BAB I
PENDAHULUAN

1.1 Latar Belakang

Percepatan transfromasi digital memaksa setiap organisasi mengadopsi Teknologi Informasi (TI) secara masif. Dalam era digitalisasi, internet memegang peran penting dalam pelbagai aktivitas lembaga. Menurut pernyataan Slamet Aji Pamungkas, Deputi Bidang Keamanan Siber dan Sandi Perekonomian BSSN, selama kurun waktu Januari hingga Mei 2024, tercatat sekitar 74 juta aktivitas digital yang dikategorikan sebagai anomali. Dari total tersebut, lebih dari 44 juta aktivitas diduga kuat merupakan serangan malware atau tindakan berbahaya yang berasal dari perangkat lunak yang tidak sah. Data ini mencerminkan tingginya tingkat ancaman keamanan siber yang dihadapi Indonesia, khususnya di sektor ekonomi digital yang terus berkembang pesat (CNN Indonesia, 2024). Selain dapat menyalahgunakan dan merusak data pribadi, *cybercrime* juga sangat berpotensi merusak aktivitas ekonomi dan bisnis (BPPTIK, 2023). Maka dari itu, mempertahankan data digital menjadi hal yang harus menjadi prioritas utama.

Keamanan sistem informasi yang telah menjadi prioritas dalam menjaga keberlangsungan organisasi baik profit, non-profit, maupun pemerintahan harus siap dalam menghadapi ancaman serangan siber. Sejak era indsutri global 4.0 yang banyak mengadopsi teknologi digital, *Internet of Things* (IoT), serta komputasi awan untuk mengelola *big data*, namun semuanya akan sia-sia jika tidak diimbangi dengan membangun sistem keamanan dalam melawan ancaman eksternal maupun dari internal perusahaan (Yusnanto et al., 2021). Regulasi terkait praktik penerapan keamanan informasi telah diatur dalam UU No. 11 Th. 2008 tentang informasi dan transaksi elektronik yang mengatur aspek keamanan informasi secara elektronik dan juga melalui Permen PAN & RB No. 47 Tahun 2018 sebagai acuan dalam pengamanan sistem informasi di instansi pemerintahan, dan pemerintah telah mengeluarkan panduan dalam menerapkan tata kelola keamanan informasi bagi penyelenggara *public service* yang mengacu pada Standar Nasional Indonesia yaitu ISO/IEC 27001 dengan

tujuan memastikan organisasi, perusahaan, maupun pemerintahan patuh terhadap peraturan yang berlaku (Manaek et al., 2023).

Dalam pengelolaan data dan Teknologi Informasi (TI) organisasi, dibutuhkan peran dari kerangka kerja Tata Kelola Teknologi Informasi (TKTI) yang telah teruji keefektifannya serta diakui sebagai standar internasional. *Control Objectives for Information and related Technology* (COBIT) sebagai *framework* komprehensif dengan fokus manajemen TI (Karkoskova & Feuerlicht, 2015). COBIT dirilis pada tahun 1996 dengan tujuan memudahkan petugas audit keuangan memonitor perkembangan di lingkungan TI dan dilakukan rilis pembaharuan oleh ISACA pada tahun 1998. COBIT versi 3 dan 4 dirilis pada tahun 2000-an yang mencakup pedoman lebih lanjut seputar keamanan siber. Lalu pada tahun 2012 COBIT 5 dipublikasikan dengan mengacu dan mengintegrasikan standar ISO, *Information Technology Infrastructure Library* (ITIL), dan *Project Management Body of Knowledge* (PMBOK). Pada tahun 2018, COBIT 2019 secara resmi diluncurkan sebagai versi terbaru hingga saat ini, dengan kerangka kerja yang lebih universal, menyeluruh, dan fleksibel, sehingga dapat diadopsi oleh berbagai jenis dan tingkat organisasi (Harisaiprasad Kumaragunta, 2020).

COBIT 2019 ini merupakan pembaharuan yang sangat besar dari versi COBIT sebelumnya, karena COBIT 2019 ini dibangun dengan mengintegrasikan lebih dari 27 tahun pengembangan di bidang COBIT untuk beradaptasi dengan perkembangan teknologi terkini saat ini (Sari et al., 2023). COBIT 2019 merupakan kerangka kerja terbaik dan sering digunakan dalam praktik pengelolaan data & TI khususnya pada sektor keamanan informasi karena terbagi menjadi bagian-bagian yang membahas isu tertentu dan dalam hal ini berfokus pada area keamanan informasi (Anugerah, 2023). Berbeda dengan pendahulunya yaitu COBIT 5 yang hanya memiliki 37 core model, COBIT 2019 dengan pembaharuannya memiliki 40 core model yang menjadikannya kerangka kerja paling optimal dalam manajemen TI (Wulandari et al., 2022).

Sebagai kerangka kerja, COBIT 2019 memiliki 5 domain yang mencakup berbagai aspek manajemen dan pengendalian teknologi informasi. Kelima domain COBIT 2019 ini dimaksudkan untuk memberikan panduan yang komprehensif dan terintegrasi guna mengatasi tantangan yang dihadapi

organisasi dalam mengelola sumber daya TI mereka. Lima domain yang dimaksud ialah *Evaluate, Direct, and Monitor* (EDM) memastikan bahwa teknologi informasi digunakan sesuai dengan tujuan organisasi dan dikelola dengan baik melalui pengawasan internal, manajemen risiko, dan pengukuran kinerja; *Align, Plan, and Organize* (APO) bertanggungjawab dalam perencanaan dan pengelolaan pemanfaatan Teknologi Informasi (TI) agar sejalan dengan arah dan strategi bisnis organisasi; *Build, Acquire, and Implement* (BAI) membahas terkait pembangunan dan penerapan sistem informasi baru. Aktivitas dalam domain ini mencakup proses perencanaan, pengembangan, serta pengujian guna memastikan bahwa sistem yang dihasilkan betul-betul sesuai kebutuhan dan tujuan bisnis organisasi; *Deliver, Service, and Support* (DSS) memastikan bahwa layanan teknologi informasi yang diberikan kepada pengguna selalu berkualitas, andal, dan sesuai dengan kebutuhan; dan *Monitor, Evaluate, and Assess* (MEA) memastikan bahwa sistem IT terus ditingkatkan dengan cara memantau kinerja, mengidentifikasi area yang perlu diperbaiki, dan mengukur tingkat kepatuhan terhadap kebijakan (ISACA, 2019b). Dari 40 kegiatan yang terdapat pada COBIT 2019, ada 3 sub-domain yang berkorelasi dengan keamanan informasi yaitu APO12 (pengelolaan risiko), APO13 (pengelolaan keamanan) dan DSS05 (pengelolaan layanan keamanan) (Nasiri, 2023).

Seiring dengan peningkatan penggunaan sistem digital di berbagai sektor, termasuk dalam organisasi non-profit seperti Lembaga Amil Zakat, Infak, dan Sedekah (LAZIS), ancaman terhadap keamanan data dan informasi semakin meningkat. LAZIS Sabilillah Malang yang mengelola data keuangan data pribadi para donator, dan data penerima manfaat, sangat bergantung pada sistem informasi yang aman dan andal untuk menjaga kepercayaan publik dalam melindungi data sensitif.

Pada Juni 2022, insiden keamanan yang signifikan terjadi pada infrastruktur utama penyimpanan data organisasi, yaitu *Network Attached Storage* (NAS) merk Synology DS220+ berkapasitas 4TB. NAS ini memiliki peran sentral sebagai penyimpanan file operasional, *database*, server LibreNMS, server *Voice over Internet Protocol* (VoIP), serta server website Sistem Informasi

LAZIS Sabilillah Terpadu (SILAT). Perangkat tersebut terhubung ke jaringan internal dan dapat diakses dari luar melalui layanan Synology QuickConnect.

Serangan *ransomware* yang tidak diketahui variannya berhasil mengenkripsi seluruh file pada NAS, mengubah ekstensi file, serta meninggalkan berkas readme yang berisi klaim dari pihak pelaku yang mengatasnamakan diri sebagai El3ven Security dan meminta tebusan berupa 0.04 Bitcoin. Upaya penebusan tidak dilakukan karena biaya terlalu mahal dan tidak ada jaminan bahwa akan diberikan kunci akses untuk membuka dekripsi, selain itu upaya dekripsi oleh pihak internal gagal dilakukan karena tidak tersedianya *decryption tool* yang sesuai untuk varian ransomware ini, sehingga seluruh data hilang permanen.

Kerugian semakin besar karena proses *restore* dari cadangan data (*backup*) juga mengalami kegagalan. Akibatnya, NAS terpaksa di-*install* ulang, dan organisasi mengubah kebijakan penyimpanan data penting dengan memindahkannya ke Google Drive yang hanya dapat diakses melalui akun resmi organisasi. Insiden ini menunjukkan lemahnya kontrol keamanan pada infrastruktur penyimpanan dan kurangnya mekanisme mitigasi risiko yang efektif, sehingga memperkuat urgensi penelitian ini untuk mengevaluasi dan memperbaiki tata kelola keamanan informasi berdasarkan kerangka kerja COBIT 2019.

Serangan ini terjadi akibat kurangnya pemahaman Sumber Daya Manusia (SDM) terhadap keamanan informasi, yang tercermin dalam kebiasaan membuka tautan *phishing*, menggunakan perangkat lunak ilegal, dan mengunduh berkas dari sumber yang tidak terpercaya. Situasi ini menunjukkan betapa pentingnya meningkatkan kesadaran dalam penerapan praktik keamanan siber terutama pada pentingnya menjaga data dan privasi di era digital (Manurung et al., 2023). LAZIS Sabilillah Malang dapat memperkuat tata kelola keamanannya dengan ketiga sub-domain ini karena kerangka kerja COBIT 2019 terdiri dari seperangkat *control objectives* pada bidang TI sehingga dapat memudahkan auditor dalam mengaudit secara terstruktur (Sepis, 2022).

Secara teoritis, *framework* COBIT 2019, khususnya sub-domain APO12, APO13 dan DSS05, telah terbukti efektif dalam meningkatkan keamanan sistem informasi melalui berbagai penelitian sebelumnya. Namun, masih terdapat

research gap terkait penerapannya pada sektor filantropi, yang memiliki karakteristik dan tantangan unik dibanding sektor profit maupun institusi pemerintahan. Kasus serangan *ransomware* pada LAZIS Sabilillah Malang menunjukkan bahwa tantangan utama dalam keamanan sistem informasi bukan hanya terletak pada teknologi, tetapi juga pada aspek SDM dan kebijakan tata kelola yang belum terkolala secara maksimal. Dengan menghubungkan *research gap* ini, penelitian ini berfokus untuk menjembatani kebutuhan spesifik LAZIS Sabilillah terhadap solusi keamanan yang lebih menyeluruh, berbasis best practices COBIT 2019.

Penelitian ini berguna untuk meningkatkan keamanan sistem informasi khususnya dalam melindungi laporan keuangan dan data pribadi donatur dengan mengevaluasi dan menerapkan APO12 (*Managed Risk*), APO13 (*Managed Security*), dan DSS05 (*Managed Security Services*) pada COBIT 2019. Melalui identifikasi kebutuhan keamanan organisasi, pemetaan proses keamanan yang ada, dan penerapan *best practices* yang diusulkan oleh COBIT 2019 (Yonal Supit & Edy Irwansyah, 2024). Berdasarkan sebagaimana uraian yang sudah dijelaskan, melalui penelitian ini diharapkan tercipta kontribusi positif dalam mendukung penguatan keamanan informasi di LAZIS Sabilillah Malang.

1.2 Rumusan Masalah

Bagaimana sub-domain APO12, APO13 dan DSS05 pada COBIT 2019 dapat diimplementasikan di LAZIS Sabilillah Malang sebagai upaya untuk meningkatkan keamanan sistem informasi ?

1.3 Tujuan

1. Menilai kondisi aktual keamanan sistem informasi di LAZIS Sabilillah Malang melalui pendekatan evaluasi *capability level* dan analisis kesenjangan berdasarkan sub-domain COBIT 2019, dengan mengacu pada hasil kuesioner dan wawancara dari pihak internal yang terlibat dalam pengelolaan TI.
2. Mengidentifikasi sub-domain COBIT 2019 yang paling relevan dan memungkinkan untuk diterapkan sesuai dengan konteks kebutuhan,

risiko, dan sumber daya organisasi, dengan mempertimbangkan urgensi serta faktor-faktor desain (*design factors*) seperti profil risiko, tujuan strategis, dan lanskap ancaman.

3. Merancang dokumen Standar Operasional Prosedur (SOP) untuk setiap proses utama pada sub-domain terpilih (APO12, APO13, dan DSS05), sebagai upaya sistematis dalam meningkatkan tata kelola keamanan informasi dan mendorong keselarasan antara TI dan tujuan strategis organisasi.

1.4 Manfaat

1.4.1 Bagi LAZIS Sabilillah Malang

1. Peningkatan Keamanan Sistem Informasi:

   Penelitian ini akan membantu LAZIS Sabilillah Malang mengidentifikasi kelemahan dalam sistem keamanan informasi yang ada dan memberikan rekomendasi perbaikan yang spesifik berdasarkan standar COBIT 2019.

2. Mencegah Kehilangan Data:

   Dengan menerapkan rekomendasi yang dihasilkan dari penelitian, LAZIS dapat mengurangi risiko terjadinya kebocoran data atau serangan siber yang dapat menyebabkan kerugian finansial dan reputasi.

3. Kepatuhan terhadap Regulasi:

   Penelitian ini dapat membantu LAZIS memenuhi regulasi dan standar keamanan informasi yang berlaku, sehingga menghindari risiko sanksi hukum

1.4.2 Bagi Peneliti

1. Peningkatan Keterampilan:

   Peneliti akan memperoleh pengalaman dalam merancang desain penelitian, melakukan pengumpulan data, menganalisis hasil temuan, serta menyusun laporan akhir penelitian.

2. Pengembangan Karir:

   Hasil penelitian bisa dipublikasikan dalam jurnal ilmiah atau konferensi, yang akan meningkatkan reputasi peneliti dan membuka peluang untuk studi lanjutan atau bekerja di bidang terkait.

Agar fokus penelitian ini tetap terarah dan tidak melebar, maka ditetapkan batasan masalah yang dijelaskan sebagai berikut.

1.5 Batasan Masalah

1. Penelitian ini dilakukan dengan menggunakan 3 sub-domain kerangka kerja COBIT 2019 yaitu sub-domain APO12 (*managed risk*) dengan tujuan untuk mengidentifikasi, mengevaluasi, serta mengelola berbagai risiko yang berpotensi menghambat pencapaian tujuan bisnis organisasi. Sub-domain selanjutnya adalah APO13 (*Manage Security*) bertujuan untuk memastikan bahwa dampak dari insiden keamanan informasi tetap berada dalam batas yang dapat dikendalikan dan ditangani oleh organisasi. Selain itu, penggunaan sub-domain DSS05 (*Manage Security Services*) juga penting dengan tujuan untuk menjaga keamanan informasi perusahaan dengan mengatur peran dan hak akses sistem informasi organisasi.
2. Penelitian ini akan dilakukan dengan studi kasus LAZIS Sabilillah Malang pada divisi IT Media

Dengan memahami batas ruang lingkup penelitian, maka struktur penyusunan laporan ini dijelaskan melalui sistematikan penulisan berikut.

1.6 Metodologi Penelitian

1.6.1. Tempat dan Waktu Penelitian

Tempat : Kantor Pusat LAZIS Sabilillah Malang, Jl. Ikan Piranha Atas 161A Tunjungsekar, Lowokwaru, Kota Malang, Jawa Timur.

Waktu : 6 Bulan (Februari 2025 – Juli 2025)

Tabel 1.1 Jadwal Penelitian

No.	Kegiatan	Periode Bulan Ke-					
		1	2	3	4	5	6
1	Kajian literatur						
2	Pengumpulan data						
3	Pengumpulan dokumen-dokumen						
4	Penilaian *Capability Level, Maturity Level,* & Analisis Kesenjangan (*Gap*)						
5	Evaluasi						
6	Rekomendasi						

1.6.2. Bahan dan Alat Penelitian

1. *Hardware*: Laptop
2. *Software*:
   a) Microsoft Word
   b) Microsoft Excel
   c) Mendeley Reference Manager
   d) *Browser* Microsoft Edge

1.6.3. Metode Penelitian

Penelitian ini menggunakan pendekatan metode penelitian kuantitatif dan melakukan studi kasus mendalam dengan pihak manajemen LAZIS Sabilillah Malang. Menurut (Assyakurrohim et al., 2022), penelitian kuantitatif adalah jenis penelitian sistematis yang melihat peristiwa, mengumpulkan data, dan kemudian menganalisis data tersebut. Penelitian kuantitatif dibagi menjadi tiga tahap: kajian literatur, observasi, wawancara, dan kuesioner. Prosedur penelitian ini nanti akan menghasilkan data yang berupa angka dan kata-kata yang bersifat subyektif. Maka dari itu perlu evaluasi dengan verifikasi hasil yang didapat dengan kenyataan melalui diskusi dengan pihak manajemen LAZIS Sabilillah dan konsultasi dengan auditor yang tersertifikasi COBIT 2019.

1.6.4. Pengumpulan Data dan Informasi

Metode atau instrumen yang digunakan untuk mengumpulkan informasi yang sesuai dengan penelitian atau studi dikenal sebagai instrumen pengumpulan data (Ardiansyah et al., 2023). Instrumen ini sangat penting untuk mendapatkan data yang akurat dan dapat diandalkan untuk menjawab pertanyaan penelitian. Pengumpulan data pada metode penelitian kuantitatif deskriptif menurut (Creswell & Creswell, 2018) antara lain:

1. Studi Literatur

   Studi literatur merupakan metode pengumpulan data yang dilakukan melalui membaca, mencatat dan mengelola bahan penelitian. Hal ini dapat dilakukan setelah menentukan topik tertentu yang akan dibahas dalam penelitian sebelum melakukan pengambilan data. Informasi pada studi literatur bisa didapatkan melalui buku, jurnal, maupun artikel selama masih berkaitan dengan konsep yang diteliti. Studi literatur juga dapat diartikan sebagai usaha dalam mengidentifikasi dan memahami semua hasil penelitian yang relevan (Fajar & Aviani, 2022).

2. Observasi

   Metode Observasi adalah aktifitas pengamatan terhadap *IT process* operasional LAZIS Sabilillah dan kesadaran dan perilaku pegawai terhadap keamanan informasi sebelum implementasi COBIT 2019 yaitu pada sub-domain APO12 (*Managed Risk*), APO13 (*Managed Security*), dan DSS05 (*Managed Security Services*).

3. Kuesioner

   Kuesioner atau angket merupakan suatu mekanisme yang kerap digunakan dalam pengumpulan data melalui serangkaian pertanyaan yang telah dirancang dan disusun berdasarkan kriteria yang telah ditentukan sebelumnya (Ardiansyah et al., 2023). Menurut Ulfah et al., 2024, salah satu skala yang lazim digunakan dalam pengumpulan data melalui kuesioner adalah skala Likert, yaitu skala yang digunakan untuk mengukur sikap, persepsi, pendapat, maupun perilaku individu terhadap suatu pernyataan atau fenomena tertentu. Skala Likert

umumnya disusun dalam bentuk pernyataan atau pertanyaan yang diikuti oleh pilihan jawaban berupa: Sangat Setuju (SS), Setuju (S), Netral (N), Tidak Setuju (TS), dan Sangat Tidak Setuju (STS). Responden diminta untuk memberikan tanggapan yang paling sesuai dengan situasi atau kondisi yang mereka alami.

4. Wawancara

Metode wawancara adalah kegiatan dimana peneliti melakukan tanya-jawab secara lisan kepada narasumber. Setelah melakukan pengisian kuesioner, peneliti akan melakukan wawancara kepada manajer operasional dengan fungsi pengembangan strategi operasi organisasi sesuai dengan tujuan jangka panjang dan evaluasi alur kerja operasional yang efisien. Kepada konsultan IT dengan fungsi diagnosis dan analisis masalah potensial, mengembangkan rencana aksi baik dari sisi waktu maupun sumber daya yang dibutuhkan. Terakhir, wawancara akan dilakukan kepada manajer divisi IT selaku penanggung jawab dalam pengelolaan dan koordinasi semua aspek teknologi informasi pada organisasi. Pemilihan narasumber wawancara ini sudah sesuai dengan struktur LAZIS Sabilillah yang akan dijabarkan melalui gambar 2.2.

1.6.5. Analisis Data

Tahapan analisis data merupakan proses menyusun dan mengolah hasil observasi, wawancara, serta teknik pengumpulan data lainnya secara sistematis, dengan tujuan untuk membantu peneliti memahami objek yang diteliti dan menyajikannya sebagai temuan yang dapat dipahami oleh pihak lain. (Syaeful Millah et al., 2023). Adapun metode analisis data yang diterapkan dalam penelitian ini meliputi hal-hal berikut:

1. *Capability Level Analysis*

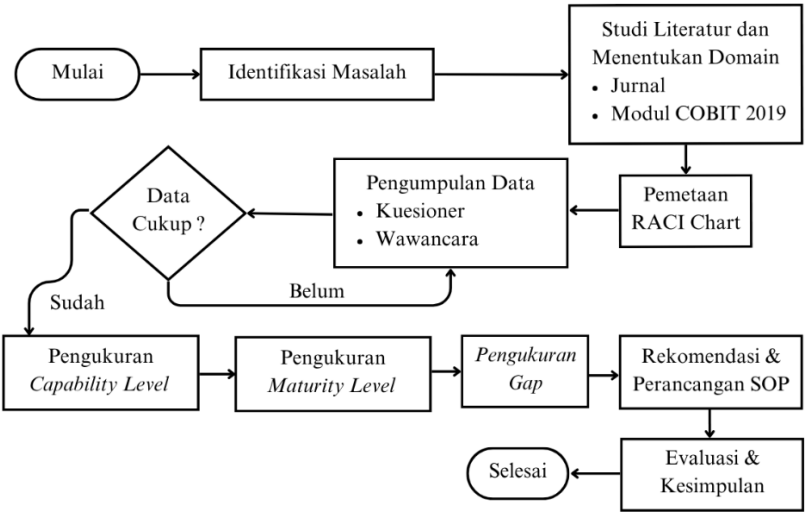
Analisis tingkat kapabilitas merupakan suatu teknik dalam proses pengukuran sejauh mana atribut proses telah tercapai (Putri et al., 2022).

2. Gap Analysis

Teknik analisis kesenjangan adalah pendekatan yang paling tepat untuk menilai kondisi *gap* pada sebuah organisasi saat ini sehingga memungkinkan penerapan perbaikan berdasarkan kesenjangan tersebut (Yulianto, 2024)

1.6.6. Prosedur Penelitian

Rancangan prosedur penelitian yang akan dilakukan dijabarkan melalui diagram alur berikut ini:



Gambar 1.1 Diagram Alur Penelitian

Penelitian ini dilakukan dalam rangka mengukur dan mengevaluasi tata kelola keamanan informasi LAZIS Sabilillah Malang dengan menggunakan *framework* COBIT 2019. Penelitian ini menggunakan pendekatan pengumpulan data melalui studi literatur, observasi, kuesioner, dan wawancara yang akan menjadi dasar dalam identifikasi masalah dan menentukan rumusan masalah yang akan dibahas dalam penelitian ini. Tahapan selanjutnya adalah wawancara kepada manajer operasional, konsultan IT, dan kepala divisi IT LAZIS Sabilillah Malang. Hasil wawancara tersebut merupakan dasar dalam melakukan analisis

perhitungan untuk menentukan capaian *Capability Level* dan analisis kesenjangan (*Gap*). Pada wawancara tersebut juga akan disepakati target capaian Capability Level untuk menentukan gap dan sebagai acuan dalam merumuskan beberapa standar operasional dengan tujuan memberikan rekomendasi kebijakan dalam mengoptimalkan keamanan informasi di LAZIS Sabilillah Malang berdasarkan sub-domain COBIT 2019 yaitu APO12, APO13 dan DSS05. Hasil temuan capaian *Capability Level* dan standar operasional tersebut akan dilakukan evaluasi dengan auditor tersertifikasi COBIT 2019 sehingga hasil yang didapat bisa dijadikan acuan dalam keamanan informasi di LAZIS Sabilillah Malang.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini memaparkan latar belakang permasalahan, perumusan masalah, tujuan dan manfaat penelitian, batasan ruang lingkup, serta sistematika penulisan yang menjadi landasan dalam penyusunan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Bagian ini memuat hasil penelitian terdahulu yang sejalan, berbagai teori yang mendasari penelitian, seperti konsep dasar TKTI, audit TI, COBIT 2019, juga pembahasan tentang sub-domain APO12, APO13, dan DSS05. Pada bab ini juga dijelaskan Gambaran terkait obyek penelitian dan kerangka berpikir sebagai acuan penelitian.

BAB III PEMETAAN DAN ANALISIS

Bagian ini berisi pemetaan sub-domain apa saja yang akan digunakan melalui *Process Assessment Model* (PAM), penentuan penggunaan *design factors*, lalu analisis kondisi saat ini serta kondisi yang diharapkan, analisis tingkat kemampuan dan kematangan serta analisis kesenjangan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan hasil pengolahan dan analisis data berdasarkan hasil kuesioner dan wawancara, termasuk

penilaian *capability level*, *gap analysis*, dan identifikasi sub-domain yang *urgent* dan *possible*. Selain itu, dibahas pula hasil analisis *design factor* dan penyusunan dokumen Standar Operasional Prosedur (SOP) pada setiap proses yang dinilai prioritas dalam penguatan keamanan sistem informasi.

BAB V PENUTUP

Menyajikan kesimpulan dari keseluruhan hasil penelitian yang telah dilakukan, serta saran untuk implementasi lebih lanjut dalam meningkatkan keamanan sistem informasi di LAZIS Sabilillah Malang.