JURNAL FASILKOM
Volume 15 No. 1 | April 2025: 185-194

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Analisis Manajemen Risiko TI Berbasis COBIT 2019 Pada Lembaga Amil Zakat Nasional XYZ

Thata Authar Razaq[1], Alva Hendi Muhammad[2]
[1,2]Program Studi Magister Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
[1]thata@students.amikom.ac.id, [2]alva@amikom.ac.id

Abstract

The analysis of Information Technology (IT) risk management at the National Zakat Amil Institution (LAZNAS) XYZ is conducted using the COBIT 2019 framework, specifically in the domains of EDM 03 (Ensure Risk Optimization), APO 12 (Manage Risk), and APO 13 (Manage Security). Given the importance of IT in supporting the operations and management of Zakat, Infak, Sadaqah, and Wakaf (ZISWAF) funds, the main objective is to assess the effectiveness of the implemented IT risk management. The methodology used is a qualitative descriptive approach through a case study, with data collection via observation, interviews, and questionnaires from respondents involved in IT management. The research results indicate that LAZNAS XYZ has achieved an adequate capability level in the domains of EDM 03 (Ensure Risk Optimization), APO 12 (Manage Risk), and APO 13 (Manage Security), with an average level of 3. However, there are gaps in the APO 12 and APO 13 domains, which require improvements to achieve level 4. The improvement recommendations include strengthening risk metric monitoring, expanding the scope of risk data collection, and enhancing the effectiveness of security policies through regular audits and staff training. The conclusion of this study is that the implementation of COBIT 2019 can help LAZNAS XYZ improve IT governance and risk management, thereby supporting donor trust and regulatory compliance. This research 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, COBIT 2019, LAZNAS, IT governance

Abstrak

Analisis pengelolaan risiko Teknologi Informasi (TI) di Lembaga Amil Zakat Nasional (LAZNAS) XYZ 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 LAZNAS XYZ 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. Namun, terdapat kesenjangan pada domain APO 12 dan APO 13, yang memerlukan peningkatan untuk mencapai level 4. Rekomendasi perbaikan meliputi penguatan pemantauan metrik risiko, perluasan cakupan pengumpulan data risiko, serta peningkatan efektivitas kebijakan keamanan melalui audit berkala dan pelatihan staf. Kesimpulan penelitian ini adalah bahwa penerapan COBIT 2019 dapat membantu LAZNAS XYZ meningkatkan tata kelola dan manajemen risiko TI, sehingga mendukung kepercayaan donatur dan kepatuhan 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, COBIT 2019, LAZNAS, tata kelola TI

1. Pendahuluan

Teknologi Informasi (TI) telah mengalami perkembangan yang sangat signifikan dan menjadi semakin krusial dalam mendukung efektivitas dan efisiensi perusahaan dalam meraih visi, misi, dan tujuannya [1]. Teknologi Informasi (TI) bukan hanya sekadar alat untuk mempercepat dan memperbaiki proses bisnis, tetapi juga menjadi katalisator utama dalam menciptakan inovasi dan efisiensi [2]. 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 [3]. 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 [4]. Risiko-risiko ini berpotensi mengakibatkan gangguan operasional, kerugian finansial, serta kerusakan reputasi yang dapat berdampak jangka panjang pada keberlangsungan

P-ISSN : 2089-3353
E-ISSN : 2808-9162

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 [5].

Lembaga Amil Zakat Nasional (LAZNAS) XYZ adalah salah satu organisasi khususnya dalam sektor filantropi di Indonesia yang sangat bergantung pada TI dalam menjalankan visi misinya. Mulanya didirikan sebagai entitas sosial di dalam organisasi korporasi di sektor keuangan, 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), LAZNAS XYZ mengelola data yang sangat sensitif terkait donatur, penerima manfaat, dan sukarelawan. Kepercayaan donatur bergantung pada transparansi dan keandalan LAZNAS XYZ dalam mengelola data dan melaporkan distribusi dana. Namun, risiko terhadap keamanan data dapat merusak kepercayaan ini dan mengancam kelangsungan operasional LAZNAS XYZ. Di sinilah audit manajemen risiko TI menjadi esensial, memastikan bahwa LAZNAS XYZ atau organisasi pada umumnya memiliki kontrol yang kuat untuk melindungi data dan menjaga kepatuhan terhadap regulasi yang ada [6].

Dalam melakukan audit manajemen risiko di lembaga tersebut kerangka kerja COBIT 2019 digunakan karena menawarkan pendekatan komprehensif untuk audit manajemen risiko serta tata kelola TI secara keseluruhan. Memastikan bahwa manajemen risiko dan tata kelola TI menjadi bagian integral yang menyatu, tidak hanya sebagai proses terpisah. 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). COBIT 2019, dapat menilai efektivitas kapabilitas dalam mengelola risiko TI dan mengidentifikasi area yang memerlukan perbaikan. Proses audit menggunakan COBIT 2019 memungkinkan untuk tidak hanya mengidentifikasi risiko, tetapi juga mengoptimalkan kontrol yang ada dan memastikan bahwa proses-proses TI mendukung tujuan strategis organisasi. Kerangka kerja ini memberikan panduan yang jelas untuk mengukur kapabilitas proses dan mengembangkan kebijakan pengelolaan risiko yang lebih baik [7]. Hal ini akan membantu lembaga yang di audit untuk meningkatkan transparansi dan akuntabilitas, yang pada gilirannya dapat memperkuat kepercayaan donatur dan mitra. Selain itu, dengan pendekatan TI berbasis standar, LAZNAS XYZ dapat memastikan bahwa manajemen risiko TI mereka selalu selaras dengan praktik terbaik internasional dan adaptif terhadap perubahan regulasi.

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 penelitian yang benar serta dapat bermanfaat dalam pengembangan penelitian bertema sama di masa mendatang. Penelitian pertama, 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 [8]. Penelitian kedua 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 [9]. Penelitian ketiga 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 [10]. Penelitian keempat berfokus pada analisis manajemen risiko teknologi informasi (TI) di Perguruan Tinggi XYZ menggunakan framework COBIT 2019, khususnya domain APO12 yang berkaitan dengan *"Manage Risk."* Tujuan utama penelitian ini adalah untuk mengukur dan mengevaluasi tingkat kapabilitas manajemen risiko TI di perguruan tinggi tersebut. [11].

Penelitian kelima berfokus pada evaluasi tata kelola teknologi informasi di perusahaan layanan TI menggunakan kerangka kerja COBIT 2019. 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 [12]. Penelitian keenam, fokus dari penelitian ini adalah menilai tata kelola teknologi informasi dan tingkat kapabilitas di PT Kwadran Lima, Indonesia, menggunakan kerangka kerja COBIT 2019. 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 [13]. Penelitian ketujuh 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

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Cendekia Indonesia dan mengukur tingkat kapabilitasnya sebagai bahan evaluasi untuk memberikan rekomendasi yang mendukung optimalisasi kinerja TI perusahaan [14]. Penelitian kedelapan berfokus pada analisis efisiensi dan efektivitas pengelolaan dana Zakat, Infak, dan Sedekah (ZIS) di Laznas Baitulmaal Muamalat, yang merupakan Lembaga Amil Zakat Nasional. 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 [15].

Dengan demikian, tujuan penelitian ini adalah menerangkan akan pentingnya audit manajemen risiko pengelolaan risiko TI dalam organisasi. Setelah menjalani audit manajemen risiko yang komprehensif, Lembaga Amil Zakat Nasional (LAZNAS) XYZ 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 Nasional. Pada umumnya, COBIT 2019 sering digunakan pada organisasi yang bergerak di sektor komersial atau pemerintahan. Namun, penelitian ini mengimplementasikan kerangka kerja tersebut dalam konteks pengelolaan risiko di LAZNAS XYZ. 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.

2. Metode Penelitian

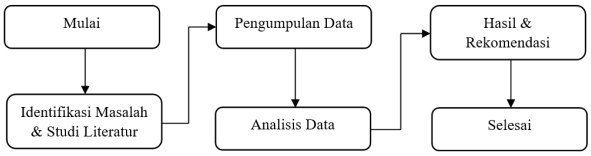
Metode Penelitian *(research method)* digunakan oleh peneliti sebagai cara atau pendekatan untuk mengumpulkan, menganalisis, dan menarik kesimpulan dari data yang diperoleh selama penelitian [16]. Metode ini sangat penting karena menentukan bagaimana penelitian dilakukan dan bagaimana hasilnya akan dianalisis untuk menjawab pertanyaan penelitian dan mencapai tujuan penelitian.

2.1. 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. Memungkinkan peneliti untuk mengeksplorasi, memahami, dan menggambarkan fenomena yang terjadi secara detail dan mendalam [17]. Sifat penelitian ini adalah eksploratif. Sifat eksploratif bertujuan untuk menggali informasi, mengidentifikasi masalah, dan memahami fenomena yang belum banyak diteliti sebelumnya [18]. 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 [19].

2.2. Alur Penelitian

Alur penelitian pada penelitian ini difungsikan sebagai langkah-langkah atau prosedur yang perlu diikuti agar tercapai tujuan penelitian [20]. Agar penelitian dapat digambarkan dengan jelas dan mudah dipahami maka dibentuklah alur sederhana dalam 4 tahapan seperti pada Gambar 1 beserta penjelasannya.



Gambar 1. Alur Penelitian

Adapun penjelasan dari Gambar 1 di uraikan berdasarkan 4 tahapan berikut :

a. Tahap 1

Identifikasi masalah & studi literatur, di mana langkah awalnya adalah mengidentifikasi permasalahan yang akan dikaji. Setelah itu, dilakukan studi literatur yang mencakup studi pustaka dan studi dokumen. Studi pustaka dilakukan dengan mengacu pada referensi dari buku, jurnal, atau artikel ilmiah yang relevan, sementara studi dokumen menggunakan dokumen-dokumen terkait untuk mendapatkan informasi tambahan yang mendukung penelitian.

b. Tahap 2

Pengumpulan data, yang diawali dengan penentuan faktor desain *(design factor)* dan pemilihan domain penelitian. Setelah domain dipilih, proses pengumpulan data dilakukan dengan tiga metode utama, yaitu pemetaan RACI, wawancara, dan kuesioner. Pemetaan RACI digunakan untuk mengidentifikasi peran dan tanggung jawab individu dalam suatu proses, wawancara dilakukan untuk menggali informasi secara mendalam dari narasumber, dan kuesioner digunakan untuk mendapatkan data dari sejumlah responden secara terstruktur. Setelah data terkumpul, tahap ini berakhir dengan penyusunan data untuk dianalisis lebih lanjut.

c. Tahap 3

Data yang telah dikumpulkan dianalisis dengan pendekatan penilaian dan gap analisis. Penilaian dilakukan untuk mengevaluasi data yang diperoleh,

P-ISSN : 2089-3353
E-ISSN : 2808-9162

sedangkan analisis gap digunakan untuk mengidentifikasi kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan. Dari hasil analisis ini, diperoleh temuan utama yang menjadi dasar dalam penyusunan rekomendasi penelitian.

d. Tahap 4

Rekomendasi dan kesimpulan merupakan tahap di mana hasil analisis digunakan untuk menyusun rekomendasi sebagai solusi terhadap permasalahan yang telah diidentifikasi sebelumnya. Setelah rekomendasi dibuat, penelitian diakhiri dengan penyusunan kesimpulan yang merangkum seluruh temuan dan hasil penelitian. Dengan demikian, penelitian ini dapat memberikan wawasan yang bermanfaat dan menjadi dasar untuk langkah selanjutnya dalam bidang yang diteliti.

2.3. Metode Pengumpulan Data

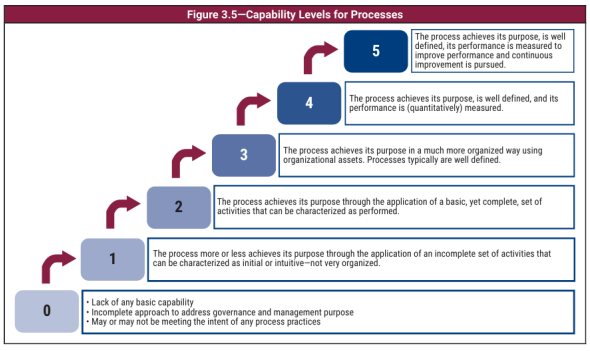
Dalam penelitian ini, metode pengumpulan data dilakukan secara sistematis untuk memastikan bahwa informasi yang diperoleh akurat dan relevan dengan tujuan penelitian. Pengumpulan data dilakukan melalui tiga metode utama, yaitu observasi, wawancara, dan kuesioner, yang sesuai dengan tahapan yang telah dirancang dalam penelitian ini. Data yang dikumpulkan dalam penelitian ini terdiri dari data primer dan data sekunder [21]. Data primer diperoleh langsung dari responden melalui observasi, wawancara, dan kuesioner. Sementara itu, data sekunder dikumpulkan dari berbagai sumber seperti laporan organisasi, dokumen kebijakan, serta literatur yang relevan dengan manajemen risiko TI dan *framework* COBIT 2019. Penggunaan data primer dan sekunder ini memungkinkan penelitian untuk mendapatkan wawasan yang lebih komprehensif dan mendalam mengenai kondisi yang sedang diteliti [22].

Metode yang pertama observasi, dilakukan untuk memahami secara langsung bagaimana praktik manajemen risiko TI diterapkan dalam organisasi. Melalui metode ini, peneliti dapat mengamati alur kerja, interaksi antar pemangku kepentingan, serta proses yang berkaitan dengan pengelolaan risiko TI. Observasi dilakukan dengan pendekatan non-partisan, yaitu tanpa memihak atau mempengaruhi dinamika organisasi yang sedang diamati. Dengan demikian, hasil observasi dapat memberikan gambaran objektif mengenai praktik yang diterapkan dan area yang memerlukan perbaikan [23]. Kemudian Wawancara dilakukan dengan pihak-pihak yang memiliki peran penting dalam pengelolaan risiko TI di organisasi. Tujuan wawancara ini adalah untuk menggali informasi secara lebih mendalam mengenai tantangan yang dihadapi serta efektivitas strategi yang telah diterapkan dalam organisasi [24]. Pertanyaan yang diajukan dalam wawancara disusun berdasarkan aspek-aspek kunci dalam framework COBIT 2019, sehingga hasilnya dapat memberikan wawasan yang lebih komprehensif mengenai kondisi manajemen risiko TI dalam organisasi yang diteliti. Selanjutnya Kuesioner digunakan untuk mengumpulkan data dari berbagai responden secara sistematis. Dalam penyusunan kuesioner, digunakan pendekatan RACI *(Responsible, Accountable, Consulted, Informed)* untuk memastikan bahwa responden yang dipilih memiliki relevansi dengan proses manajemen risiko TI [25]. Kuesioner dirancang untuk mendapatkan pandangan yang lebih jelas mengenai efektivitas manajemen risiko TI dalam organisasi [26]. Pertanyaan dalam kuesioner mencakup berbagai aspek terkait manajemen risiko TI, termasuk identifikasi risiko, mitigasi risiko, serta pemantauan dan keberlanjutan strategi yang diterapkan.

Setelah data terkumpul, langkah selanjutnya adalah melakukan pengolahan dan analisis data. Data yang diperoleh dari observasi, wawancara, dan kuesioner dikompilasi untuk mendapatkan gambaran yang lebih jelas mengenai kondisi manajemen risiko TI di organisasi yang diteliti. Dengan pendekatan ini, penelitian dapat menghasilkan temuan yang lebih valid dan dapat digunakan sebagai dasar dalam penyusunan rekomendasi yang lebih tepat guna [27]. Secara keseluruhan, metode pengumpulan data yang digunakan dalam penelitian ini memastikan bahwa informasi yang diperoleh mencerminkan kondisi nyata yang ada, sehingga dapat memberikan kontribusi berarti dalam evaluasi serta perbaikan sistem manajemen risiko TI pada organisasi yang direkomendasikan berdasarkan *framework* COBIT 2019.

2.4. Metode Analisis Data

Data yang diperoleh dianalisis secara deskriptif untuk memberikan gambaran mendalam mengenai praktik manajemen risiko TI di LAZNAS XYZ, mengidentifikasi pengaruhnya terhadap pengelolaan risiko TI. Kemudian analisis tingkat kapabilitas dilakukan dengan mengacu pada model kematangan COBIT 2019. Proses ini bertujuan untuk mengukur sejauh mana kapabilitas pengelolaan risiko TI dalam organisasi telah memenuhi standar yang direkomendasikan [28]. Penilaian dilakukan dengan menggunakan skala kapabilitas COBIT 2019, yang terdiri dari Level 0 (Tidak Ada/*Incompleted*), Level 1 (Dilakukan/*Performed*), Level 2 (Dikelola/*Managed*), Level 3 (Ditetapkan/*Established*), Level 4 (Dapat diprediksi/*Predictable*), dan Level 5 (Mengoptimalkan/*Optimizing*). Berikut informasi lebih rinci mengenai level capability level pada COBIT 2019, terlihat pada Gambar 2.



Gambar 2. *Capability Level Process*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Selanjutnya analisis kesenjangan (*gap analysis*) diterapkan untuk mengidentifikasi perbedaan antara kondisi saat ini dan kondisi ideal yang diinginkan berdasarkan COBIT 2019 [29]. Melalui analisis ini, penelitian dapat menentukan area yang memerlukan perbaikan serta menyusun rekomendasi yang lebih efektif untuk meningkatkan kapabilitas manajemen risiko TI di LAZNAS XYZ. Dengan menerapkan metode analisis data ini, penelitian diharapkan dapat memberikan hasil yang akurat dan bermanfaat dalam meningkatkan tata kelola serta manajemen risiko TI di LAZNAS XYZ.

3. Hasil dan Pembahasan

Bagian ini menyajikan temuan utama dari analisis manajemen risiko TI pada Lembaga Amil Zakat Nasional XYZ dengan pendekatan COBIT 2019. Hasil penelitian dikaji berdasarkan domain dan proses yang relevan dalam kerangka kerja COBIT 2019, dengan fokus pada tingkat kapabilitas, kesenjangan antara kondisi yang ada dan target, serta rekomendasi peningkatan. Selain itu, pembahasan dilakukan untuk menyoroti implikasi dari hasil yang diperoleh terhadap efektivitas pengelolaan risiko TI, kepatuhan terhadap standar yang berlaku, serta dampaknya terhadap operasional lembaga.

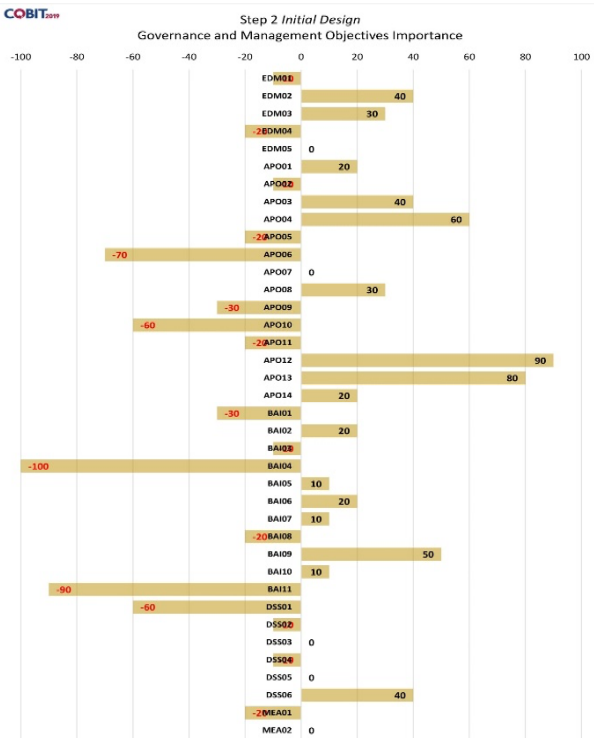
3.1 Observasi

Observasi dilakukan secara non-partisipan, di mana pengamat tidak terlibat langsung dalam aktivitas yang diamati, tetapi hanya mengamati dan mencatat temuan berdasarkan pengelolaan TI dan manajemen risiko TI di Lembaga Amil Zakat Nasional XYZ. Observasi ini bertujuan untuk mendapat gambaran mengenai praktik pengelolaan risiko TI yang telah diterapkan dalam organisasi. Proses observasi dilakukan dengan mengikuti setiap aktivitas yang berkaitan dengan pengelolaan risiko TI pada LAZNAS XYZ, mulai dari pengumpulan data risiko TI, identifikasi & analisis data risiko TI, penyusunan kebijakan risiko TI, implementasi kebijakan risiko TI, hingga pemantauan & evaluasi pengelolaan risiko TI. Temuan atau hasil observasi dituangkan ke dalam *Design Factor* COBIT 2019 yang meliputi faktor *Enterprise Strategy (DF1), Enterprise Goal (DF2), Risk Profile (DF3), dan IT-Related Issues (DF4).* Berikut informasi dari hasil observasi tersaji dalam bentuk Tabel 1 di bawah.

Tabel 1. Hasil Observasi

No	Faktor	Keterangan
1	DF1	Strategi TI telah mendukung misi sosial lembaga, meskipun masih ada ruang untuk perbaikan strategi, terkhusus strategi penanganan risiko TI agar lebih optimal.
2	DF2	Pengelolaan TI secara umum selaras dengan tujuan organisasi, namun perlu ada pembenahan khususnya terkait cara mengukur keberhasilan implementasi kebijakan risiko TI.
3	DF3	Pengenalan risiko TI telah dilakukan, tetapi masih perlu penguatan seperti dalam memantau ancaman, serta risiko TI yang terus berkembang.
4	DF4	Ditemukan beberapa isu yang menyangkut pengelolaan keamanan serta risiko TI, diantaranya isu kepatuhan terhadap regulasi dan isu kepercayaan donatur terhadap lembaga.

Dari 4 faktor *Design Factor* COBIT 2019 tersebut, menghasilkan gambaran menyeluruh di bagian *Step 2 Initial Design*, seperti yang terlihat pada Gambar 3.



Gambar 3. *Initial Design*

Hasil *Initial Design* pada *Design Factor* menunjukkan COBIT *Core Model* atau domain yaitu APO12 diangka 90 dan APO13 diangka 80 memiliki tingkat kepentingan yang tinggi, menandai kebutuhan untuk memperkuat pengelolaan risiko dan keamanan TI pada organisasi, selain pada dua domain tersebut peneliti melihat ada relevansi domain lainnya yaitu EDM3 walaupun memiliki tingkat kepentingan yang lebih kecil yaitu diangka 30, domain tersebut erat kaitannya dengan risiko sehingga perlu untuk diikutsertakan. Berikut keterangan domain yang terpilih dapat dilihat pada Tabel 2.

Tabel 2. Domain

No	Domain	Pembahasan
1	EDM 03	*Ensure Risk Optimization*
2	APO 12	*Manage Risk*
3	APO 13	*Manage Security*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

3.2. Wawancara

Setelah mengetahui domain mana saja yang terpilih maka langkah berikutnya adalah menentukan responden untuk diwawancarai. Penentuan responden ini akan diawali dengan menyinkronkan peran-peran yang ditentukan oleh COBIT 2019 berdasarkan domain yang terpilih dengan peran-peran yang ada pada organisasi. Berikut hasil sinkronisasi peran responden untuk diwawancarai terlihat pada Tabel 3.

Tabel 3. Peran Responden

COBIT 2019	LAZNAS XYZ
Chief Risk Officer	Kepatuhan, Risiko dan Audit (KRA)
Chief Information Officer	Direktur Operasional
Chief Digital Officer	Marcom, CRM & Digital (MCD)
Head IT Operations	Teknologi
Head IT Administration	Teknologi, Legal & General Affairs (TLG)

3.3. Kuesioner

Pembuatan kuesioner dalam penelitian ini didasarkan pada aktivitas yang terdapat dalam domain-domain COBIT 2019 yang telah terpilih, yaitu *APO12 (Manage Risk)*, APO13 *(Manage Security)*, dan EDM3 *(Ensure Risk Optimization)*. Domain APO12 mencakup 36 aktivitas, APO13 terdiri dari 19 aktivitas, dan EDM3 melibatkan 16 aktivitas. Kuesioner dirancang untuk mengumpulkan informasi dari responden yang terpilih, dengan tujuan sudah sejauh mana implementasi manajemen risiko TI di organisasi. Kuesioner disusun dengan pendekatan terstruktur untuk memastikan bahwa setiap pertanyaan mengacu pada praktik terbaik dalam kerangka kerja COBIT 2019.

Menggunakan skala guttman sebagai metode pengukuran. Skala guttman merupakan skala pengukuran yang bersifat konsisten dan tegas, berupa dua alternatif yang berbeda, misalnya "Ya" dan "Tidak". Skala guttman pada penelitian ini akan digunakan untuk menilai setiap aktivitas pada domain. Apabila aktivitas telah dilakukan maka akan diberikan skor nilai 1 dan apabila aktivitas belum dilakukan maka diberi skor nilai 0. Berikut rumus yang digunakan dalam perhitungan rekapitulasi jawaban kuesioner dengan skala guttman :

$$CC = \frac{\Sigma CLa}{\Sigma Po} x\ 100\% \quad (1)$$

Nilai pencapaian capability level *CC* merupakan hasil perbandingan antara jumlah aktivitas yang terlaksana dengan jumlah seluruh aktivitas dalam domain. Jumlah aktivitas yang terlaksana dilambangkan dengan *ΣCLa*, sedangkan jumlah seluruh aktivitas dalam domain dilambangkan dengan *ΣPo*. Hasil perbandingan ini dinyatakan dalam bentuk persentase untuk menggambarkan tingkat pencapaian *capability level*. Dengan menggunakan skala ini, hasil kuesioner dapat dianalisis secara lebih objektif dalam menentukan kesiapan dan tingkat kapabilitas organisasi dalam mengadopsi manajemen risiko berdasarkan COBIT 2019.

Kuesioner tidak hanya berfungsi sebagai alat pengumpulan data, tetapi juga sebagai cermin untuk mengevaluasi kesiapan organisasi dalam menghadapi tantangan TI. Hasilnya akan menjadi dasar rekomendasi spesifik, seperti peningkatan pelatihan atau adopsi perangkat manajemen risiko, yang dapat meningkatkan kapabilitas organisasi sehingga menjadi lebih tinggi berdasar COBIT 2019.

3.4. Analisis Deskriptif

Berdasarkan data dari kuesioner, analisis kapabilitas di Lembaga Amil Zakat Nasional XYZ menunjukkan implementasi yang cukup baik dalam pengelolaan risiko TI dan keamanan informasi, namun beberapa area masih perlu perbaikan. Domain EDM 03 *(Ensure Risk Optimization)* sebagian besar aktivitas terkait evaluasi, pengelolaan & pemantauan risiko TI sudah terlaksana dengan baik (nilai 1), meskipun ada beberapa aktivitas seperti mengidentifikasi tujuan utama metrik dari proses tata kelola dan manajemen risiko serta memantau tujuan utama metrik dari proses tata kelola dan manajemen risiko terhadap targetnya. Selanjutnya domain APO 12 *(Manage Risk)* Sebagian besar aktivitas dalam pengumpulan data, analisis, pemeliharaan, pengartikulasian, definisi dan respon risiko sudah dilaksanakan dengan baik, namun ada beberapa area yang masih perlu perhatian, seperti memvalidasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan serta peninjauan celah yang teridentifikasi dan eksposur kerugian terkait IT untuk menentukan kebutuhan akan analisis risiko tambahan serta. Terakhir domain APO 13 *(Manage Security)* Aktivitas pengelolaan keamanan informasi, terutama dalam membangun dan memelihara, mendefinisikan dan memelihara serta memantau dan meninjau sistem manajemen keamanan informasi, sudah terlaksana dengan baik. Namun, masih ada beberapa area yang perlu perbaikan, terutama dalam menentukan cara untuk mengukur efektivitas praktik manajemen keamanan informasi yang digunakan.

Secara keseluruhan, pengelolaan risiko TI dan keamanan informasi di Lembaga Amil Zakat Nasional XYZ sudah cukup baik, namun beberapa area seperti pemantauan berkala dan implementasi konsisten perlu diperbaiki untuk mencapai tingkat kapabilitas yang lebih tinggi.

3.5 Capability Level Test

Melakukan penilaian terhadap tingkat kapabilitas manajemen risiko TI di Lembaga Amil Zakat Nasional XYZ, 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. *Capability Level Processes* memiliki lima level kapabilitas yang menggambarkan perjalanan organisasi dalam meningkatkan manajemen dan

P-ISSN : 2089-3353
E-ISSN : 2808-9162

pengelolaan proses TI dari tahap yang paling dasar hingga tahap yang optimal.

Hasil dari uji kapabilitas ini akan memberikan gambaran mengenai sejauh mana masing-masing sub-domain tersebut diimplementasikan dan efektivitasnya dalam mengelola risiko TI. Selanjutnya, hasil uji kapabilitas ini juga akan menjadi dasar dalam menyusun rekomendasi untuk peningkatan manajemen risiko TI di organisasi yang diteliti. Penilaian terhadap kapabilitas manajemen risiko TI di Lembaga Amil Zakat Nasional XYZ dilakukan berdasarkan 3 domain berikut :

a. EDM 03 Ensure Risk Optimization

Tabel 4. 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	3
Rata-Rata		2,66 = 3

Tabel 4 menunjukkan hasil dari *Capability Level Test* untuk domain EDM 03 *Ensure Risk Optimization* yang mencakup tiga aktivitas utama. 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. Rata-rata untuk domain ini adalah 2,66, yang lebih mendekati 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.

b. APO 12 Manage Risk

Tabel 5. Capability Level Test APO 12

No	Sub Domain	Capability Level (as-is)
1	APO 13.01	4
2	APO 13.02	3
3	APO 13.03	3
4	APO 13.04	3
5	APO 13.05	3
6	APO 13.06	4
Rata-Rata		3,33 = 3

Tabel 5 menunjukkan hasil dari *Capability Level Test* untuk domain APO 12 *Manage Risk*, yang mencakup enam aktivitas utama. APO 12.02, APO 12.03, 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 12.06 menunjukkan level kapabilitas 4. Dengan Level 4 pada APO 12.01 dan APO 12.06, artinya organisasi telah mencapai level yang dapat diprediksi, berdasarkan data dan respon terhadap terhadap risiko yang ada saat ini dan yang mungkin terjadi di masa depan, namun tetap ada peluang peningkatan seperti terhadap komukasi kepada pengambil keputusan yang perlu dilengkapi dengan informasi yang utuh terhadap penyebab, respon serta perbaikan proses pengelolaan risiko. Rata-rata untuk domain ini adalah 3,33 dengan nilai yang paling dekat adalah level 3, menunjukkan bahwa pengelolaan risiko di organisasi ini berada pada level yang mapan, meskipun ada area-area yang masih membutuhkan penyempurnaan demi mencapai tingkat yang lebih baik.

c. APO 13 Manage Security

Tabel 6. 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	4
Rata-Rata		3

Tabel 6 menunjukkan hasil dari *Capability Level Test* untuk domain APO 13 *Manage Security*, yang mencakup tiga aktivitas utama. 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 4, yang berarti bahwa pemantauan dan peninjauan terkait manajemen keamanan sudah dapat diprediksi hasilnya. 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.

3.6. Gap Analisis

Mengetahui nilai gap dilakukan 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 Lembaga Amil Zakat Nasional XYZ. 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.

Tabel 7. Gap Domain

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

Tabel 7 di atas menggambarkan gap analisis yang dilakukan untuk tiga domain utama, EDM 03 *Ensure*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Risk Optimization, APO 12 *Manage Risk*, dan APO 13 *Manage Security*. EDM 03 secara keseluruhan menunjukkan bahwa saat ini organisasi berada pada level 3 yaitu mapan, dengan nilai gap 0 antara capability level saat ini dan target kapabilitas level yaitu level 3. Selanjutnya APO 12 saat ini menunjukkan level 3, sementara targetnya adalah level 4. Gap di sini sebesar 1, menunjukkan bahwa meskipun proses pengelolaan risiko TI sudah cukup mapan, tetapi masih diperlukan perbaikan untuk mencapai target kapabilitas level. APO 13 juga berada pada level 3 saat ini, dengan target level 4, menggambarkan adanya gap sebesar 1. Untuk mencapai target kapabilitas level 4, organisasi perlu mengoptimalkan proses manajemen keamanan TI dengan cara yang lebih inovatif dan berkelanjutan.

Rata-rata gap untuk ketiga domain ini adalah 1, yang menunjukkan bahwa secara keseluruhan, Lembaga Amil Zakat Nasional XYZ 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.

3.7. Rekomendasi

Berdasarkan hasil analisis gap kapabilitas level dan temuan penelitian, berikut rekomendasi yang disusun untuk meningkatkan manajemen risiko TI di LAZNAS XYZ :

a. *EDM 03 Ensure Risk Optimization*

Meskipun LAZNAS XYZ telah mencapai capability level 3 pada domain EDM 03 Ensure Risk Optimization, yang juga merupakan target level, ada beberapa area yang tetap perlu ditingkatkan untuk mempertahankan atau memperkuat kapabilitas yang ada. Pemantauan metrik risiko perlu diperkuat dengan menyusun prosedur pemantauan yang lebih rinci dan menetapkan metrik yang lebih spesifik untuk memastikan bahwa semua risiko tetap berada dalam batas toleransi yang dapat diterima. Organisasi disarankan untuk memperkenalkan prosedur pemantauan yang lebih terstruktur untuk mengidentifikasi penyimpangan lebih awal dan mengambil langkah mitigasi yang lebih tepat waktu, memastikan bahwa risiko yang ada dapat diatasi dengan cepat dan efisien.

Selain itu, organisasi harus meningkatkan evaluasi risiko secara lebih proaktif, dengan melibatkan tim lintas fungsi dalam proses identifikasi dan evaluasi risiko. Ini mencakup risiko eksternal yang mungkin tidak terdeteksi dalam proses pemantauan saat ini. Dengan evaluasi risiko yang lebih berkala dan memperkenalkan kerangka evaluasi risiko yang lebih komprehensif, LAZNAS XYZ dapat mengantisipasi ancaman lebih dini dan membuat keputusan yang lebih tepat sebelum risiko berkembang menjadi masalah besar. Dengan langkah-langkah ini, organisasi akan lebih siap menghadapi perubahan atau ancaman yang tidak terduga di masa depan..

b. APO 12 Manage Risk

Untuk mencapai target capability level 4 pada domain APO 12 Manage Risk, penting untuk memperbaiki beberapa aspek dalam pengumpulan data risiko dan validasi hasil analisis risiko. Meskipun pengumpulan data risiko telah dilakukan, perluasan cakupan dengan melibatkan sumber data eksternal, data historis, dan tren industri akan memberikan gambaran yang lebih lengkap tentang potensi ancaman. Dengan sistem pengumpulan data yang lebih komprehensif, LAZNAS XYZ akan dapat mendeteksi potensi risiko lebih awal dan mengidentifikasi area yang sebelumnya tidak terlihat. Penggunaan data yang lebih beragam memungkinkan organisasi untuk membuat keputusan yang lebih tepat dalam merencanakan mitigasi risiko.

Kemudian, proses validasi hasil analisis risiko perlu diperkuat untuk memastikan bahwa hasil yang diperoleh lebih akurat dan dapat diandalkan. Oleh karena itu, disarankan untuk memperkenalkan prosedur validasi yang lebih ketat dengan melibatkan berbagai pihak terkait dalam proses verifikasi hasil analisis. Selain itu, untuk mencapai level 4, penting untuk memperdalam analisis dampak bisnis agar hasilnya mencakup lebih banyak skenario risiko dan dapat diandalkan dalam proses pengambilan keputusan. Dengan langkah-langkah ini, LAZNAS XYZ dapat meningkatkan kapabilitasnya dalam mengelola risiko TI secara lebih efektif dan efisien.

c. APO 13 Manage Security

Pada domain *APO 13 Manage Security*, saat ini LAZNAS XYZ berada pada capability level 3, dan target capability level 4. Untuk mencapai target tersebut LAZNAS XYZ perlu memperbaiki cara memantau dan mengukur efektivitas kebijakan keamanan yang diterapkan. Organisasi perlu mengadopsi sistem pemantauan yang lebih baik yang memungkinkan untuk menilai secara rutin apakah kebijakan keamanan yang ada cukup efektif dalam mengidentifikasi dan menangani ancaman. Pemantauan ini akan memberikan gambaran yang jelas tentang keberhasilan kebijakan serta area mana yang perlu diperbaiki. Dengan cara ini, LAZNAS XYZ dapat melakukan penyesuaian yang cepat untuk memastikan kebijakan yang diterapkan selalu dapat mengatasi ancaman dengan baik.

Disisi lain, LAZNAS XYZ perlu memperkuat proses audit dan pengujian sistem keamanan secara berkala untuk memastikan bahwa kebijakan dan sistem yang ada tetap efektif seiring berjalannya waktu. Disarankan untuk melakukan audit rutin serta pengujian penetrasi untuk mendeteksi potensi kerentanannya sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Selain itu, pelatihan berbasis simulasi untuk staf mengenai bagaimana merespon ancaman secara tepat juga sangat penting. Dengan simulasi ini, staf akan

P-ISSN : 2089-3353
E-ISSN : 2808-9162

lebih siap menghadapi dan mengatasi masalah keamanan dengan lebih efisien.

4. Kesimpulan

Penelitian ini mengevaluasi manajemen risiko TI di Lembaga Amil Zakat Nasional (LAZNAS) XYZ menggunakan kerangka kerja COBIT 2019. Hasil analisis menunjukkan bahwa LAZNAS XYZ telah mencapai tingkat kapabilitas yang memadai dalam pengelolaan risiko TI, khususnya pada domain EDM 03 (Ensure Risk Optimization), APO 12 (Manage Risk), dan APO 13 (Manage Security). Namun, masih terdapat kesenjangan antara kondisi saat ini (as-is) dan target (to-be), terutama pada domain APO 12 dan APO 13, yang memerlukan penyempurnaan untuk mencapai level kapabilitas yang lebih tinggi.

Implikasi dari temuan ini adalah bahwa penerapan COBIT 2019 dapat membantu LAZNAS XYZ meningkatkan transparansi, akuntabilitas, dan kepercayaan donatur melalui pengelolaan risiko TI yang lebih efektif. Dengan memperbaiki proses pemantauan risiko, validasi analisis, dan pengukuran efektivitas keamanan, organisasi dapat mengurangi potensi gangguan operasional dan kerugian finansial. Selain itu, pendekatan ini juga mendukung kepatuhan terhadap regulasi dan standar internasional, yang sangat penting bagi lembaga filantropi yang mengelola data sensitif.

Sebagai saran untuk penelitian selanjutnya, disarankan untuk mengeksplorasi integrasi kerangka kerja lain seperti ISO 27001 atau ISO 31000 guna memperkuat analisis manajemen risiko TI. Studi lanjutan juga dapat dilakukan pada organisasi filantropi sejenis untuk membandingkan temuan dan mengembangkan praktik terbaik yang lebih komprehensif. Dengan demikian, penelitian ini tidak hanya memberikan rekomendasi praktis bagi LAZNAS XYZ, tetapi juga membuka peluang pengembangan pengetahuan dalam penerapan tata kelola TI di sektor nirlaba.

Daftar Rujukan

[1] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of E-Business Information System in Indonesia: Prospects and Challenges," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 180-188, Oct. 2021. doi: 10.34306/ijcitsm.v1i2.49.

[2] G. Robertsone and I. Lapiņa, "Digital Transformation as a Catalyst for Sustainability and Open Innovation," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 9, no. 1, p. 100017, Mar. 2023, doi: 10.1016/j.joitmc.2023.100017.

[3] I. Beerepoot *et al.*, "The Biggest Business Process Management Problems to Solve Before We Die," *Computers in Industry*, vol. 146, p. 103837, Apr. 2023, doi: 10.1016/j.compind.2022.103837.

[4] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, and D. Guerri, "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach," *Cognition, Technology and Work*, vol. 24, no. 2, pp. 371–390, May 2022, doi: 10.1007/s10111-021-00683-y.

[5] D. Settembre-Blundo, R. González-Sánchez, S. Medina-Salgado, and F. E. García-Muiña, "Flexibility and Resilience in Corporate Decision Making: A New Sustainability-Based Risk Management System in Uncertain Times," *Global Journal of Flexible Systems Management*, vol. 22, pp. S107–S132, Dec. 2021, doi: 10.1007/s40171-021-00277-7.

[6] M. Ikhlas Rosele, A. Muneem, N. Naemah Binti Abdul Rahman, and A. Karim Ali, "The Digitalized Zakat Management System in Malaysia and the Way Forward," *Jurnal Hukum dan Pranata Sosial*, vol. 17, no. 1, pp. 242–272, 2022, doi: 10.19105/al-Ihkam.v17i1.5365.

[7] ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*. Rolling Meadows, IL: ISACA, 2018. ISBN 978-1-60420-764-4.

[8] A. Safitri, I. Syafii, and K. Adi, "Measuring the Performance of Information System Governance using Framework COBIT 2019," International Journal of Computer Applications, vol. 174, no. 31, pp. 23–30, Apr. 2021. doi: 10.5120/ijca2021921253.

[9] H. Berrada, J. Boutahar, and S. El Ghazi El Houssaini, "Simplified IT Risk Management Maturity Audit System Based on COBIT 5 for Risk." *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, pp. 641–652, 2021. doi: 10.14569/IJACSA.2021.0120875.

[10] R. Setyadi and H. N. Prabowo, "Risk Management Analysis of Bus Transportation Application Using COBIT 4.1," *Jurnal Teknologi dan Sistem Informasi*, vol. 7, no. 2, pp. 203–212, Apr. 2021, doi: 10.33330/jurteksi.v7i2.1046.

[11] R. Anugrah, E. Utami, and A. H. Muhammad, "Analisis Manajemen Risiko TI pada Perguruan Tinggi XYZ Berbasis COBIT 2019 dengan Pertimbangan Domain APO12," *Jurnal Ilmiah Universitas Batanghari Jambi*, vol. 22, no. 2, pp. 991-995, Jul. 2022, doi: 10.33087/jiubj.v22i2.2175.

[12] E. Enrique and M. I. Fianty, "Enhancing Risk Management in an IT Service Company: A COBIT 2019 Framework Approach," *Jurnal Riset Informatika*, vol. 5, no. 4, pp. 499–506, Sep. 2023, doi: 10.34288/jri.v5i4.212.

[13] M. Brian Hardjadinata and J. Wiratama, "Capability Assessment of IT Governance Using the COBIT 2019 Framework for the IT Business Consultant Industry." *International Journal of Science, Technology & Management*, vol. 4, no. 4, pp. 1034–1039, Jul. 2023. doi: 10.46729/jjstm.v4i4.902.

[14] A. Harits, G. Muhamad Noer, and A. P. Widodo, "Capability Level Measurement Using COBIT 5: A Case Study of PT Jasa Cendekia Indonesia," *Journal of Information Systems and Informatics*, vol. 3, no. 2, pp. 341-351, 2021, doi:10.33557/journalisi.v3i2.134.

[15] H. Mualo and A. N. Rohim, "Analisis Efisiensi dan Efektivitas Pengelolaan Dana ZIS pada LAZNAS Baitulmaal Muamalat," Islamic Economics and Business Review, vol. 2, no. 1, pp. 11–23, 2023. [Online]. Available: https://ejournal.upnyi.ac.id/edst/n/article/view/5490.

[16] G. Guest, E. Namey, and M. Chen, "A Simple Method to Assess and Report Thematic Saturation in Qualitative Research," *PLOS One*, vol. 15, no. 5, p. e0232076, May 2020, doi: 10.1371/journal.pone.0232076.

[17] A. R. Tanaamah, A. F. Wijaya, and S. A. Maylinda, "Tata Kelola Teknologi Informasi pada Sektor Publik: Penyelarasan Teknologi Informasi dengan Visi Kepemimpinan (Studi Kasus: Kota Salatiga dan Kabupaten Bengkayang*)," Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 8, no. 6, pp. 1319-1330, Dec. 2021, doi: 10.25126/jtiik.202185379.

[18] F. Ebert, F. Castor, N. Novielli, and A. Serebrenik, "An Exploratory Study on Confusion in Code Reviews," *Empirical Software Engineering*, vol. 26, no. 12, pp. 1-48, Jan. 2021, doi: 10.1007/s10664-020-09909-5.

[19] R. Bell and V. Warren, "Illuminating a Methodological Pathway for Doctor of Business Administration Researchers: Utilizing Case Studies and Mixed Methods for Applied Research," *Social Sciences and Humanities Open*, vol. 7, no. 1, p. 100391, Jan. 2023, doi: 10.1016/j.ssaho.2022.100391.

[20] E. Barroga and G. J. Matanguihan, "Creating Logical Flow in Scientific Article Writing," *J Korean Med Sci*, vol. 36, no. 40, p. e275, Oct. 2021, doi: 10.3346/jkms.2021.36.e275.

[21] N. Aminudin, F. Aprilia, S. B. Wicaksono, A. Z. Salsabila A, and F. Ardhy, "Inovasi Sistem Layanan dan Rujukan Terpadu (SLRT) Bersahaja di Kabupaten Pringsewu: Evaluasi dan Kontribusinya terhadap Pengentasan Kemiskinan" *Jurnal Fasilkom*, vol. 15, no. 1, pp. 40-48, Apr. 2025, doi: 10.37859/jf.v15i1.8520.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

[22] A. Schneider *et al.*, "Primary and Secondary Data in Emergency Medicine Health Services Research: A Comparative Analysis in a Regional Research Network on Multimorbid Patients," *BMC Medical Research Methodology*, vol. 23, no. 1, pp. 1-12, Dec. 2023, doi: 10.1186/s12874-023-01855-2.

[23] L. Busetto, W. Wick, and C. Gumbinger, "How to Use and Assess Qualitative Research Methods," May 27, 2020, *Neurological Research and Practice,* vol. 2, no. 14, pp. 1–10, 2020. doi: 10.1186/s42466-020-00059-z.

[24] Y. Kamil, S. Lund, and M. S. Islam, "Information Security Objectives and Output Legitimacy of ISO/IEC 27001: Stakeholders' Perspectives in Swedish Private Organizations," *Information Systems and e-Business Management*, vol. 2, no. 14, pp. 699–722, 2020, doi: 10.1007/s10257-023-00646-y.

[25] M. Shilenge and A. Telukdarie, "4IR Integration of Information Technology Best Practice Framework in Operational Technology," *Journal of Industrial Engineering and Management*, vol. 14, no. 3, pp. 457–476, 2021, doi: 10.3926/jiem.3429.

[26] S. Varga, J. Brynielsson, and U. Franke, "Cyber-Threat Perception and Risk Management in the Swedish Financial Sector," *Comput & Security*, vol. 105, p. 102239 Jun. 2021, doi: 10.1016/j.cose.2021.102239.

[27] D. Triyunsari, E. S. Negara, M. I. Herdiansyah, and N. R. Damayanti, "Analisis Tingkat Kesiapan Teknologi Sistem Informasi Perpustakaan SMA Negeri 19 Palembang Menggunakan Framework ITIL V3," *Jurnal Fasilkom*, vol. 14, no. 3, pp. 695-704, Dec. 2024, doi: 10.37859/jf.v14i3.8215.

[28] D. P. Siagian, B. Purwandari, and N. W. Trisnawaty, "Enhancing Information Technology Maturity Using COBIT 2019: A Case Study of ABC University," *The Indonesian Journal of Computer Science*, vol. 14, no. 1, pp. 434-454, Feb. 2025, doi: 10.33022/ijcs.v14i1.4638.

[29] A. Yusuf, W. A. Saputra, and Jamilah, "Capability Gap Analysis in IT Governance for a Logistics Company Using COBIT 2019," *Journal of Information Systems and Informatics*, vol. 6, no. 3, pp. 1804–1821, Sep. 2024, doi: 10.51519/journalisi.v6i3.832.