang atau dampak dari terjadinya risiko	Dapat memanfaatkan platform penyusunan dokumen rekomendasi risiko berbasis digital yang mendukung kolaborasi dan pelacakan perubahan, serta penggunaan media visualisasi untuk menyajikan usulan langkah respon risiko TI secara lebih sistematis dan mudah dipahami sehingga mempercepat proses persetujuan oleh Direktur Eksekutif.
			Analisis dampak bisnis termasuk opsi respon seperti menghindari, mengurangi, memitigasi,	Opsi respon seperti menghindari, mengurangi, dan memitigasi risiko, yang dapat mempengaruhi bisnis di	Memanfaatkan platform manajemen proyek dan risiko untuk membuat template standar analisis

			dan lainnya di LAZNAS Baitulmaal Muamalat (BMM) di buat oleh Manajer Teknologi, Legal & General Affairs (TLG) dan manajer Teknologi.	LAZNAS Baitulmaal Muamalat (BMM) diharapkan terus disusun secara komprehensif dan didokumentasikan dengan jelas.	dampak bisnis dan rencana respon risiko, memastikan konsistensi dan kelengkapan dokumentasi.
		APO 12.03 (Memelihara Profil Risiko)	LAZNAS Baitulmaal Muamalat (BMM) melakukan inventarisasi terhadap layanan TI dan sumber daya TI yang dimiliki guna menambah informasi dalam profil risiko, dilaksanakan oleh manajer Teknologi.	Inventarisasi terhadap layanan TI dan sumber daya TI di LAZNAS Baitulmaal Muamalat (BMM) diharapkan dapat terus dilakukan secara rutin, berkala dan terperinci oleh manajer Teknologi. Hal ini penting untuk memperbarui profil risiko dengan informasi yang akurat dan terbaru.	Sistem manajemen aset TI terpusat dapat diimplementasikan untuk mengotomatiskan pendataan dan pemantauan aset TI, serta menyinkronkannya dengan profil risiko secara *real time*.
			LAZNAS Baitulmaal Muamalat (BMM) memiliki perencanaan atau skenario yang digunakan untuk meminimalisir terjadinya risiko yang dituangkan dalam bentuk SOP.	LAZNAS Baitulmaal Muamalat (BMM) perlu memastikan bahwa perencanaan atau skenario yang digunakan untuk meminimalkan risiko TI ditinjau dan diperbarui secara berkala. Lalu memastikan skenario tersebut dituangkan dalam bentuk SOP yang jelas dan mudah diikuti, agar langkah-langkah mitigasi risiko dapat diimplementasikan dengan efektif dan efisien oleh seluruh pihak terkait.	Menggunakan sistem manajemen dokumen terpusat dengan fitur kontrol versi dan notifikasi untuk mengelola siklus hidup SOP, memastikan semua pihak selalu mengakses versi terbaru dan tinjauan berkala tidak terlewat
			LAZNAS Baitulmaal Muamalat (BMM) menangkap perisitiwa risiko yang pernah terjadi di masa lalu kemudian di catatkan dalam profil risiko dalam bentuk logbook milik manajer Teknologi.	Risiko TI yang pernah terjadi di masa lalu diharapkan konsisten dicatat secara terstruktur dan detail oleh manajer Teknologi, data ini penting untuk analisis profil risiko yang lebih akurat, serta untuk membantu dalam merencanakan langkah mitigasi dan mengantisipasi risiko serupa di masa depan.	Mengimplementasikan sistem pencatatan insiden dan basis pengetahuan risiko terpusat untuk menggantikan logbook fisik, guna memastikan konsistensi, kelengkapan data, dan kemudahan analisis historis.
		APO 12.04 (Mengartikulasikan Risiko)	Di LAZNAS Baitulmaal Muamalat (BMM) pelaporan hasil analisis risiko kepada pemangku kepentingan, laporan mencakup potensi kerugian dan keuntungan, serta terkait kategori dampak lainnya. Dilaporkan oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi yang bersinergi dengan manajer Kepatuhan, Risiko & Audit (KRA) kepada pemangku kepentingan dalam hal ini adalah Direktur Eksekutif.	Laporan hasil analisis risiko TI yang mencakup potensi kerugian, keuntungan, serta kategori dampak lainnya perlu disusun oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi secara jelas dan terperinci agar memuat informasi yang utuh bagi pemangku kepentingan atau pengambil keputusan Direktur Eksekutif LAZNAS Baitulmaal Muamalat (BMM).	Mengaplikasikan platform yang memiliki dashboard dan *business intelligence* yang terintegrasi dengan data risiko untuk menghasilkan laporan eksekutif yang visual, interaktif, dan *real time*, menggantikan laporan manual yang statis.
			Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi memberikan	Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi perlu mempertahankan pemberian	Mengembangkan portal atau dashboard risiko TI interaktif yang dapat diakses secara terpusat oleh

			pemahaman mengenai profil risiko TI yang ada kepada pemangku kepentingan.	pemahaman mengenai profil risiko TI yang ada kepada majaner Kepatuhan, Risiko & Audit (KRA), penyampaian pemahaman dan informasi tersebut selanjutnya diteruskan secara jelas kepada pengambil keputusan sehingga pengambil keputusan yaitu Direktur Eksekutif dapat memahami kondisi nyata risiko yang dihadapi dan dapat membuat keputusan yang tepat.	semua pemangku kepentingan, untuk memvisualisasikan profil risiko secara real-time dan menyediakan konteks yang jelas.
			Dalam melakukan audit LAZNAS Baitulmaal Muamalat (BMM) belum pernah melibatkan pihak ke eksternal.	LAZNAS Baitulmaal Muamalat (BMM) perlu mempertimbangkan untuk melibatkan pihak ketiga yang independen dalam proses audit di masa mendatang. Hal ini dapat membantu memastikan objektivitas, transparansi, dan memberikan perspektif yang lebih luas dalam menilai manajemen risiko TI di organisasi.	Mempersiapkan dan menyediakan akses terkelola *(managed access)* ke sistem dan data audit TI secara aman dan teraudit untuk pihak eksternal, guna mendukung efisiensi dan efektivitas pekerjaan auditor independen.
		APO 12.05 (Mendefinisikan Portofolio Tindakan Manajemen Risiko)	LAZNAS Baitulmaal Muamalat (BMM) menginventarisasi aktivitas kontrol ke dalam skenario manajemen risiko TI melalui manajer Teknologi & manajer Kepatuhan, Risiko & Audit (KRA).	LAZNAS Baitulmaal Muamalat (BMM) melanjutkan dan memperkuat inventarisasi aktivitas kontrol yang ada dalam skenario manajemen risiko TI, dengan memastikan bahwa proses ini dilakukan secara lebih mendalam dan sistematis oleh pihak yang berwenang yaitu manajer Teknologi, manajer Teknologi, *Legal & General Affairs* & manajer Kepatuhan, Risiko & Audit (KRA), sehingga kontrol yang diterapkan mampu mengatasi potensi risiko dengan tepat.	Mengimplementasikan sistem terpusat untuk memetakan dan mengelola hubungan antara risiko TI, kontrol, dan kepatuhan secara *real time*, menggantikan pendataan manual yang tersebar.
			Setiap bagian di LAZNAS Baitulmaal Muamalat (BMM) memiliki peran dalam memantau dan menangani risiko TI sesuai tanggung jawab masing-masing, pengarahan diberikan oleh manajer Teknologi.	Setiap level karyawan pada bagian masing – masing yang terlibat dalam memantau dan menangani risiko TI di LAZNAS Baitulmaal Muamalat (BMM) diharapkan memiliki pemahaman yang jelas mengenai peran dan tanggung jawab masing-masing.	Membuat portal terpusat yang berisi matriks tanggung jawab (*RACI Chart)* interaktif dan modul e-learning singkat tentang peran setiap posisi dalam manajemen risiko TI.
			Proyek atau perencanaan di LAZNAS Baitulmaal Muamalat (BMM) dalam rangka mengatasi risiko TI dirancang oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi, dengan mempertimbangan faktor-faktor yang ada.	Mempertahankan dan bila diperlukan meningkatkan proyek atau perencanaan yang dirancang oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi untuk mengatasi risiko TI, dilakukan dengan mempertimbangkan faktor-faktor yang ada, agar risiko TI semakin minin.	Aplikasi manajemen proyek yang terintegrasi dengan sistem manajemen risiko dapat dimanfaatkan untuk merencanakan, melacak, dan mengevaluasi efektivitas proyek-proyek mitigasi risiko TI.
			Dalam merespon risiko LAZNAS Baitulmaal Muamalat (BMM) memiliki langkah-langkah	Langkah-langkah dalam merespon risiko yang telah dituangkan dengan jelas dalam bentuk SOP diharapkan	Menggunakan sistem workflow automation untuk mengotomatiskan eksekusi SOP saat insiden risiko

		APO 12.06 (Merespon Risiko)	dalam bentuk SOP yang dapat dijalankan ketika suatu peristiwa risiko terjadi.	dapat dijalankan secara efektif oleh pihak yang bertanggung jawab, ketika suatu peristiwa risiko terjadi LAZNAS Baitulmaal Muamalat (BMM).	terjadi, memastikan respons yang cepat dan konsisten sesuai prosedur.
			LAZNAS Baitulmaal Muamalat (BMM) melalu manajer Teknologi dalam *logbook* mencatat kerugian akibat risiko yang pernah terjadi di masa lalu untuk mengetahui penyebab utamanya, sehingga bisa dijadikan sebagai bahan pertimbangan menyusun langkah antisipasi risiko di masa mendatang.	Setiap kerugian akibat risiko TI yang terjadi di masa lalu diharapkan dapat konsisten dicatat dengan lengkap dan terperinci oleh manajer Tekonologi. Informasi tersebut dapat digunakan untuk menganalisis penyebab utama terjadinya risiko, sehingga menjadi bahan pertimbangan dalam menyusun langkah antisipasi dan mitigasi risiko yang lebih efektif di masa depan.	Sistem manajemen insiden dan problem yang terintegrasi dapat diimplementasikan untuk mencatat kerugian, menganalisis akar penyebab *(Root Cause Analysis/RCA)*, dan membangun basis pengetahuan mitigasi risiko TI.
			LAZNAS Baitulmaal Muamalat (BMM) mengkomunikasikan setiap hal yang berkaitan dengan manajemen risiko kepada pemangku kepentingan di level eksekutif yang tertinggi dalam hal ini adalah Direktur Eksekutif.	Mempertahankan komunikasi informasi terkait manajemen risiko TI secara jelas dan tepat waktu kepada pemangku kepentingan di level eksekutif, terutama Direktur Eksekutif. Hal ini penting agar keputusan terkait pengelolaan risiko dapat diambil dengan cepat dan berdasarkan informasi yang akurat serta lengkap.	Sistem dashboard eksekutif dan notifikasi otomatis yang menyajikan informasi risiko TI secara *real time* dan terpusat dapat dimanfaatkan untuk mendukung pengambilan keputusan yang cepat.
3	APO 13 (Mengelola Keamanan)	APO 13.01 (Membangun dan Memelihara Sistem Manajemen Keamanan Informasi)	LAZNAS Baitulmaal Muamalat (BMM) menentukan ruang lingkup dan batasan sistem manajemen keamanan informasi, serta menyesuaikannya dengan karakteristik perusahaan dan teknologi yang digunakan, tertuang dalam Renstra (Rencana Strategis) 2019-2025.	LAZNAS Baitulmaal Muamalat (BMM) diharapkan konsisten mencantumkan bahasan mengenai sistem keamanan informasi di dalam renstra-resntra berikutnya,mengingat pentingnya keamanan sistem informasi di dalam organisasi.	Menggunakan platform tata kelola TI *(IT Governance)* untuk mengintegrasikan tujuan keamanan informasi ke dalam perencanaan strategis organisasi dan memantau pencapaiannya.
			Menyelaraskan batasan sistem keamanan informasi sesuai dengan kebijakan dan kondisi perusahaan, serta menyampaikan batasan tersebut kepada seluruh bagian yang terlibat baik peran, tanggung jawab & batasan dalam pengelolaan keamanan informasi, dalam persoalan keamanan sistem informasi di LAZNAS Baitulmaal Muamalat (BMM), di kelola oleh manajer Teknologi, Legal & General Affairs (TLG).	Manajer Teknologi, Legal & General Affairs (TLG) senantiasa memastikan bahwa batasan sistem keamanan informasi diselaraskan dengan kebijakan dan kondisi perusahaan, serta disosialisasikan dengan jelas kepada seluruh bagian yang terlibat, setiap peran dan tanggung jawab dalam pengelolaan keamanan informasi dipahami dengan baik oleh seluruh pihak terkait agar dapat menjalankan sistem keamanan informasi dengan benar.	Membuat portal kebijakan keamanan informasi terpusat dan sistem manajemen akses yang mencerminkan batasan keamanan secara otomatis.

		APO 13.02 (Metapkan dan Mengelola Keamanan Informasi dan Merencanakan Penanganan Risiko Privasi)	LAZNAS Baitulmaal Muamalat (BMM) khusunya Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi & majaner Kepatuhan, Risiko & Audit (KRA), menyusun dan memperbarui rencana penanganan risiko TI dan keamanan informasi yang mendukung tujuan perusahaan, serta mencatat komponen-komponen solusi yang diperlukan.	Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi & majaner Kepatuhan, Risiko & Audit (KRA) terus konsisten memperbarui rencana penanganan risiko keamanan informasi yang mendukung tujuan perusahaan, agar meminimalkan ancaman terhadap sistem keamanan informasi.	Sistem manajemen risiko keamanan siber *(Cyber Risk Management)* yang terintegrasi dapat dimanfaatkan untuk otomatisasi pemantauan ancaman dan pembaruan rencana penanganan risiko TI.
			Setiap orang di LAZNAS Baitulmaal Muamalat (BMM) berhak memberikan masukan untuk desain dan pengembangan solusi keamanan.	Diharapakan selalu mendorong partisipasi aktif dari setiap orang di dalam LAZNAS Baitulmaal Muamalat (BMM) untuk memberikan masukan terkait desain dan pengembangan solusi keamanan. Dengan melibatkan seluruh pihak dalam proses ini, diharapkan dapat tercipta solusi yang lebih relevan guna mengatasi berbagai potensi risiko keamanan yang dihadapi oleh organisasi.	Menyediakan saluran kolaborasi digital yang terstruktur dan mudah diakses untuk pengumpulan dan evaluasi masukan dari seluruh karyawan terkait solusi keamanan.
			LAZNAS Baitulmaal Muamalat (BMM) memilikli program pelatihan untuk meningkatkan kesadaran terkait keamanan dan privasi yang diadakan oleh manajer Teknologi.	LAZNAS Baitulmaal Muamalat (BMM) mempertahankan & mengembangkan program pelatihan terkait keamanan dan privasi yang diadakan, mencakup seluruh level karyawan untuk meningkatkan kesadaran terhadap pentingnya perlindungan data dan penerapan kebijakan keamanan yang tepat.	Platform *Learning Management System (LMS)* khusus keamanan siber dapar digunakan untuk menyelenggarakan pelatihan berkelanjutan, simulasi phishing, dan tracking progress kesadaran keamanan karyawan.
			LAZNAS Baitulmaal Muamalat (BMM) belum merinci bagaimana cara mengukur bahwa sudah sejauh mana praktik manajemen yang dipilih efektif.	LAZNAS Baitulmaal Muamalat (BMM) perlu menyusun dan menetapkan metode yang jelas untuk mengukur efektivitas praktik manajemen keamanan informasi yang diterapkan. Hal ini dapat dilakukan dengan menentukan indikator kinerja yang terukur dan dilanjutkan dengan melakukan evaluasi secara berkala terhadap penerapan manajemen yang telah dipilih, untuk memastikan bahwa tindakan yang diambil tepat.	Mengimplementasikan platform *continuous security monitoring* dan *Governance, Risk Management, & Compliance* (GRC) untuk mengotomasi pengukuran KPI keamanan, *compliance scoring*, dan pelaporan efektivitas kontrol keamanan.
		APO 13.03 (Memantau dan Meninjau Sistem	LAZNAS Baitulmaal Muamalat (BMM) melalui manajer Teknologi meninjau secara rutin efektivitas sistem keamanan dan	Manajer Teknologi melanjutkan dan memperkuat proses peninjauan rutin terhadap efektivitas sistem keamanan. Proses ini harus mencakup evaluasi menyeluruh terhadap	Platform *Security Posture Management* dapat digunakan yang mana bisa memberikan visibilitas terus-menerus terhadap efektivitas kontrol keamanan dan keselarasan dengan tujuan bisnis.

		Manajemen Keamanan Informasi)	memastikan sistem tersebut berjalan sesuai kebijakan dan tujuan yang ditetapkan.	kebijakan yang ada, serta memastikan bahwa sistem keamanan yang diterapkan sesuai dengan tujuan organisasi.	
			Melakukan audit internal secara berkala yang dilakukan oleh manajer Teknologi dengan mengevaluasi dan memeriksa sistem keamanan guna memastikan bahwa semua aspek kemanan informasi tetap terjaga dan diperbaiki jika ada kekeliruan.	Mempertahankan audit internal yang dilakukan secara berkala oleh manajer Teknologi, dengan fokus pada evaluasi dan pemeriksaan sistem keamanan, untuk memastikan bahwa semua aspek keamanan informasi tetap terjaga dengan baik dan dapat diperbaiki segera jika ditemukan kekeliruan atau celah dalam sistem yang ada.	Menyediakan platform audit keamanan otomatis yang dapat melakukan scanning berkala, memeriksa compliance, dan menghasilkan laporan audit secara *real-time*.
			LAZNAS Baitulmaal Muamalat (BMM) mencatat peristiwa yang mempengaruhi kinerja sistem keamanan informasi dilakukan oleh manajer Teknologi lalu di catatkan pada *logbook* nya.	Setiap peristiwa yang mempengaruhi kinerja sistem keamanan informasi diharapkan senantiasa dicatat dengan detail oleh manajer Teknologi agar menjadi bahan penting untuk analisis lebih lanjut dan sebagai referensi untuk memperbaiki dan meningkatkan sistem keamanan informasi di masa depan.	*Sistem Security Information and Event Management* terpusat dimanfaatkan untuk mengumpulkan, menganalisis, dan menyimpan semua log keamanan secara otomatis dan terstruktur.
			Setiap orang di LAZNAS Baitulmaal Muamalat berhak memberi masukan terkait keamanan sistem termasuk pemeliharaan, rancangan, aktivitas pemantau sistem keamanan yang ada di organisasi.	LAZNAS Baitulmaal Muamalat (BMM) diharapkan konsisten mendorong setiap orang dalam organisasi untuk aktif memberikan masukan terkait keamanan sistem, meliputi pemeliharaan, perancangan, serta kegiatan pemantauan terhadap sistem keamanan yang ada, guna memastikan bahwa sistem keamanan yang diterapkan terus berkembang dan dapat mengatasi potensi ancaman dengan lebih efektif.	Membuat platform *crowdsourcing* keamanan siber internal yang memungkinkan karyawan melaporkan kelemahan, memberikan ide peningkatan, dan berpartisipasi dalam program bug bounty internal.

4.4.4. Prioritas & Implementasi Rekomendasi

Berdasarkan rekomendasi yang telah di susun maka selanjutnya adalah menetapkan prioritas guna menentukan rekomendasi mana saja yang perlu di implementasikan terlebih dahulu agar mencapai *Target Capability Level*, prioritas disusun berdasar rekomendasi, hasil identifikasi gap yang didapat antara *Capability Level (as-is)* dan *Target Capability Level (to-be)* serta area yang memerlukan perbaikan, dapat dilihat padat Tabel 4.30. dibawah.

Tabel 4.30. Prioritas & Implementasi Rekomendasi

No	Sub Domain	Rekomendasi Aktivitas Umum	Waktu Pengerjaan	Bentuk Tindakan	Rekomendasi Berbasis Penerapan TI	Alat	Pihak Terlibat
Nilai GAP 1							
1	APO 12.04	Laporan hasil analisis risiko TI yang mencakup potensi kerugian, keuntungan, serta kategori dampak lainnya perlu disusun oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi secara jelas dan terperinci agar memuat informasi yang utuh bagi pemangku kepentingan atau pengambil keputusan Direktur Eksekutif LAZNAS Baitulmaal Muamalat (BMM).	Setelah Risiko Terjadi (1 – 2 Minggu)	Menyusun Laporan Hasil Analisis Risiko TI	Mengaplikasikan platform yang memiliki dashboard dan *business intelligence* yang terintegrasi dengan data risiko untuk menghasilkan laporan eksekutif yang visual, interaktif, dan *real time*, menggantikan laporan manual yang statis.	• Microsoft Power BI terintegrasi baik dengan produk Microsoft lainnya, ideal untuk membuat dashboard visual yang menampilkan metrik risiko, tren, dan ringkasan dampak (kerugian/keuntungan) secara real-time untuk Direktur Eksekutif. • Tableau Platform visualisasi data yang powerful untuk membuat dashboard yang sangat interaktif dan mudah dipahami, memungkinkan analisis mendalam oleh manajemen.	Manajer Kepatuhan Risiko & Audit, Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)*, Direktur Eksekutif
		Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi perlu mempertahankan pemberian pemahaman mengenai profil risiko TI	Rutin (4 Bulan Sekali)	Mengkomunikasikan Profil Risiko TI Kepada	Mengembangkan portal atau dashboard risiko TI interaktif yang dapat diakses secara terpusat oleh semua pemangku	• Microsoft Power BI digunakan khusus untuk membuat dashboard eksekutif yang menampilkan status, level, dan tren risiko TI secara visual dan real-time. Memudahkan	Manajer Kepatuhan Risiko & Audit, Manajer Teknologi,

		yang ada kepada majaner Kepatuhan, Risiko & Audit (KRA), penyampaian pemahaman dan informasi tersebut selanjutnya diteruskan secara jelas kepada pengambil keputusan sehingga pengambil keputusan yaitu Direktur Eksekutif dapat memahami kondisi nyata risiko yang dihadapi dan dapat membuat keputusan yang tepat.		Pemangku Kepentingan	kepentingan, untuk memvisualisasikan profil risiko secara real-time dan menyediakan konteks yang jelas.	Direktur Eksekutif untuk memahami "kondisi nyata" secara cepat. • Microsoft SharePoint berfungsi sebagai portal terpusat dan repositori dokumen. Dashboard dari Power BI disematkan di sini, dan dilengkapi dengan dokumen pendukung seperti analisis mendalam, profil risiko lengkap, dan prosedur mitigasi yang dapat diakses oleh manajer KRA dan Teknologi. • Qlik Sense platform analytics yang memungkinkan pembuatan aplikasi dashboard interaktif, memudahkan eksplorasi data risiko secara mandiri untuk pemahaman yang lebih mendalam.	Manajer Teknologi, *Legal & General Affairs (TLG)*, Direktur Eksekutif
		LAZNAS Baitulmaal Muamalat (BMM) perlu mempertimbangkan untuk melibatkan pihak ketiga yang independen dalam proses audit di masa mendatang. Hal ini dapat membantu memastikan objektivitas, transparansi, dan memberikan perspektif yang lebih luas dalam menilai manajemen risiko TI di organisasi.	Rutin (1 Tahun Sekali)	Kerjasama Dengan Auditor Eksternal	Mempersiapkan dan menyediakan akses terkelola *(managed access)* ke sistem dan data audit TI secara aman dan teraudit untuk pihak eksternal, guna mendukung efisiensi dan efektivitas pekerjaan auditor independen.	• Microsoft 365 Compliance Manager alat untuk memetakan kepatuhan terhadap standar regulasi, menghasilkan laporan kesiapan audit, dan membagikan bukti kepatuhan secara aman kepada auditor eksternal melalui portal terpusat. • Varonis Data Security Platform solusi untuk memantau dan mengamankan akses data. Dapat memberikan akses *view-only* yang terbatas dan terawasi kepada auditor untuk menganalisis log akses dan aktivitas data tanpa mengganggu operasional.	Manajer Kepatuhan Risiko & Audit, Auditor Eksternal, Bagian lain yang di butuhkan Auditor Eksternal.
2	APO 13.02	Manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi & majaner Kepatuhan, Risiko & Audit (KRA) terus konsisten memperbarui rencana penanganan risiko keamanan informasi yang mendukung tujuan perusahaan, agar meminimalkan	Rutin (3 Bulan Sekali)	Memperbarui Perencanaan Keamanan Informasi	Sistem manajemen risiko keamanan siber *(Cyber Risk Management)* yang terintegrasi dapat dimanfaatkan untuk otomatisasi pemantauan ancaman dan pembaruan rencana penanganan risiko TI.	• Tenable.io platform manajemen kerentanan siber yang secara otomatis memindai, menilai risiko, dan merekomendasikan rencana penanganan berdasarkan tingkat keparahan ancaman. • Qualys VMDR solusi manajemen kerentanan dan respons ancaman yang terintegrasi untuk	Manajer Kepatuhan Risiko & Audit, Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)*

		ancaman terhadap sistem keamanan informasi.				mengidentifikasi risiko keamanan secara real-time dan membantu menyusun prioritas mitigasi.	
		Diharapkan selalu mendorong partisipasi aktif dari setiap orang di dalam LAZNAS Baitulmaal Muamalat (BMM) untuk memberikan masukan terkait desain dan pengembangan solusi keamanan. Dengan melibatkan seluruh pihak dalam proses ini, diharapkan dapat tercipta solusi yang lebih relevan guna mengatasi berbagai potensi risiko keamanan yang dihadapi oleh organisasi.	Rutin (3 Bulan Sekali)	Menyerap Solusi Terkait Keamanan Sistem	Menyediakan saluran kolaborasi digital yang terstruktur dan mudah diakses untuk pengumpulan dan evaluasi masukan dari seluruh karyawan terkait solusi keamanan.	• Microsoft Teams dapat membuat saluran *(channel)* khusus *"Security Improvement"* di platform kolaborasi yang sudah ada, tempat karyawan dapat memberikan ide, masukan, dan melaporkan potensi kerentanan keamanan. • User Voice platform umpan balik khusus yang memungkinkan karyawan mengajukan ide solusi keamanan, melakukan voting, dan tim TI dapat memberikan tanggapan serta status pengembangan.	Semua level karyawan
		LAZNAS Baitulmaal Muamalat (BMM) mempertahankan & mengembangkan program pelatihan terkait keamanan dan privasi yang diadakan, mencakup seluruh level karyawan untuk meningkatkan kesadaran terhadap pentingnya perlindungan data dan penerapan kebijakan keamanan yang tepat.	Rutin (3 Bulan Sekali)	Mengadakan Pelatihan Terkait Kemanan Privasi	Platform *Learning Management System (LMS)* khusus keamanan siber dapat digunakan untuk menyelenggarakan pelatihan berkelanjutan, simulasi phishing, dan tracking progress kesadaran keamanan karyawan.	• KnowBe4 platform pelatihan keamanan kesadaran terkemuka yang menyediakan konten pelatihan, simulasi serangan phishing, dan pelacakan metrik peningkatan kesadaran keamanan karyawan. • Curricula platform pelatihan keamanan siber yang menyenangkan dengan konten pelatihan berbasis cerita dan simulasi phishing yang mudah diikuti semua level karyawan.	Semua level karyawan
		LAZNAS Baitulmaal Muamalat (BMM) perlu menyusun dan menetapkan metode yang jelas untuk mengukur efektivitas praktik manajemen keamanan informasi yang diterapkan. Hal ini dapat dilakukan dengan menentukan indikator kinerja yang terukur dan dilanjutkan dengan melakukan evaluasi secara berkala terhadap penerapan manajemen yang	Rutin (1 Tahun Sekali)	Membuat Metode Evalusi Keberhasilan Manajemen Keamanan Informasi	Mengimplementasikan platform *continuous security monitoring* dan *Governance, Risk Management, & Compliance* (GRC) untuk mengotomasi pengukuran KPI keamanan, *compliance scoring*, dan pelaporan efektivitas kontrol keamanan.	• Security Scorecard platform peringkatan keamanan siber yang memberikan skor keamanan berbasis data eksternal dan metrik KPI yang terukur untuk mengevaluasi efektivitas program keamanan. • Drata platform otomasi compliance dan security posture management yang secara kontinu memantau kontrol keamanan dan menghasilkan laporan efektivitas terhadap framework standar seperti ISO 27001/NIST.	Manajer Kepatuhan Risiko & Audit (KRA)

		telah dipilih, untuk memastikan bahwa tindakan yang diambil tepat.					
3	EDM 03.02	Pemahaman dan penerapan strategi risiko TI diharapakan dapat dipertahankan dengan memastikan komunikasi yang efektif antara pihak yang terlibat langsung yaitu manajer Teknologi dan manajer Kepatuhan, Risiko & Audit (KRA), serta seluruh level karyawan yang dalam hal ini sebagai pihak yang diberi pemahaman. Kemudian penting untuk memastikan bahwa mekanisme pelaksanaan risiko diterapkan secara konsisten, dengan mengikuti prosedur standar operasi (SOP) yang jelas agar setiap risiko yang teridentifikasi, serta dapat segera ditangani dengan tepat oleh pihak yang berwenang.	Saat Risiko Terdeteksi & Terjadi	Pelatihan, Sosialiasi & Implementasi SOP	Platform kolaborasi virtual dapat digunakan untuk mendukung komunikasi dan koordinasi penanganan risiko antara manajer Teknologi, manajer KRA, dan unit terkait, serta penerapan sistem pelaporan risiko berbasis TI agar setiap insiden atau potensi risiko dapat dilaporkan, ditindaklanjuti, dan dipantau sesuai SOP secara lebih cepat, terdokumentasi, dan terstruktur.	• Microsoft Teams untuk kolaborasi komunikasi & koordinasi penanganan risiko secara terpusat. • ServiceNow Incident Management guna membuat pelaporan dan penanganan insiden risiko dengan workflow standar SOP	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)*, Manajer Kepatuhan, Risiko & Audit (KRA), Seluruh level karyawan
		LAZNAS Baitulmaal Muamalat (BMM) perlu untuk terus memastikan bahwa pelaporan terkait manajemen risiko TI dilakukan secara terstruktur dan tepat waktu oleh manajer Kepatuhan, Risiko & Audit (KRA) kepada pengambil keputusan tertinggi, yaitu Direktur Eksekutif. Hal ini untuk memastikan bahwa keputusan strategis terkait risiko TI dapat diambil dengan cepat dan berdasarkan informasi yang akurat serta *up to date*.	Saat Risiko Terdeteksi	Komunikasi Terkait Risiko TI Antar Pihak Terkait	Memanfaatkan sistem dashboard eksekutif dan pelaporan otomatis yang menyajikan informasi risiko TI secara real-time, terstruktur, dan dapat diakses kapan saja oleh Direktur Eksekutif.	• Tableau platform visualisasi data untuk membuat dashboard eksekutif interaktif yang menampilkan metrik risiko kunci, tren, dan status mitigasi secara real-time dan mudah dipahami. • Microsoft Power BI alat business intelligence untuk membuat laporan dan dashboard terstruktur yang terhubung langsung dengan sumber data risiko, memastikan informasi selalu akurat dan terkini.	Manajer Kepatuhan, Risiko & Audit (KRA), Direktur Eksekutif
		Diharapkan untuk menentukan dan mengadopsi pendekatan, metode, dan	Rutin	Membuat Metode	Penerapan sistem penilaian keberhasilan manajemen risiko	• RiskScore platform penilaian dan analisis kinerja risiko berbasis indikator untuk	Manajer Teknologi,

		teknik yang terukur dan sistematis guna mengevaluasi keberhasilan manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Hal ini untuk mengidentifikasi tingkat keberhasilan terhadap manajemen risiko yang sudah dibuat.	(1 Tahun Sekali)	Evalusi Keberhasilan Manajemen Risiko TI	TI berbasis digital melalui pengukuran indikator kinerja risiko dan parameter pencapaian yang terdokumentasi dalam platform evaluasi risiko, sehingga hasil pengukuran keberhasilan manajemen risiko dapat dilakukan lebih terstruktur, transparan, serta mudah dilaporkan kepada pemangku kepentingan.	mengukur efektivitas manajemen risiko dan memvisualisasikan capaian keberhasilan secara periodik.	Manajer Teknologi, *Legal & General Affairs (TLG)*, Manajer Kepatuhan Risiko & Audit (KRA), Auditor Eksternal.
Nilai GAP 0							
1	APO 12.01	Diharapkan LAZNAS Baitulmaal Muamalat (BMM) mempertahankan dan bila memungkinan memperkuat proses pengumpulan data risiko TI dengan memastikan bahwa data yang dikumpulkan, baik dari internal maupun eksternal, dilakukan secara menyeluruh dan lengkap, kemudian manajer Teknologi perlu terus mendalami serta menganalisis data historis dan mencatat semua informasi yang relevan guna memudahkan pemantauan dan pengambilan keputusan yang lebih akurat dalam mengelola risiko TI.	Rutin (3 Bulan Sekali) & Setelah Risiko Terjadi	Mengumpulkan Data Risiko TI	makai platform pengumpulan dan penyimpanan data risiko TI untuk mengelola data secara terstruktur dan terpusat sehingga proses analisis historis, identifikasi tren risiko, serta dokumentasi penyebab risiko dapat dilakukan lebih cepat, akurat, dan tidak bergantung pada pencatatan manual.	• Google Forms untuk mengumpulkan data risiko dari internal dan eksternal secara terstandar dan periodik. • Google Sheets untuk mengolah, memvisualisasikan, dan menyimpan data historis risiko yang terhubung langsung dengan input dari Google Forms.	Manajer Teknologi, Manajer Kepatuhan Risiko & Audit (KRA), Mitra Eksternal.
		LAZNAS Baitulmaal Muamalat (BMM) perlu terus mempertahankan dan memastikan bahwa analisis mengenai penyebab, faktor, dan dampak risiko TI bagi bisnis dilakukan secara tepat dan	Saat Risiko Terdeteksi & Rutin (3 Bulan Sekali)	Membuat Laporan Analisi Risiko TI	Platform dokumentasi dan visualisasi analisis risiko dapat dimanfaatkan untuk menstandarisasi format penyajian penyebab, faktor, dan dampak risiko agar	• Google Docs untuk penyusunan dan dokumentasi analisis risiko secara terstruktur yang dapat dikolaborasikan antar manajer. • Google Slides untuk menyajikan visualisasi hasil analisis penyebab, faktor, dan dampak	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)*.

		didokumentasikan dengan jelas. Agar dapat mendukung pengambilan keputusan yang lebih baik dalam pengelolaan risiko TI oleh pemangku kepentingan utama.			informasi yang dipaparkan lebih lengkap, komprehensif, dan mudah dipahami oleh pemangku kepentingan selama proses presentasi dan pengambilan keputusan.	risiko secara lebih sistematis dalam forum paparan risiko.	
2	APO 12.02	Komunikasi antara manajer Teknologi, *Legal & General Affairs (TLG)*, dan manajer Kepatuhan, Risiko, dan Audit (KRA) di LAZNAS Baitulmaal Muamalat guna memperbarui dan mengidentifikasi faktor-faktor risiko TI yang berkembang perlu terus dipertahankan dan penting untuk memastikan bahwa analisis risiko mencakup semua faktor.	Saat Risiko Terdeteksi & Rutin (3 Bulan Sekali)	Mengkomunikasikan Faktor Penyebab Risiko TI	Menggunakan platform kolaborasi digital untuk memfasilitasi pembaruan analisis risiko secara berkala, dan dashboard evaluasi risiko untuk mendukung penilaian faktor risiko serta dampaknya terhadap proses bisnis secara lebih sistematis dan transparan.	• Microsoft Teams sebagai paltform komunikasi dan kolaborasi rutin antar pemangku risiko. • Power BI untuk visualisasi indikator risiko, dampak, dan tren evaluasi yang dibahas melalui sesi koordinasi Teams.	Manajer Teknologi, *Legal & General Affairs (TLG)* & Manajer Kepatuhan Risiko & Audit (KRA)
		Usulan untuk langkah respon risiko TI yang telah dibuat, disusun dan dipastikan bahwa setiap usulan dapat dipertimbangkan oleh Direktur Eksekutif, sebagai upaya memperkecil peluang atau dampak dari terjadinya risiko.	Rutin (3 Bulan Sekali)	Menyusun & Menyampaikan Usulan	Dapat memanfaatkan platform penyusunan dokumen rekomendasi risiko berbasis digital yang mendukung kolaborasi dan pelacakan perubahan, serta penggunaan media visualisasi untuk menyajikan usulan langkah respon risiko TI secara lebih sistematis dan mudah dipahami sehingga mempercepat proses persetujuan oleh Direktur Eksekutif.	• Google Docs untuk menyusun, mengedit, dan mengkolaborasikan draft usulan respon risiko secara bersama-sama. • Google Slides untuk menyajikan visualisasi ringkas usulan respon risiko yang akan dipaparkan kepada Direktur Eksekutif	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG).*
		Opsi respon seperti menghindari, mengurangi, dan memitigasi risiko, yang dapat mempengaruhi bisnis di	Saat Risiko Terdeteksi	Menyusun Opsi Respon	Memanfaatkan platform manajemen proyek dan risiko untuk membuat template	• Trello sebagai board dan kartu dengan daftar periksa *(checklist)* terstruktur untuk memandu	Manajer Teknologi, Manajer

		LAZNAS Baitulmaal Muamalat (BMM) diharapkan terus disusun secara komprehensif dan didokumentasikan dengan jelas.			standar analisis dampak bisnis dan rencana respon risiko, memastikan konsistensi dan kelengkapan dokumentasi.	proses analisis dampak dan pemilihan opsi respon. Bersifat visual dan mudah digunakan. • ManRisk sebagai aplikasi manajemen risiko yang sudah ada, dengan menambahkan form input khusus untuk analisis dampak bisnis dan opsi respon, sehingga semua data tersimpan terpusat.	Teknologi, *Legal & General Affairs (TLG)* & Manajer Kepatuhan Risiko & Audit (KRA).
3	APO 12.03	Inventarisasi terhadap layanan TI dan sumber daya TI di LAZNAS Baitulmaal Muamalat (BMM) diharapkan dapat terus dilakukan secara rutin, berkala dan terperinci oleh manajer Teknologi. Hal ini penting untuk memperbarui profil risiko dengan informasi yang akurat dan terbaru.	Rutin (1 Tahun Sekali)	Menginventarisasi Layanan & Sumber Daya TI	Sistem manajemen aset TI terpusat dapat diimplementasikan untuk mengotomatiskan pendataan dan pemantauan aset TI, serta menyinkronkannya dengan profil risiko secara *real time*.	• Manage Engine Service Desk Plus sebagai *Suite all-in-one* yang memiliki modul IT Asset Management untuk melacak aset perangkat keras, lunak, dan kontrak secara detail dan terintegrasi dengan tiket layanan. • Snipe IT sebagai Aplikasi web sumber terbuka yang khusus dirancang untuk manajemen aset IT, memudahkan pelacakan, pembaruan, dan pelaporan aset secara rutin.	Manajer Teknologi
		LAZNAS Baitulmaal Muamalat (BMM) perlu memastikan bahwa perencanaan atau skenario yang digunakan untuk meminimalkan risiko TI ditinjau dan diperbarui secara berkala. Lalu memastikan skenario tersebut dituangkan dalam bentuk SOP yang jelas dan mudah diikuti, agar langkah-langkah mitigasi risiko dapat diimplementasikan dengan efektif dan efisien oleh seluruh pihak terkait.	Rutin (4 Bulan Sekali)	Meninjau & Membuat SOP	Menggunakan sistem manajemen dokumen terpusat dengan fitur kontrol versi dan notifikasi untuk mengelola siklus hidup SOP, memastikan semua pihak selalu mengakses versi terbaru dan tinjauan berkala tidak terlewat.	• Microsoft Share Point sebagai platform kolaborasi untuk menyimpan dan mengelola SOP dengan fitur persetujuan (approval workflow), notifikasi pembaruan, dan pelacakan versi. • Confluence untuk membuat, meninjau, dan menyebarluaskan SOP dengan antarmuka yang terstruktur dan mudah dicari.	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)* & Manajer Kepatuhan Risiko & Audit (KRA).
		Risiko TI yang pernah terjadi di masa lalu diharapkan konsisten dicatat secara terstruktur dan detail oleh manajer Teknologi, data ini penting untuk analisis profil risiko yang lebih akurat, serta untuk membantu dalam	Setelah Risiko Terjadi & Rutin (1 Tahun Sekali)	Mencatat Risiko TI Yang Pernah Terjadi	Mengimplementasikan sistem pencatatan insiden dan basis pengetahuan risiko terpusat untuk menggantikan logbook fisik, guna memastikan konsistensi, kelengkapan data,	• Service Now Incident Management sebagai modul khusus untuk mencatat, melacak, dan menganalisis setiap insiden risiko TI dengan detail yang terstruktur, serta membangun basis pengetahuan dari solusi yang telah berhasil	Manajer Teknologi & Manajer Kepatuhan, Risiko & Audit (KRA).

		merencanakan langkah mitigasi dan mengantisipasi risiko serupa di masa depan.			dan kemudahan analisis historis.	• Freshservice yaitu *platform IT service management* yang memiliki fitur manajemen insiden dan knowledge base terintegrasi, memudahkan pencatatan dan referensi ulang kejadian masa lalu.	
4	APO 12.05	LAZNAS Baitulmaal Muamalat (BMM) melanjutkan dan memperkuat inventarisasi aktivitas kontrol yang ada dalam skenario manajemen risiko TI, dengan memastikan bahwa proses ini dilakukan secara lebih mendalam dan sistematis oleh pihak yang berwenang yaitu manajer Teknologi, manajer Teknologi, *Legal & General Affairs* & manajer Kepatuhan, Risiko & Audit (KRA), sehingga kontrol yang diterapkan mampu mengatasi potensi risiko dengan tepat.	Rutin (1 Tahun Sekali)	Menginventarisasi Aktivitas Kontrol Risiko TI	Mengimplementasikan sistem terpusat untuk memetakan dan mengelola hubungan antara risiko TI, kontrol, dan kepatuhan secara *real time*, menggantikan pendataan manual yang tersebar.	• Standard Fusion platform *Governance, Risk Management, dan Compliance* (GRC) berbasis cloud yang dirancang khusus untuk memudahkan inventarisasi kontrol, penilaian risiko, dan manajemen bukti kepatuhan dalam satu tempat terpusat. • Logic Gate Risk Cloud aplikasi yang membantu membuat peta hubungan antara risiko, kontrol, dan proses bisnis secara visual, sehingga efektivitas kontrol dapat dipantau dan dinilai dengan sistematis.	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)* & Manajer Kepatuhan Risiko & Audit (KRA).
		Setiap level karyawan pada bagian masing – masing yang terlibat dalam memantau dan menangani risiko TI di LAZNAS Baitulmaal Muamalat (BMM) diharapkan memiliki pemahaman yang jelas mengenai peran dan tanggung jawab masing-masing.	Rutin (3 Tahun Sekali)	Sosialisasi Peran & Tanggung Jawab Terkait Risiko TI	Membuat portal terpusat yang berisi matriks tanggung jawab (*RACI Chart)* interaktif dan modul e-learning singkat tentang peran setiap posisi dalam manajemen risiko TI.	• Microsoft Share Point digunakan untuk membuat halaman portal terpusat yang berisi matriks RACI digital yang jelas, yang dapat diperbarui secara real-time dan diakses oleh semua karyawan. • Talent LMS *Platform Learning Management System* (LMS) untuk membuat dan mendistribusikan modul pelatihan singkat (micro-learning) tentang prosedur dan tanggung jawab penanganan risiko TI sesuai peran masing-masing.	Semua Level Karyawan
		Mempertahankan dan bila diperlukan meningkatkan proyek atau perencanaan yang dirancang oleh manajer Teknologi, Legal & General Affairs (TLG) & manajer Teknologi	Rutin (1 Tahun Sekali)	Membuat Proyek Manajemen Risiko TI Baru	Aplikasi manajemen proyek yang terintegrasi dengan sistem manajemen risiko dapat dimanfaatkan untuk merencanakan, melacak, dan	• Jira platform manajemen proyek yang powerful untuk membuat project timeline, memberikan penugasan, dan melacak progres implementasi rencana mitigasi risiko secara real-time oleh semua pihak terkait.	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs*

		untuk mengatasi risiko TI, dilakukan dengan mempertimbangkan faktor-faktor yang ada, agar risiko TI semakin minin.			mengevaluasi efektivitas proyek-proyek mitigasi risiko TI.	• Asana aplikasi manajemen kerja yang intuitif untuk merencanakan dan mengoordinasikan proyek mitigasi risiko, memastikan setiap langkah terpetakan dengan jelas dan tepat waktu.	*(TLG)* & Manajer Kepatuhan Risiko & Audit (KRA).
5	APO 12.06	Langkah-langkah dalam merespon risiko yang telah dituangkan dengan jelas dalam bentuk SOP diharapkan dapat dijalankan secara efektif oleh pihak yang bertanggung jawab, ketika suatu peristiwa risiko terjadi LAZNAS Baitulmaal Muamalat (BMM).	Saat Risiko Terjadi	Implementasi SOP	Menggunakan sistem workflow automation untuk mengotomatiskan eksekusi SOP saat insiden risiko terjadi, memastikan respons yang cepat dan konsisten sesuai prosedur.	• ServiceNow IT Service Management platform ITSM yang memiliki fitur workflow engine kuat untuk mengotomatiskan alur kerja respons risiko berdasarkan SOP, termasuk notifikasi otomatis ke pihak terkait dan eskalasi. • Kissflow platform workflow dan BPM yang mudah digunakan untuk mendigitalkan SOP respons risiko menjadi alur kerja terstruktur yang dapat dijalankan secara konsisten oleh tim.	Semua Level Karyawan
		Setiap kerugian akibat risiko TI yang terjadi di masa lalu diharapkan dapat konsisten dicatat dengan lengkap dan terperinci oleh manajer Tekonologi. Informasi tersebut dapat digunakan untuk menganalisis penyebab utama terjadinya risiko, sehingga menjadi bahan pertimbangan dalam menyusun langkah antisipasi dan mitigasi risiko yang lebih efektif di masa depan.	Setelah Risiko Terjadi & Rutin (1 Tahun Sekali)	Mencatat & Meninjau Risiko TI	Sistem manajemen insiden dan problem yang terintegrasi dapat diimplementasikan untuk mencatat kerugian, menganalisis akar penyebab *(Root Cause Analysis/RCA)*, dan membangun basis pengetahuan mitigasi risiko TI.	• Freshservice Problem Management modul khusus untuk mencatat insiden berulang dan melakukan analisis akar penyebab secara terstruktur, dilengkapi basis pengetahuan untuk menyimpan solusi permanen. • Jira Service Management Platform ITSM yang memiliki fitur problem management untuk melacak kerugian risiko, menganalisis pola, dan mendokumentasikan pelajaran yang dipetik *(Lessons Learned)*.	Manajer Teknologi
		Mempertahankan komunikasi informasi terkait manajemen risiko TI secara jelas dan tepat waktu kepada pemangku kepentingan di level eksekutif, terutama Direktur Eksekutif. Hal ini penting agar keputusan terkait pengelolaan risiko	Saat Risiko Terdeteksi & Rutin (3 Bulan Sekali)	Mengkomunikasikan & Menyampaikan Informasi	Sistem dashboard eksekutif dan notifikasi otomatis yang menyajikan informasi risiko TI secara *real time* dan terpusat dapat dimanfaatkan untuk mendukung pengambilan keputusan yang cepat.	• Microsoft Power BI membangun dashboard eksekutif interaktif yang menampilkan metrik risiko kunci, status mitigasi, dan tren secara visual, dapat diakses kapan saja oleh Direktur Eksekutif. • Klipfolio platform dashboard bisnis real-time yang dapat mengkonsolidasi data dari berbagai	Manajer Kepatuhan Risiko & Audit (KRA) & Direktur Eksekutif

		dapat diambil dengan cepat dan berdasarkan informasi yang akurat serta lengkap.				sumber dan mengirimkan notifikasi/peringatan otomatis ketika metrik risiko melebihi batas toleransi.	
6	APO 13.01	LAZNAS Baitulmaal Muamalat (BMM) diharapkan konsisten mencantumkan bahasan mengenai sistem keamanan informasi di dalam renstra-resntra berikutnya,mengingat pentingnya keamanan sistem informasi di dalam organisasi.	Rutin (5 Tahun Sekali)	Membuat Rencana Strategis (Renstra)	Menggunakan platform tata kelola TI *(IT Governance)* untuk mengintegrasikan tujuan keamanan informasi ke dalam perencanaan strategis organisasi dan memantau pencapaiannya.	• Service Now GRC platform terintegrasi untuk menyelaraskan strategi keamanan informasi dengan tujuan bisnis, serta memantau kepatuhan terhadap rencana strategis secara *real-time*. • iServer Suite alat tata kelola arsitektur perusahaan yang membantu memetakan dan menghubungkan rencana keamanan informasi dengan tujuan strategis organisasi secara visual.	Direktur Ekseckutif, Dewan Pengurus & Dewan Pengawas Syariah
		Manajer Teknologi, Legal & General Affairs (TLG) senantiasa memastikan bahwa batasan sistem keamanan informasi diselaraskan dengan kebijakan dan kondisi perusahaan, serta disosialisasikan dengan jelas kepada seluruh bagian yang terlibat, setiap peran dan tanggung jawab dalam pengelolaan keamanan informasi dipahami dengan baik oleh seluruh pihak terkait agar dapat menjalankan sistem keamanan informasi dengan benar.	Rutin (4 Bulan Sekali)	Sosialisasi Terkait Peran Dalam Pengelolaan Keamanan Informasi	Membuat portal kebijakan keamanan informasi terpusat dan sistem manajemen akses yang mencerminkan batasan keamanan secara otomatis.	• Microsoft SharePoint membuat portal terpusat untuk menyimpan dan menyebarluaskan dokumen kebijakan keamanan, batasan sistem, dan matriks tanggung jawab (RACI) yang dapat diakses semua karyawan. • Sail Point Identity IQ Platform manajemen identitas dan akses yang menerapkan batasan keamanan secara otomatis berdasarkan peran *(role-based access control)*, memastikan akses sesuai kebijakan.	Semua Level Karyawan
7	APO 13.03	Manajer Teknologi melanjutkan dan memperkuat proses peninjauan rutin terhadap efektivitas sistem keamanan. Proses ini harus mencakup evaluasi menyeluruh terhadap kebijakan yang ada, serta memastikan bahwa sistem	Rutin (1 Tahun Sekali)	Meninjau & Mengevaluasi Kebijakan Kemanan Sistem	Platform *Security Posture Management* dapat digunakan yang mana bisa memberikan visibilitas terus-menerus terhadap efektivitas kontrol keamanan dan keselarasan dengan tujuan bisnis.	• Rapid7 InsightVM platform manajemen kerentanan dan kepatuhan keamanan yang memberikan penilaian risiko terus-menerus, mengukur efektivitas kontrol keamanan, dan kesesuaiannya dengan kebijakan. • Crowd Strike Falcon Spotlight solusi assessment kerentanan berbasis cloud yang	Manajer Teknologi

		keamanan yang diterapkan sesuai dengan tujuan organisasi.				terintegrasi dengan *Endpoint Detection and Response* (EDR), memberikan visibilitas real-time terhadap exposure keamanan dan efektivitas kontrol endpoint.	
		Mempertahankan audit internal yang dilakukan secara berkala oleh manajer Teknologi, dengan fokus pada evaluasi dan pemeriksaan sistem keamanan, untuk memastikan bahwa semua aspek keamanan informasi tetap terjaga dengan baik dan dapat diperbaiki segera jika ditemukan kekeliruan atau celah dalam sistem yang ada.	Rutin (1 Tahun Sekali)	Melakukan Audit Risiko TI Dari Internal	Menyediakan platform audit keamanan otomatis yang dapat melakukan scanning berkala, memeriksa compliance, dan menghasilkan laporan audit secara *real-time*.	• Nessus Professional Scanner kerentanan komprehensif untuk melakukan audit keamanan internal secara otomatis, mendeteksi celah keamanan, dan memastikan kepatuhan terhadap standar keamanan. • OpenVAS solusi open-source untuk scanning kerentanan dan audit keamanan yang dapat dijadwalkan secara berkala untuk memeriksa seluruh infrastruktur TI.	Manajer Teknologi
		Setiap peristiwa yang mempengaruhi kinerja sistem keamanan informasi diharapkan senantiasa dicatat dengan detail oleh manajer Teknologi agar menjadi bahan penting untuk analisis lebih lanjut dan sebagai referensi untuk memperbaiki dan meningkatkan sistem keamanan informasi di masa depan.	Saat Ancaman Keamanan Terdeteksi	Mencatat Perisitiwa Yang Mempengaruhi Sistem Keamanan	*Sistem Security Information and Event Management* terpusat dimanfaatkan untuk mengumpulkan, menganalisis, dan menyimpan semua log keamanan secara otomatis dan terstruktur.	• Splunk Enterprise Security platform SIEM enterprise untuk agregasi log terpusat, deteksi ancaman, dan investigasi insiden keamanan dengan kemampuan analitik yang mendalam. • AlienVault OSSIMsSolusi SIEM *opensource* terintegrasi yang menyatukan fungsi monitoring keamanan, deteksi ancaman, dan manajemen log dalam satu platform.	Manajer Teknologi
		LAZNAS Baitulmaal Muamalat (BMM) diharapkan konsisten mendorong setiap orang dalam organisasi untuk aktif memberikan masukan terkait keamanan sistem, meliputi pemeliharaan, perancangan, serta kegiatan pemantauan terhadap sistem keamanan yang ada, guna memastikan bahwa sistem keamanan yang diterapkan terus berkembang dan	Saat Risiko Terdeteksi & Rutin (3 Bulan Sekali)	Membuat Forum Diskusi Untuk Menampung Masukan	Membuat platform *crowdsourcing* keamanan siber internal yang memungkinkan karyawan melaporkan kelemahan, memberikan ide peningkatan, dan berpartisipasi dalam program bug bounty internal.	• HackerOne platform manajemen kerentanan dan bug bounty yang dapat dikonfigurasi untuk program internal, memungkinkan karyawan melaporkan celah keamanan secara terstruktur dan anonim. • Bugcrowd platform crowdsourced security yang menyediakan portal pelaporan kerentanan dan program insentif untuk mendorong partisipasi aktif dalam meningkatkan keamanan sistem.	Semua Level Karyawan

		dapat mengatasi potensi ancaman dengan lebih efektif.					
8	EDM 03.01	LAZNAS Baitulmaal Muamalat (BMM) perlu mempertahankan pemahaman organisasi dan konteksnya mengenai risiko TI dalam Rencana Strategis (Renstra) & secara berkala meninjau dan memperbarui toleransi risiko yang tercantum dalam Renstra 2019-2025 untuk memastikan kebijakan tersebut tetap relevan dengan kondisi dan tantangan yang dihadapi organisasi, serta memastikan bahwa risiko yang dapat diterima sesuai dengan kemampuan dan tujuan strategis BMM.	Rutin (5 Tahun Sekali)	Membuat Rencana Strategis (Renstra)	Mengimplementasikan sistem dashboard digital yang terintegrasi dengan indikator dan target risiko TI dalam Renstra 2019 - 2025 untuk memantau perubahan tingkat risiko dan kesesuaiannya dengan batas toleransi yang ditetapkan, serta penggunaan sistem manajemen dokumen digital untuk mendukung pembaruan kebijakan risiko dan parameter toleransi risiko sesuai peninjauan rutin dalam Renstra.	• Power BI untuk visualisasi indikator risiko Renstra secara *real-time*. • Share Point sebagai penyimpanan terpusat pembaruan dokumen risiko Renstra.	Manajer Teknologi, Manajer Teknologi, *Legal & General Affairs (TLG)* & Manajer Kepatuhan Risiko & Audit (KRA), Direktur Eksekutif, Dewan Pengurus & Dewan Pengawas Syariah
		LAZNAS Baitulmaal Muamalat (BMM) diharapkan terus konsisten mengevaluasi aktivitas dan faktor – faktor yang berpotensi menimbulkan risiko, serta memastikan bahwa evaluasi terhadap aktivitas dan faktor-faktor yang berpotensi menimbulkan risiko TI dilakukan secara rutin.	Rutin (3 Bulan Sekali)	Mengevaluasi Penyebab Risiko TI	Aplikasi evaluasi risiko berbasis web dapat dimanfaatkan untuk mencatat, memantau dan memperbarui daftar risiko TI secara berkala, termasuk status evaluasi dan tindak lanjutnya, sehingga proses evaluasi rutin dapat dilakukan lebih terstruktur, terdokumentasi, dan mudah dikomunikasikan antar unit terkait.	• ManRisk sebagai platform manajemen risiko untuk pencatatan evaluasi risiko, monitoring status dan pelaporan tindak lanjut secara terintegrasi.	Manajer Teknologi
9	EDM 03.03	Informasi yang terkait manajemen risiko TI dapat kontinyu disampaikan secara jelas kepada Dewan Pengurus dan Dewan Pengawas Syariah melalui	Rutin (1 Tahun Sekali)	Sosialisasi Terkait Manajemen Risiko TI	Platform penyajian data manajemen risiko berbasis dashboard digital dapat digunakan untuk menampilkan perkembangan risiko, status	• Power BI sebagai dashboard visual untuk menampilkan laporan risiko, status mitigasi, tren historis, dan indikator kinerja risiko dalam format yang lebih informatif dan mudah dipresentasikan	Direktur Eksekutif, Dewan Pengurus & Dewan Pengawas Syariah

		Rapat Kerja Anggaran Tahunan (RKAT).			mitigasi, dan capaian kinerja risiko secara visual dan real-time sehingga memudahkan penyampaian informasi yang akurat dan komprehensif kepada Dewan Pengurus dan Dewan Pengawas Syariah dalam forum RKAT		
		Senantiasa memastikan adanya koordinasi yang intens antara manajer Teknologi dan manajer Kepatuhan, Risiko & Audit (KRA) dalam memonitor dan memantau risiko TI.	Saat Risiko Terdeteksi	Melakukan Komunikasi & Pemantaun Risiko TI	Memakai platform monitoring risiko berbasis sistem untuk mendukung koordinasi *real-time* antara manajer Teknologi dan manajer Kepatuhan, Risiko & Audit (KRA) melalui pelacakan status risiko, pembaruan tindak lanjut, serta notifikasi otomatis sehingga monitoring risiko dapat dilakukan lebih cepat, transparan, dan terstruktur.	• Jira Service Management, platform monitoring risiko dan insiden berbasis workflow dengan notifikasi otomatis dan tracking status tindak lanjut	Manajer Teknologi, Manajer Kepatuhan Risiko & Audit (KRA)
		LAZNAS Baitulmaal Muamalat (BMM) perlu mempertimbangkan untuk menambah sumber daya manusia (SDM) yang terlibat dalam pemantauan risiko TI guna meningkatkan efektivitas dan efisiensi proses tersebut. Dengan melibatkan lebih banyak personel yang terlatih, analisis penyebab penyimpangan dan tindakan perbaikan dapat dilakukan dengan lebih cepat dan tepat, sehingga meminimalkan keterlambatan dalam mengatasi risiko.	2 – 4 Minggu	Merekrut Kayawan Spesialisasi TI	Memanfaatkan platform otomatisasi pemantauan risiko TI yang dapat membantu mengidentifikasi penyimpangan secara otomatis, menyediakan rekomendasi tindakan awal, serta memungkinkan kolaborasi lintas unit sehingga proses analisis tidak hanya bergantung pada satu personel serta mempercepat pengambilan keputusan mitigasi risiko, sehingga	• Manage Engine OpManager sebagai platform otomatisasi monitoring risiko dan kinerja infrastruktur TI dengan notifikasi otomatis terhadap penyimpangan & dashboard pemantauan real-time	Manajer *Human Capital Management (HCM)*

					keterbatasan SDM bisa tutup dengan pemanfaatan platform yang tepat.		
		Direkomendasikan mengalokasikan waktu khusus untuk melakukan peninjauan dan pembahasan terkait manajemen risiko dengan dewan direksi atau pemangku kepentingan utama, selain dilakukan pada saat RKAT (Rapat Kerja Anggaran Tahunan), sehingga pembahasan mengenai risiko bisa lebih spesifik tanpa di campur dengan pembahasan persoalan lain.	Rutin (1 Tahun Sekali)	Membuat Forum Pembahasan Risiko TI	Memanfaatakan platform rapat virtual dan dashboard risiko untuk mendukung penjadwalan rapat evaluasi risiko secara berkala, serta penyediaan akses visual perkembangan risiko dan status mitigasi secara *real-time*, sehingga keputusan yang berkaitan dengan risiko TI dapat dibuat lebih cepat tanpa menunggu RKAT tahunan.	• Microsoft Teams sebagai media rapat khusus pembahasan risiko secara berkala. • Power BI untuk menampilkan dashboard perkembangan risiko dan status mitigasi yang dibahas melalui Teams	Direktur Eksekutif, Dewan Pengurus & Dewan Pengawas Syariah

4.5. Dampak & Evaluasi

Dampak yang dibahas pada bagian ini merujuk pada pengaruh yang dapat ditimbulkan dari penerapan rekomendasi. Analisis dampak dilakukan untuk menilai sejauh mana rekomendasi mampu memperkuat proses pengelolaan risiko TI pada area prioritas & secara keseluruhan. Selain itu, dimuat juga hasil evaluasi yang diperoleh melalui instrumen penilaian yang diberikan kepada pihak terkait, dengan tujuan untuk mengukur tingkat kejelasan, relevansi, dan kelayakan rekomendasi. Evaluasi ini menjadi aspek penting untuk memastikan bahwa rekomendasi yang disusun tidak hanya tepat sasaran, tetapi juga realistis untuk diimplementasikan.

4.5.1. Penguatan Pengelolaan Risiko TI

Penerapan rekomendasi yang telah dirumuskan bertujuan untuk memperkuat dan meningkatkan pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM) secara menyeluruh. Penguatan ini terwujud pada bagian – bagian yang selaras dengan domain dan rekomendasi yang diusulkan.

1. Penguatan Struktur Tata Kelola TI dan Akuntabilitas

Rekomendasi akan mentransformasi pendekatan tata kelola risiko TI dari yang bersifat insidental menjadi sistematis dan terintegrasi dengan strategi bisnis. Penyelarasan tolok ukur risiko *(risk appetite)* dengan Renstra dan pemantauannya melalui dashboard eksekutif akan memastikan bahwa keputusan manajemen selalu mempertimbangkan eksposur risiko terkini. Mekanisme pelaporan yang terstruktur dan *real time* kepada Direktur Eksekutif serta Dewan Pengawas akan meningkatkan transparansi dan akuntabilitas, memungkinkan pengambilan keputusan strategis yang lebih cepat dan berbasis data. Forum pembahasan risiko khusus di luar RKAT

akan memberikan ruang bagi analisis yang lebih mendalam, mengangkat diskusi risiko dari sekadar bagian laporan tahunan menjadi agenda strategis rutin.

2. Peningkatan Kematangan dan Efisiensi Proses Operasional

Rangkaian rekomendasi akan mendorong evolusi proses manajemen risiko dari ketergantungan pada catatan individu *(logbook)* dan komunikasi *ad-hoc* menuju alur kerja yang terdokumentasi, terdigitalisasi, dan kolaboratif. Otomatisasi pengumpulan data, analisis, dan respons melalui platform khusus (seperti *ITAM, GRC*, dan sistem *workflow*) akan mengurangi beban administratif manual, meminimalkan kesalahan, dan mempercepat waktu respon terhadap insiden. Pembuatan basis pengetahuan terpusat dari insiden masa lalu akan mengubah pengalaman individu menjadi aset organisasional, mendukung analisis akar penyebab yang lebih baik dan pembelajaran yang berkelanjutan. Integrasi antara identifikasi risiko, rencana mitigasi, dan pelacakan proyek dalam satu ekosistem digital akan menciptakan siklus pengelolaan risiko yang tertutup dan dapat diaudit.

3. Penumbuhan Budaya Keamanan dan Kesadaran Risiko yang Proaktif

Di luar aspek teknis dan prosedural, rekomendasi dirancang untuk membangun budaya kolektif di mana kesadaran terhadap risiko TI dan keamanan informasi menjadi tanggung jawab bersama. Program pelatihan berkelanjutan yang interaktif dan diukur efektivitasnya akan meningkatkan literasi digital dan kewaspadaan seluruh karyawan. Saluran partisipasi yang terstruktur untuk melaporkan kelemahan atau memberikan masukan keamanan akan mendorong rasa kepemilikan *(ownership)* dan mengubah setiap karyawan menjadi *line of defense* pertama. Koordinasi yang intensif dan terbuka antara unit Teknologi,

Kepatuhan/Risiko, dan unit bisnis lainnya, yang difasilitasi platform kolaborasi, akan memecah silo dan menciptakan pemahaman bersama tentang konteks bisnis dari setiap risiko TI.

4. Pencapaian Nilai dan Ketahanan Organisasional

Pada akhirnya, konsistensi dalam mengimplementasikan rekomendasi akan menghasilkan nilai nyata bagi organisasi. Pengelolaan risiko yang lebih matang akan mengurangi kemungkinan gangguan operasional dan kerugian finansial akibat insiden TI. Efisiensi yang diperoleh dari proses yang terotomatisasi akan mengalihkan sumber daya dari tugas rutin ke aktivitas bernilai tinggi seperti analisis strategis dan inovasi. Yang terpenting, LAZNAS Baitulmaal Muamalat (BMM) akan membangun ketahanan siber dan operasional yang lebih tangguh, mampu mengantisipasi dan beradaptasi dengan lanskap ancaman yang terus berubah, sehingga dapat terus fokus pada pencapaian misi sosialnya dengan kepercayaan diri yang lebih tinggi.

Secara keseluruhan, penguatan yang diwujudkan tidak hanya akan meningkatkan level kapabilitas, tetapi juga akan menciptakan lingkungan yang lebih tangguh *(resilient)* di mana risiko TI dikelola secara efektif sebagai bagian integral dari operasional dan strategi organisasi.

4.5.2. Peningkatan Pada Proses Bisnis

Penerapan rekomendasi tidak hanya berdampak pada penguatan manajemen risiko TI internal, tetapi juga secara signifikan meningkatkan efektivitas, keandalan, dan kepercayaan pada seluruh rantai bisnis utama di LAZNAS Baitulmaal

Muamalat (BMM). Berikut adalah peningkatan yang pada setiap tahap proses bisnis :

1. Tahap Penghimpunan Dana ZISWAF

   a. Peningkatan Kepercayaan dan Keamanan Transaksi

      Dengan diterapkannya kontrol keamanan informasi yang lebih ketat, keamanan platform donasi digital akan meningkat, hal ini akan selaras dalam mengurangi risiko kebocoran data dan penyalahgunaan transaksi, yang pada gilirannya memperkuat kepercayaan publik dan mendorong peningkatan partisipasi dalam penghimpunan dana.

   b. Ketersediaan Layanan yang Optimal

      Pemantauan risiko proaktif dan rencana pemulihan insiden yang terdokumentasi dengan baik akan meminimalkan downtime sistem penghimpunan dana. Donatur dapat mengakses layanan kapan saja tanpa gangguan teknis yang signifikan, sehingga mengoptimalkan potensi penghimpunan dana.

2. Tahap Pengelolaan Dana & Pembuatan Program

   a. Integritas dan Akurasi Data yang Terjaga

      Sistem manajemen data yang terpusat dan aman akan memastikan bahwa data dana dan penerima manfaat tetap akurat, konsisten, dan terlindungi dari kerusakan atau perubahan yang tidak sah. Hal ini menjadi dasar untuk perencanaan program yang tepat sasaran dan alokasi dana yang akuntabel.

   b. Pengambilan Keputusan Program yang Lebih Baik

Dashboard analisis risiko dan kinerja dapat diintegrasikan dengan data program, memungkinkan tim manajemen program untuk mengidentifikasi area dengan risiko operasional tertinggi atau peluang efisiensi. Analisis ini mendukung penyusunan program yang lebih tangguh dan berdampak besar.

3. Tahap Penyaluran pada Penerima Manfaat

   a. Efisiensi dan Ketepatan Penyaluran

      Otomatisasi proses verifikasi dan pencairan dana yang didukung oleh sistem yang baik dan memiliki rencana kontinjensi akan mempercepat penyaluran bantuan kepada penerima manfaat. Pengurangan kesalahan manual, penundaan teknis dan memastikan bantuan tepat waktu.

   b. Transparansi dan *Traceability* yang Meningkat

      Setiap langkah dalam rantai penyaluran, dari keputusan hingga pencairan, dapat dilacak dan diaudit dalam sistem terpusat. Hal ini menciptakan bukti digital yang kuat untuk memastikan dana sampai pada tujuan yang benar, memperkuat akuntabilitas LAZNAS Baitulmaal Muamalat (BMM) di mata donatur dan regulator.

4. Tahap Pelaporan & Evaluasi Program

   a. Pelaporan yang Akurat, Cepat, dan *Real Time*

      Laporan otomatis dari sistem terintegrasi menggantikan proses kompilasi manual yang rentan. Pemangku kepentingan, termasuk donatur dan dewan pengawas, dapat menerima laporan yang lebih detail, visual, dan tepat waktu mengenai penggunaan dana dan dampak program.

   b. Evaluasi Berbasis Data untuk Perbaikan Berkelanjutan

Basis pengetahuan yang menyimpan catatan insiden dan keberhasilan masa lalu menjadi alat berharga untuk mengevaluasi efektivitas program. Pola risiko TI yang dianalisis memungkinkan perbaikan desain program di masa depan, sehingga setiap siklus program menjadi lebih efektif dan efisien daripada sebelumnya.

Secara holistik, penguatan manajemen risiko TI berfungsi sebagai *enabler* dan *protector* bagi proses bisnis LAZNAS Baitulmaal Muamalat (BMM). Tidak hanya melindungi aset dan reputasi organisasi dari gangguan teknologi tetapi juga secara aktif meningkatkan kinerja setiap tahapan dari menghimpun kepercayaan donatur hingga mendemonstrasikan dampak sosial yang akuntabel. Pada akhirnya, ini mewujudkan siklus operasional yang lebih cepat, aman, transparan, dan berorientasi pada dampak, yang sesuai dengan nilai - nilai amanah dan profesionalisme yang dijunjung tinggi oleh lembaga zakat.

4.5.3. Evaluasi Rekomendasi

Evaluasi rekomendasi dilaksanakan menggunakan kuesioner sebagai instrumen penilaian lalu diserahkan kepada responden terkait agar di isi. Evaluasi ini bertujuan untuk mengetahui seberapa jelas, detail, spesifik, dan relevan rekomendasi-rekomendasi tersebut terhadap kebutuhan dan kondisi di LAZNAS Baitulmaal Muamalat (BMM) saat ini. Selain itu, evaluasi juga mencakup perkiraan terhadap potensi dampak dari implementasi rekomendasi, termasuk kesiapan organisasi dalam menindaklanjutinya serta tantangan yang mungkin dihadapi saat proses implementasi kedepan. Evaluasi yang dilakukan diharapkan tidak hanya sekedar menjadi penilaian bagi rekomendasi, tetapi juga sebagai upaya

penyempurnaan, bilamana ditemukan rekomendasi-rekomendasi yang kurang sesuai dan memerlukan perbaikan.

Kuesioner sebagai instrumen penilaian dalam proses evaluasi terdiri dari 5 bagian yaitu, Informasi Responden, Evaluasi Rekomendasi, Penerapan & Pengaruh, Tindak Lanjut & Saran, Penilaian Keseluruhan, dengan masing – masing bagian berisi 5 pertanyaan. Dalam kuesioner terdapat 2 jenis pertanyaan yaitu pilihan ganda dan isian, untuk pilihan ganda menggunakan skala *likert* yang terdiri dari 3 jenis pertanyaan pilihan ganda, yaitu 2, 4 dan 5 pilihan jawaban, kemudian dicari rata – ratanya dengan menjumlah total nilai yang didapat kemudian di bagi sesuai jumlah responden yaitu 5 dengan begitu akan terlihat, kecenderungan pilihan jawaban responden terhadap pertanyaan yang diajukan dalam setiap bagian kuesioner. Sedangkan untuk jawaban isian menggunakan nilai 1 apabila jawaban diisi dan 0 apabila tidak diisi, kemudian dari jawaban yang diisi di kategorisasi berdasarkan jawaban yang diberikan sehingga bisa di tarik kesimpulan kecenderungan jawaban responden. Berikut hasil rekapitulasi jawaban responden pada setiap bagian kuesioner.

a. Informasi Responden

Bagian ini terdiri dari 5 pertantanyaan, pertanyaan pertama terdiri dari 2 pilihan jawaban yaitu laki – laki ditandai dengan nilai (1) dan perempuan dengan nilai (2). Kemudian kedua terdiri dari 4 pilihan jawaban yaitu 20 – 30 tahun (1), 31 – 40 tahun (2), 41 – 50 tahun (3), dan 51 tahun ke atas (4). Selanjutnya ketiga terdiri dari 5 pilihan jawaban yaitu, SMA/Sederajat (1), D3 (2), S1(3), S2 (4), dan S3 (5). Berikutnya keempat terdiri dari 4 pilihan jawaban yaitu Kurang dari 1 tahun (1), 1

– 3 tahun (2), 4 – 6 tahun (3) dan Lebih dari 6 tahun (4). Terakhir pertanyaan kelima terdiri dari 5 pilihan jawaban yaitu Sangan Baik (5), Baik (4), Cukup (3), Kurang (2) dan Sangat Kurang (1).

Tabel 4.31. Rekap Jawaban Informasi Responden

No	Pertanyaan	Jenis Pertanyaan	Responden 1	Responden 2	Responden 3	Responden 4	Responden 5	Rata-Rata
1	Mohon pilih gender Anda.	Pilihan Ganda	2	1	1	1	1	1,2
2	Berapa usia Anda ?	Pilihan Ganda	3	4	2	3	3	3
3	Apa pendidikan terakhir yang Anda tempuh ?	Pilihan Ganda	3	2	3	4	3	3
4	Sudah berapa lama Anda bekerja di LAZNAS BMM ?	Pilihan Ganda	4	4	2	4	4	3,6
5	Seberapa besar pengetahuan Anda tentang manajemen risiko TI di LAZNAS BMM ?	Pilihan Ganda	3	3	5	4	3	3,6

Tabel 4.31. diatas menunjukkan bahwa mayoritas responden berjenis kelamin laki-laki dengan hasil nilai rata-rata jawaban 1,2. Usia bernilai rata-rata 3 menunjukkan bahwa mayoritas responden berada di rentang usia 41-50 tahun. Sebagian besar responden memiliki pendidikan akhir di tingkat sarjana (S1) dengan nilai rata-rata 3, mencerminkan tingkat pendidikan yang cukup tinggi. Dalam hal pengalaman kerja, mayoritas responden telah bekerja di LAZNAS BMM selama lebih dari 6 tahun ditunjukkan dari nilai rata-rata yang diperoleh yaitu 3,6 condong dekat dengan nilai 4, menunjukkan tingkat retensi yang baik di organisasi. Mengenai pengetahuan tentang manajemen risiko TI, sebagian besar responden merasa memiliki pengetahuan yang baik, terlihat dari nilai rata-rata yang dihasilkan yaitu 3,6 lebih dekat dengan nilai 4. Ditarik kesimpulan bahwa bagian ini

menggambarkan profil demografis responden yang berusia matang dan berpendidikan tinggi, dengan pengalaman kerja yang signifikan di LAZNAS Baitulmaal Muamalat (BMM) dan pengetahuan yang baik tentang manajemen risiko TI di organisasi.

b. Evaluasi Rekomendasi

Bagian evaluasi rekomendasi terdiri dari 5 pertanyaan dengan masing-masing memiliki pilihan jawaban yang berbeda. Pertanyaan pertama terdiri dari 5 pilihan jawaban yaitu Sangat Jelas (5), Jelas (4), Cukup Jelas (3), Tidak Jelas (2), dan Sangat Tidak Jelas (1). Pertanyaan kedua terdiri dari 5 pilihan jawaban yaitu Sangat Detail (5), Detail (4), Cukup Detail (3), Tidak Detail (2), dan Sangat Tidak Detail (1). Pertanyaan ketiga terdiri dari 5 pilihan jawaban yaitu Sangat Spesifik (5), Spesifik (4), Cukup Spesifik (3), Tidak Spesifik (2), dan Sangat Tidak Spesifik (1). Pertanyaan keempat terdiri dari 5 pilihan jawaban yaitu Sangat Runtut (5), Runtut (4), Cukup Runtut (3), Tidak Runtut (2), dan Sangat Tidak Runtut (1). Terakhir, pertanyaan kelima terdiri dari 5 pilihan jawaban yaitu Sangat Layak (5), Layak (4), Cukup Layak (3), Tidak Layak (2), dan Sangat Tidak Layak (1).

Tabel 4.32. Rekap Jawaban Evaluasi Rekomendasi

No	Pertanyaan	Jenis Pertanyaan	Responden 1	Responden 2	Responden 3	Responden 4	Responden 5	Rata-Rata
1	Seberapa jelas & mudah dipahami rekomendasi yang diajukan ?	Pilihan Ganda	3	3	5	4	4	3,8
2	Seberapa detail rekomendasi yang diajukan ?	Pilihan Ganda	3	3	5	3	4	3,6
3	Seberapa spesifik rekomendasi yang diajukan ?	Pilihan Ganda	3	3	5	3	4	3,6
4	Seberapa runtut rekomendasi yang	Pilihan Ganda	4	3	5	3	4	3,8

	diajukan ?							
5	Seberapa layak untuk di implementasi rekomendasi yang diajukan ?	Pilihan Ganda	4	4	5	4	4	4,2

Tabel 4.32. diatas menggambarkan bagaimana responden menilai kualitas rekomendasi yang diajukan dari segi kejelasan, detail, spesifikasi, keruntutan, dan kelayakan. Tabel tersebut menunjukkan bahwa mayoritas responden menilai rekomendasi yang diajukan umumnya sudah jelas dengan nilai rata-rata jawaban 3,8, detail 3,6, spesifik 3,6, runtut 3,8 serta layak bernilai 4,2 untuk diimplementasikan. Hal ini mengindikasikan jika rekomendasi yang diajukan berpeluang bisa dipahami dengan utuh dan menyeluruh, juga berpotensi dapat diterapkan dalam konteks yang relevan dengan LAZNAS Baitulmaal Muamalat (BMM). Sehingga bisa ditarik kesimpulan bahwa rekomendasi yang disusun sudah baik dan berada pada jalur yang tepat untuk diimplementasikan.

c. Penerapan & Pengaruh

Bagian penerapan & pengaruh terdiri dari 5 pertanyaan, yang bertujuan untuk mengevaluasi penerapan dan pengaruh rekomendasi yang diajukan kepada LAZNAS BMM. Pertanyaan pertama terdiri dari 5 pilihan jawaban yaitu, Sangat Siap (5), Siap (4), Cukup Siap (3), Tidak Siap (2), dan Sangat Tidak Siap (1). Pertanyaan kedua terdiri dari 4 pilihan jawaban yaitu, Ya, banyak tantangan (5), Ya, ada beberapa tantangan (4), Tidak ada tantangan signifikan (3), dan Tidak ada tantangan sama sekali (2). Pertanyaan ketiga berbentuk isian, di mana responden diminta untuk menuliskan tantangan atau hambatan utama dalam penerapan rekomendasi yang diajukan. Jika ada jawaban, nilai akan diberikan 1, dan jika tidak

ada jawaban, nilai akan diberikan 0. Pertanyaan keempat terdiri dari 5 pilihan jawaban yaitu: Sangat Besar (5), Besar (4), Sedang (3), Kecil (2), dan Tidak Ada Dampak (1). Pertanyaan kelima berbentuk isian, di mana responden diminta untuk menjelaskan pengaruh yang mereka harapkan jika rekomendasi yang diajukan diterapkan. Penilaian pada pertanyaan ini juga diberikan 1 jika ada jawaban dan 0 jika tidak ada jawaban.

Tabel 4.33. Rekap Jawaban Penerapan & Pengaruh

No	Pertanyaan	Jenis Pertanyaan	Responden 1	Responden 2	Responden 3	Responden 4	Responden 5	Rata-Rata
1	Menurut Anda bagaimana tingkat kesiapan LAZNAS BMM dalam menerapkan rekomendasi yang diajukan ?	Pilihan Ganda	3	4	5	3	3	3,6
2	Apakah Anda melihat adanya tantangan dalam penerapan rekomendasi yang diajukan ?	Pilihan Ganda	3	3	4	3	2	3
3	Jika ada, tuliskan tantangan atau hambatan utama penerapan rekomendasi yang diajukan.	Isian	1	1	1	1	0	0,8
4	Jika diterapkan bagaimana Anda melihat dampak atau pengaruh yang dihasilkan oleh rekomendasi terhadap pengelolaan risiko TI di LAZNAS BMM ?	Pilihan Ganda	3	4	5	3	4	3,8
5	Apa pengaruh yang Anda harapkan bila rekomendasi yang diajukan dapat diterapkan ?	Isian	1	1	1	1	0	0,8

Tabel 4.33. di atas menunjukkan hasil rekap jawaban dari responden mengenai penerapan dan pengaruh rekomendasi yang diajukan kepada LAZNAS BMM. Pertanyaan pertama nilai rata-rata sebesar 3,6 menunjukkan bahwa mayoritas responden menilai kesiapan organisasi unruk menerapan rekomendasi

baik, karena nilai rata-rata lebih mendekati angka 4, yang berarti kesiapan untuk penerapan sudah baik. Pada pertanyaan kedua, nilai rata-rata 3 menunjukkan bahwa mayoritas responden melihat adanya beberapa tantangan yang perlu diatasi. Pada pertanyaan ketiga, yang berbentuk isian, responden diminta untuk menjelaskan tantangan atau hambatan yang mereka lihat dalam penerapan rekomendasi. Nilai rata-rata 0,8 menunjukkan bahwa mayoritas responden memberikan penjelasan terkait tantangan yang mereka identifikasi. Pada pertanyaan keempat nilai rata-rata 3,8 yang mendekati 4 menunjukkan bahwa mayoritas responden percaya bahwa dampak atau pengaruh yang dihasilkan dari penerapan rekomendasi besar sehingga memberikan pengaruh yang signifikan terhadap pengelolaan risiko TI di organisasi. Dari hasil ini, dapat disimpulkan bahwa responden umumnya melihat bahwa kesipaan organisasi untuk menerapkan rekomendasi baik, namun ada beberapa tantangan yang harus dihadapi dalam implementasinya. Selain itu, mayoritas responden juga merasa bahwa pengaruh dari penerapan rekomendasi ini terhadap pengelolaan risiko TI akan signifikan.

d. Tindak Lanjut & Saran

Bagian tindak lanjut dan saran terdiri dari 5 pertanyaan. Pertanyaan pertama terdiri dari 5 pilihan jawaban yaitu Sangat Urgen (5), Urgen (4), Cukup Urgen (3), Tidak Urgen (2), dan Sangat Tidak Urgen (1). Pertanyaan kedua terdiri dari 2 pilihan jawaban yaitu Ya (1) dan Tidak (2) jika responden memilih "Ya" maka mereka diminta untuk menuliskan rencana tindak lanjut terkait rekomendasi. Pada pertanyaan ketiga, yang berbentuk isian, responden diminta untuk menjelaskan hal-hal yang perlu dipertimbangkan untuk melanjutkan rekomendasi yang diajukan.

Penilaian pada pertanyaan ini diberikan nilai 1 jika ada jawaban yang diisi dan 0 jika tidak ada jawaban. Pertanyaan keempat terdiri dari 2 pilihan jawaban yaitu Ya (1) dan Tidak (2), jika responden memilih "Ya", mereka diminta untuk memberikan penjelasan lebih lanjut mengenai aspek lain yang perlu mendapatkan perhatian lebih dan belum tercantum dalam rekomendasi yang diajukan. Terakhir, pertanyaan kelima terdiri dari 2 pilihan jawaban yaitu Ya (1) dan Tidak (2), jika memilih "Ya", responden diharapkan memberikan saran rekomendasi lain yang belum ada dalam rekomendasi yang diajukan.

Tabel 4.34. Rekap Jawaban Tindak Lanjut & Saran

No	Pertanyaan	Jenis Pertanyaan	Responden 1	Responden 2	Responden 3	Responden 4	Responden 5	Rata-Rata
1	Menurut Anda, seberapa urgen rekomendasi yang diajukan untuk dapat di tindak lanjuti ?	Pilihan Ganda	4	3	5	3	3	3,6
2	Apakah Anda memiliki rencana tindak lanjut terkait rekomendasi yang diajukan ?	Pilihan Ganda (Disertai Penjelasan)	1	1	1	2	1	1,2
3	Menurut Anda, apa hal yang perlu di pertimbangkan bila menindaklanjuti rekomendasi yang diajukan ?	Isian	1	1	1	1	0	0,8
4	Apakah Anda melihat ada aspek lain yang perlu mendapat perhatian lebih dan belum tercantum dalam rekomendasi yang diajukan ?	Pilihan Ganda (Disertai Penjelasan)	2	2	2	2	2	2
5	Apakah Anda memiliki saran rekomendasi lain yang belum ada dalam rekomendasi yang diajukan ?	Pilihan Ganda (Disertai Penjelasan)	2	2	2	2	2	2

Tabel 4.34. di atas menunjukkan hasil rekap jawaban dari responden mengenai tindak lanjut dan saran terkait rekomendasi yang diajukan. Pertanyaan

pertama mengenai seberapa urgennya rekomendasi yang diajukan untuk dapat ditindaklanjuti, nilai rata-rata didapat sebesar 3,6 menunjukkan bahwa mayoritas responden menilai rekomendasi tersebut urgen karena nilai rata-rata mendekati angka 4. Pada pertanyaan kedua, mengenai apakah responden memiliki rencana tindak lanjut terkait rekomendasi yang diajukan, nilai rata-rata 1,2 menunjukkan bahwa sebagian besar responden menjawab "Ya", dan disertai dengan penjelasan lebih lanjut, mengindikasikan bahwa mereka memiliki rencana tindak lanjut terkait rekomendasi tersebut. Pada pertanyaan ketiga, yang berbentuk isian, responden diminta untuk menjelaskan hal-hal yang perlu dipertimbangkan dalam melanjutkan rekomendasi yang diajukan. Dengan rata-rata nilai 0,8, dapat disimpulkan bahwa mayoritas responden memberikan penjelasan mengenai hal-hal yang perlu dipertimbangkan. Pada pertanyaan keempat, nilai rata-rata 2 menunjukkan bahwa mayoritas responden menjawab "Tidak", yang berarti mereka tidak melihat adanya aspek lain yang perlu diperhatikan atau belum tercakup dalam rekomendasi. Pada pertanyaan kelima, nilai rata-rata 2 juga menunjukkan bahwa mayoritas responden menjawab "Tidak", yang berarti mereka tidak memberikan saran tambahan untuk meningkatkan rekomendasi yang ada. Dari hasil ini, dapat disimpulkan bahwa responden umumnya melihat bahwa rekomendasi yang diajukan urgen untuk ditindaklanjuti dan sebagian besar responden sudah memikirkan langkah-langkah tindak lanjut. Selain itu mayoritas responden tidak melihat adanya aspek lain yang perlu diperhatikan atau memberikan saran tambahan untuk meningkatkan rekomendasi yang ada.

e. Penilaian Keseluruhan

Bagian terkahir teriri dari 5 pertanyaan, pertanyaan pertama terdiri dari 5 pilihan jawaban yaitu Sangat Relevan (5), Relevan (4), Cukup Relevan (3), Kurang Relevan (2), dan Tidak Relevan (1). Pertanyaan kedua menanyakan seberapa besar responden melihat potensi perbaikan terhadap pengelolaan risiko TI di LAZNAS BMM dengan penerapan rekomendasi yang diajukan. Pilihan jawaban yang tersedia adalah Sangat Besar (5), Besar (4), Cukup Besar (3), Kecil (2), dan Sangat Kecil (1). Pada pertanyaan ketiga, responden diminta untuk menilai seberapa bermanfaat rekomendasi yang diajukan. Pilihan jawaban yang tersedia adalah Sangat Bermanfaat (5), Bermanfaat (4), Cukup Bermanfaat (3), Kurang Bermanfaat (2), dan Tidak Bermanfaat (1). Pertanyaan keempat menanyakan bagaimana responden menilai kualitas rekomendasi yang diajukan secara keseluruhan, dengan pilihan jawaban: Sangat Baik (5), Baik (4), Cukup (3), Kurang (2), dan Sangat Kurang (1). Terakhir, pertanyaan kelima terdiri dari 2 pilihan jawaban yaitu Ya (1) dan Tidak (2). Jika responden memilih "Ya", mereka diminta untuk memberikan penjelasan mengenai penilaian yang ingin mereka sampaikan dalam bentuk narasi.

Tabel 4.35. Rekap Jawaban Penilaian Keseluruhan

No	Pertanyaan	Jenis Pertanyaan	Responden 1	Responden 2	Responden 3	Responden 4	Responden 5	Rata-Rata
21	Seberapa relevan rekomendasi yang diajukan dengan persoalan pengelolaan risiko TI di LAZNAS BMM ?	Pilihan Ganda	3	4	5	3	3	3,6
22	Seberapa besar Anda melihat potensi perbaikan terhadap pengelolaan risiko TI di LAZNAS BMM dengan diajukannya rekomendasi-rekomendasi tersebut ?	Pilihan Ganda	3	4	5	3	3	3,6
23	Apakah Anda merasa	Pilihan	4	4	5	4	3	4

	bahwa rekomendasi yang diajukan dapat menghadirkan manfaat yang nyata ?	Ganda						
24	Secara keseluruhan, bagaimana Anda menilai kualitas rekomendasi yang diajukan ?	Pilihan Ganda	4	4	5	4	4	4,2
25	Apakah Anda memiliki penilain yang ingin disampaikan dalam bentuk narasi?	Pilihan Ganda (Disertai Penjelasan)	2	2	2	2	2	2

Tabel 4.35. di atas menunjukkan hasil rekap jawaban dari responden mengenai penilaian keseluruhan terhadap rekomendasi yang diajukan. Pertanyaan pertama bernilai rata-rata 3,6 menunjukkan bahwa mayoritas responden menilai rekomendasi tersebut relevan, karena nilai rata-rata lebih mendekati angka 4, yang berarti rekomendasi tersebut cukup sesuai dengan kebutuhan organisasi. Pada pertanyaan kedua, mengenai seberapa besar potensi perbaikan yang dihasilkan dari penerapan rekomendasi tersebut terhadap pengelolaan risiko TI, nilai rata-rata 3,6 menunjukkan bahwa mayoritas responden menilai potensi perbaikan tersebut besar, dengan nilai rata-rata yang lebih dekat ke angka 4, yang berarti responden melihat adanya potensi perbaikan yang signifikan dari penerapan rekomendasi yang diajukan. Pada pertanyaan ketiga, dengan nilai rata-rata 4 menunjukkan bahwa mayoritas responden menilai bahwa rekomendasi ini cukup bermanfaat, dengan angka rata-rata yang lebih dekat ke angka 4, yang berarti mereka merasa rekomendasi ini akan memberikan manfaat yang signifikan. Pertanyaan keempat, nilai rata-rata 4,2 menunjukkan bahwa mayoritas responden menilai kualitas rekomendasi tersebut baik, yang berarti rekomendasi tersebut dianggap memiliki kualitas yang baik. Pada pertanyaan kelima, nilai rata-rata 2 menunjukkan bahwa

mayoritas responden menjawab "Tidak", yang berarti mereka tidak memiliki penilaian tambahan yang ingin disampaikan dalam bentuk narasi. Dapat disimpulkan bahwa mayoritas responden menilai rekomendasi yang diajukan relevan dengan kebutuhan organisasi, dan mereka juga melihat potensi perbaikan yang signifikan dalam pengelolaan risiko TI jika rekomendasi tersebut diterapkan. Selain itu, responden merasa bahwa rekomendasi ini bermanfaat dan memiliki kualitas yang baik, yang menunjukkan bahwa rekomendasi ini dapat memberikan kontribusi positif bagi organisasi.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil dari penelitian yang dilakukan pada LAZNAS Baitulmaal Muamalat (BMM), maka terdapat beberapa kesimpulan yang dapat disampaikan sebagai berikut :

1. *Framework* COBIT 2019 digunakan untuk melakukan audit terhadap pengelolaan manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM), hasil audit memberikan gambaran yang jelas mengenai kondisi aktual penerapan dan proses pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM). Pada domain EDM03 *(Ensure Risk Optimization)*, hasil audit menemukan bahwa proses pengelolaan risiko telah dijalankan secara konsisten, mulai dari kegiatan evaluasi, pengarahan, hingga pemantauan risiko, sehingga organisasi mampu menjaga kesesuaian pengelolaan risiko dengan tujuan strategis. Pada domain APO12 *(Manage Risk)*, audit memperlihatkan bahwa mekanisme identifikasi, analisis, dokumentasi, dan penanganan risiko telah berlangsung secara terstruktur, dengan proses yang berjalan efektif dan didukung oleh pelibatan unit terkait. Sementara itu, pada domain APO13 *(Manage Security)*, audit menemukan bahwa kegiatan pengamanan informasi, pengendalian akses, serta pemantauan keamanan telah diterapkan, meskipun masih terdapat area yang memerlukan penguatan terutama dalam penyempurnaan pengendalian keamanan dan penerapan tata kelola keamanan secara lebih komprehensif.

Secara keseluruhan, hasil audit memberikan gambaran bahwa pengelolaan risiko TI di BMM telah berjalan dengan baik, meskipun pada aspek keamanan masih perlu ditingkatkan.

2. Berdasarkan hasil audit pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM) diketahui *capability level* pada domain EDM03 *(Ensure Risk Optimization)*, APO12 (Manage Risk), dan APO13 (Manage Security) berada pada level kapabilitas dengan nilai rata-rata *capability level* saat ini *(as-is)* sebesar 3. Domain EDM03 *(Ensure Risk Optimization)*, berada pada level 3 dan sesuai dengan target yang telah ditetapkan yaitu level 3 sehingga tidak memiliki gap. Domain APO12 *(Manage Risk)*, berada pada level kapabilitas 4 dan juga selaras dengan target yaitu level 4, sehingga tidak menunjukkan kesenjangan. Namun pada domain APO13 *(Manage Security)*, *capability level* saat ini berada pada level 3 sedangkan targetnya adalah level 4, sehingga terdapat gap sebesar 1 yang menunjukkan bahwa peningkatan masih diperlukan khususnya pada aspek pengelolaan keamanan TI. Secara keseluruhan, rata-rata gap untuk ketiga domain adalah 1, yang menandakan bahwa meskipun pengelolaan risiko TI BMM berada pada kategori yang mapan, masih terdapat kebutuhan peningkatan di bagian keamana informasi agar dapat mencapai target level kapabilitas yang ditetapkan.
3. Rekomendasi yang diberikan berdasar temuan hasil audit pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM) mencakup peningkatan pada sisi dokumentasi risiko, penguatan kompetensi SDM yang menangani risiko TI, penyempurnaan peran dan tanggung jawab pengelolaan risiko, peningkatan

mekanisme evaluasi risiko, peningkatan koordinasi dan komunikasi antar *stakeholder*, serta keterlibatan pihak eksternal dalam proses audit keamanan dan kepatuhan. Rekomendasi ini dirancang untuk mendorong peningkatan *capability level* dan penguatan terhadap pengelolaan risiko TI di LAZNAS Baitulmaal Muamalat (BMM).

5.2. Saran

Berdasarkan hasil penelitian yang telah dilakukan pada LAZNAS Baitulmaal Muamalat (BMM), terdapat beberapa saran yang dapat diberikan, yaitu:

1. Penelitian selanjutnya disarankan untuk mennerapkan *framework* COBIT 2019 spesifik dalam pembahasan manajemen risiko TI pada organisasi serupa, sehingga bisa menjadi penambah literasi terhadap penelitian bertema sama.
2. Penelitian berikutnya disarankan untuk menggunakan metode audit lain, serta membandingkan framework COBIT 2019 dengan kerangka kerja lainnya guna memperoleh perbandingan yang lebih jelas terhadap hasil audit.
3. Penelitian selanjutnya disarankan untuk melibatkan lebih banyak *stakeholder* dalam keterlibatan penelitian manajemen risiko TI di LAZNAS Baitulmaal Muamalat (BMM).

DAFTAR PUSTAKA

PUSTAKA BUKU

ISACA. (2018). COBIT® 2019 Framework: Governance and Management Objectives. ISACA. ISBN 978-1-60420-764-4.

Solechan, A. (2021). *Audit sistem informasi*. Yayasan Prima Agus Teknik.

Setia Sandi, A. (2022). *Manajemen risiko TI*. CV. Elvaretta Buana.

Kusbandono, H., Ariyadi, D., & Lestariningsih, T. (2019). *Tata kelola teknologi informasi*. Nata Karya.

Sarjana, S., Nardo, R., Hartono, R., Siregar, Z. H., Irmal, Sohilauw, M. L., Wahyuni, S., Rasyid, A., Djaha, Z. A., & Badrianto, Y. (Ed.). (2022). *Manajemen risiko* (Vol. 1). Media Sains Indonesia.

Kristiana, R., Rochman, A. S., Yusuf, M., Sediyanto, S., Bagho, K. L., Sutikno, A., Hafidah, A., Wedhasari, T., Sukwika, T., Saepudin, A., & Afriansyah. (2022). *Manajemen risiko*. CV. Mega Press Nusantara.

PUSTAKA JURNAL

Vasilopoulou, C., Theodorakopoulos, L., & Giotopoulos, K. (2023). Big Data Analytics: A Catalyst for Digital Transformation in e-Government. *Technium Social Sciences Journal*, 45, 449-459.

Safitri, A., Syafii, I., & Adi, K. (2021). Measuring the performance of information system governance using framework COBIT 2019. *International Journal of Computer Applications, 174*(31), 23-30.

Berrada, H., Boutahar, J., & El Ghazi El Houssaïni, S. (2021). Simplified IT risk management maturity audit system based on "COBIT 5 for Risk". *International Journal of Advanced Computer Science and Applications, 12*(8), 641-652.

Setyadi, R., & Prabowo, H. N. (2021). Risk management analysis of bus transportation application using COBIT 4.1. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, 7(2), 203-212.

Anugrah, R., Utami, E., & Muhammad, A. H. (2022). Analisis manajemen risiko TI pada perguruan tinggi XYZ berbasis COBIT 2019 dengan pertimbangan domain APO12. *Jurnal Ilmiah Universitas Batanghari Jambi*, 22(2), 991-995.

Enrique, E., & Fianty, M. I. (2023). Enhancing risk management in an IT service company: A COBIT 2019 framework approach. *Jurnal Riset Informatika, 5*(4), 499-506.

Hardjadinata, M. B., & Wiratama, J. (2023). Capability assessment of IT governance using the 2019 COBIT framework for the IT business consultant industry. *International Journal of Science, Technology & Management, 4*(2), 1034-1039.

Harits, A., Noer, G. M., & Widodo, A. P. (2021). Capability level measurement using COBIT 5 (Case Study: PT. Jasa Cendekia Indonesia). *Journal of Information Systems and Informatics, 3*(2), 341-351.

Mualo, H., & Rohim, A. N. (2023). Analisis efisiensi dan efektivitas pengelolaan dana ZIS pada Laznas Baitulmaal Muamalat. *Islamic Economics and Business Review, 2*(1), 11-23.

Noble, H., & Smith, J. (2025). Ensuring validity and reliability in qualitative research. *Evidence-Based Nursing*, 0(0), 1-4.

Lim, W. M. (2025). What is qualitative research? An overview and guidelines. *Australasian Marketing Journal,* 33(2), 199-229.

Arias Valencia, M. M. (2022). Principles, scope, and limitations of the methodological triangulation. *Investigación y Educación en Enfermería*, 40(2), e03.

Mo, Z., Li, X., Zhai, Y., Men, Y., Tang, Y., Qiao, J., Jia, X., Huang, Y., & Wang, B. (2023). Reliability and validity of a questionnaire measuring knowledge, attitude and practice regarding "oil, salt and sugar" among canteen staff. *Scientific Reports*, 13(20442).

Cui, Q., Harshman, J. T., & Komperda, R. (2024). Validity and reliability of survey data: Key to empowering chemical health and safety research. *ACS Chemical Health & Safety*, 31(2), 121-126.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44, 100548.

Memon, M. A., Ting, H., Cheah, J. H., Ramayah, T., Chuah, F., & Cham, T. H. (2020). Sample size for survey research: *Review and recommendations. Journal of Applied Structural Equation Modeling*, 4(2), i-xx.

PUSTAKA LAPORAN PENELITIAN

Lubna. (2023). *Identifikasi level tata kelola TI pada manajer associate product menggunakan COBIT 2019 domain APO 11: Studi kasus di Innovation Center Universitas Amikom Yogyakarta* (Tesis Magister, Program Pascasarjana Teknik Informatika, Universitas AMIKOM Yogyakarta).

Washilatul Arba'ah, Z. D. K. (2023). *Audit teknologi informasi layanan e-government menggunakan COBIT 2019 (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Sleman)* (Tesis Magister, Program Pascasarjana Teknik Informatika, Universitas Amikom Yogyakarta).

Suphian. (2022). *Audit tata kelola TI menggunakan COBIT 2019 pada UPTD RSUD Tarakan Provinsi Kalimantan Utara* (Tesis Magister, Program Pascasarjana Teknik Informatika, Universitas AMIKOM Yogyakarta).

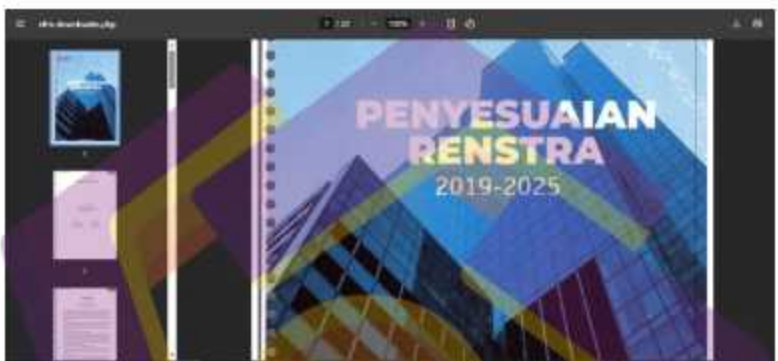
Hakim, W. R. (2022). *Evaluasi penerapan tata kelola infrastruktur TI menggunakan COBIT 5 (Studi Kasus: Sekolah Tinggi Agama Islam Sufyan Tsauri Majenang)* (Tesis Magister, Program Pascasarjana Teknik Informatika, Universitas AMIKOM Yogyakarta).

Kholimatin, A. (2022). *Evaluasi tata kelola teknologi informasi pada domain Evaluate Direct and Monitor dengan menggunakan framework COBIT 5.0* (Tesis Magister, Teknik Informatika, Program Pascasarjana Universitas AMIKOM Yogyakarta).

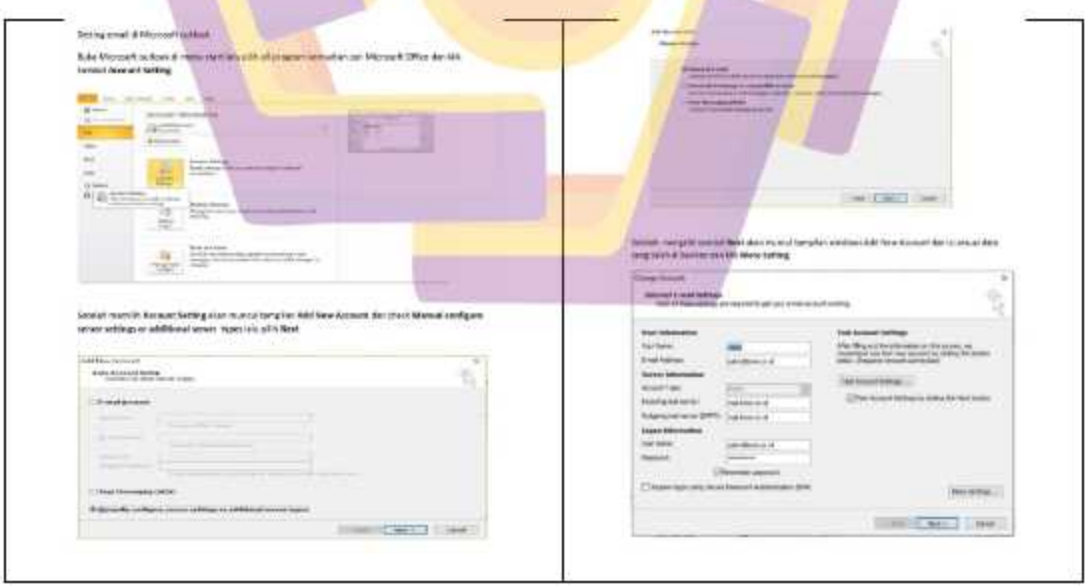
LAMPIRAN

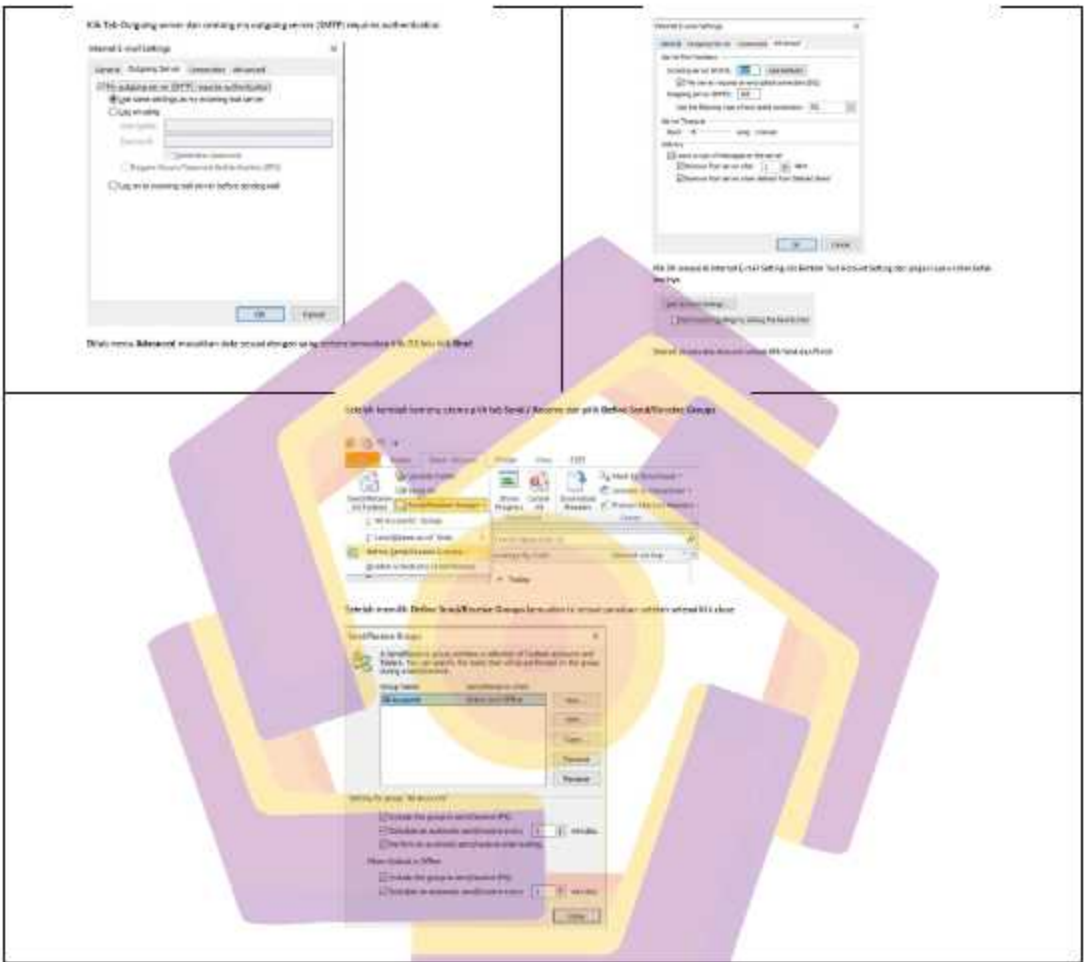
Lampiran 1 Bukti Dokumen Pendukung Penelitian

1. Dokumen Rencana Strategis (RESNTRA 2019 – 2025).



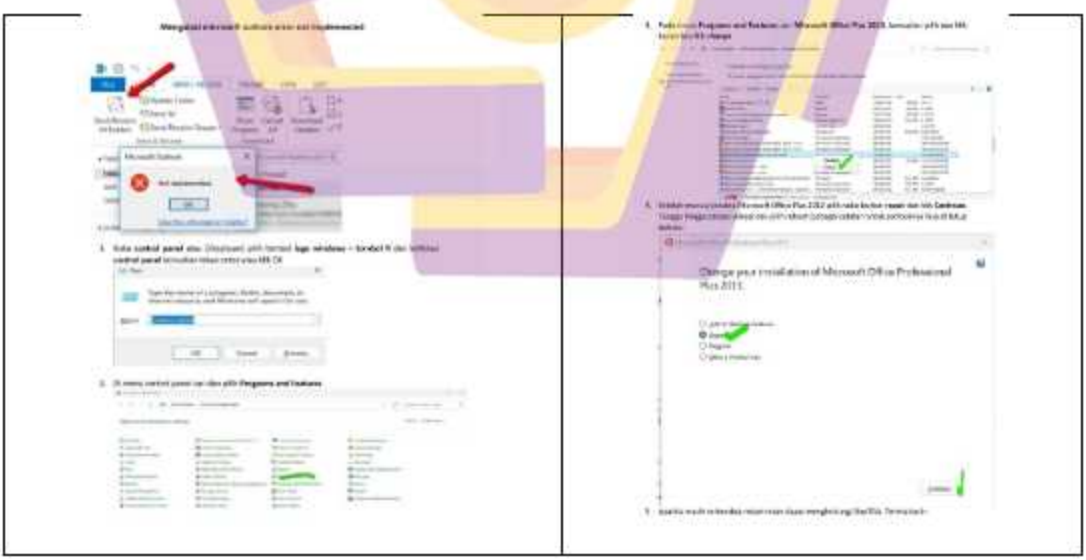
2. Prosedur Penggunaan Email Outlook untuk Semua Karyawan.





3. Prosedur Cek Kapasitas Email.

4. Prosedur Saat Email Error.

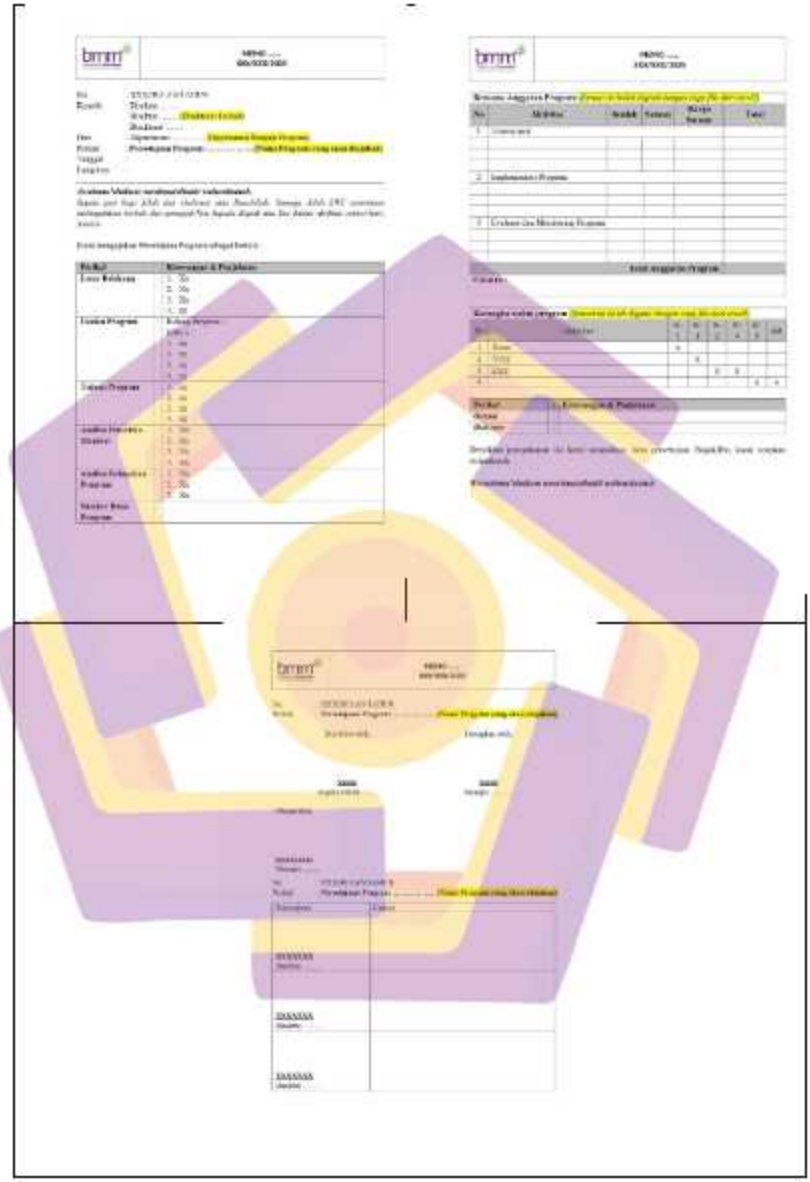


5. Prosedur Penggunaan Email Outlook di HP.

6. Form Berita Acara Serah Terima (BAST) sebagai bagian dari pencatatan atau dokumentasi resmi kaitannya dengan perpindahan kepemilikan atau penyerahan, aset, tanggung jawab, tugas dan lainnya.

7. Memo Internal sebagai dokumen komunikasi resmi untuk menyampaikan intruksi, pemberitahuan, pengumam dan informasi secara umum.

8. Memo Persetujuan Program sebagai dokumen yang digunakan untuk mendokumentasikan, menginformasikan dan mendapatkan persetujuan resmi atas suatu program atau inisiatif tertentu.



9. Form Pengelurana Dana yaitu dokumen resmi yang digunakan untuk mengontrol setiap dana atau uang yang keluar.

FORM PENGELUARAN DANA (FPD)

XXX/XXX/2025

10. Form Persetujuan Pengeluaran Dana yaitu dokumen komunikasi yang digunakan untuk memberi persetujuan atau otorisasi terkait setiap dana atau uang yang keluar.

bmm

FORM PERSETUJUAN PENGELUARAN DANA (FPPD)

XXX/XXX/2025

Nomor	:		
Latar Belakang	1	Mengacu pada MP No :	
	2	Budget Program sesuai MP :	Rp -
	3		
Tujuan Penyaluran	1		
	2		
	3		
Verifikasi Penerima Manfaat		Pihak yang Diverifikasi/Dikonfirmasi :	
	1	Nama	:
	2	Lembaga	:
	3	Jabatan	:
	4	Telpon	:
	5	Alamat	:
		Hasil Verifikasi/Konfirmasi	
	1		
	2		
	3		
Analisa Kelayakan	1		
	2		
	3		
Program Penyaluran		Rincian Anggaran Biaya	

No	Aktivitas	Jumlah	Satuan	Harga Satuan	Total
					-
					-
					-
					-
Total Anggaran Program				Rp	-

Catatan :
Sisa anggaran untuk pendayagunaan berikutnya / hak amil / pengembalian dll

	1	Asnaf Penerima Manfaat	: Sesuai dengan peruntukan
	2	Jumlah Penerima Manfaat	: Sesuai dengan peruntukan
	3	Nominal	: Rp -
	4	Dana Diberikan Melalui	:
	5	Rekening Penerima	:
	6	Pelaksana Teknis Kegiatan	: (Manager/Staf)
	7	Penanggung Jawab Kegiatan	: (WA/SI Kab/Kc)

Disetujui Oleh,	Diketahui Oleh,	Diperiksa Oleh,	Dibuat Oleh,
XXX Direktur	XXX Kadiv	XXX Manajer	XXX Staf .....