BAB III
PEMETAAN DAN ANALISIS

3.1 Pemetaan

3.1.1 Pemetaan *Process Assessment Model*

Tujuan Teknologi Informasi (TI) perusahaan harus sejalan dengan tujuan keseluruhan perusahaan. Dengan demikian, pengembangan tujuan TI perlu diselaraskan dengan visi dan misi perusahaan. Selain itu, pengelolaan TI juga harus dilakukan secara efektif dan efisien, dengan memperhatikan keseimbangan antara pencapaian manfaat, pengoptimalan risiko, dan pemanfaatan sumber daya. Dalam penelitian ini, penulis mengacu pada kerangka kerja COBIT 2019 sebagai panduan. Sebagai langkah awal, penulis melakukan observasi untuk memahami tujuan bisnis, tujuan TI, serta proses TI di LAZIS Sabilillah Malang. Hasil observasi ini berimplikasi pada kriteria definisi domain yang dipilih dalam penelitian ini. Terdapat tiga sub-domain yang berkaitan dengan keamanan informasi, yaitu APO12, APO13, dan DSS05.

Pemilihan sub-domain APO12 (*Managed Risk*), APO13 (*Managed Security*), dan DSS05 (*Managed Security Services*) dalam penelitian ini didasarkan pada hasil observasi awal serta wawancara dengan pihak manajemen LAZIS Sabilillah Malang. Ketiga sub-domain ini dipilih karena memenuhi kriteria berikut:

1. Relevansi Langsung dengan Insiden Keamanan yang Terjadi
   Serangan ransomware pada Juni 2022 yang memanfaatkan kerentanan pada *Network Attached Storage* (NAS) menunjukkan bahwa kelemahan utama organisasi terletak pada aspek pengelolaan risiko TI, pengendalian keamanan informasi, dan penyediaan layanan keamanan. APO12, APO13, dan DSS05 secara langsung memuat proses yang berhubungan dengan deteksi, pencegahan, dan penanggulangan ancaman serupa.

2. Fokus pada Penguatan Teknis *Security Posture*

APO12 memberikan kerangka kerja sistematis untuk mengidentifikasi, menganalisis, dan memitigasi risiko yang dapat menghambat pencapaian tujuan organisasi. APO13 memastikan penerapan kebijakan dan kontrol keamanan yang terintegrasi, sedangkan DSS05 mengatur penyediaan layanan keamanan, termasuk perlindungan terhadap *malware*, pengelolaan identitas pengguna, dan kontrol *physical* maupun *logical access*. Kombinasi ketiga sub-domain ini mencakup siklus penuh dari pengelolaan risiko hingga implementasi kontrol operasional.

3. Kesesuaian dengan Prioritas Strategis Organisasi

Berdasarkan wawancara dengan pihak manajemendan konsultan IT, prioritas LAZIS Sabilillah adalah memastikan kerahasiaan data donatur, integritas laporan keuangan, dan ketersediaan layanan digital sebagaimana penerapan prinsip utama CIA Triad. Ketiga sub-domain terpilih selaras dengan tujuan tersebut, karena berfokus pada perlindungan data, pencegahan serangan, dan keberlanjutan layanan TI.

4. Dukungan terhadap Kepatuhan Regulasi

Implementasi APO12, APO13, dan DSS05 membantu organisasi mematuhi ketentuan dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Permen PAN RB No. 47 Tahun 2018 tentang Pengamanan Sistem Informasi Instansi Pemerintah, yang mengharuskan adanya pengelolaan risiko dan kontrol keamanan yang terukur sebagaimana telah dibahas pada latar belakang penelitian ini.

5. Pertimbangan Efisiensi Penelitian

Meskipun domain APO07 (*Managed Human Resources*) relevan dengan aspek perilaku SDM, domain ini tidak dijadikan prioritas karena fokus penelitian diarahkan pada perbaikan kontrol teknis. Namun, elemen penguatan SDM tetap diintegrasikan ke dalam rekomendasi pada domain APO13 dan DSS05, sehingga faktor

manusia tetap terakomodasi tanpa memperluas lingkup analisis capability level.

Dengan pertimbangan tersebut, pemilihan APO12, APO13, dan DSS05 dinilai paling tepat untuk menjawab kebutuhan penelitian sekaligus menghasilkan rekomendasi *Standard Operating Procedure* (SOP) yang dapat diimplementasikan secara praktis oleh LAZIS Sabilillah Malang.

3.1.1.1 APO12 *Managed Risk*

Fokus utama dari sub-domain ini adalah mengidentifikasi, menilai, dan mengendalikan risiko-risiko yang berhubungan dengan TI dalam rangka memastikan pengelolaan sistem informasi organisasi berjalan secara aman dan efektif. Sehingga pada bagian ini dikelompokkan ke dalam 6 proses. Proses-proses yang termasuk dalam sub-domain ini adalah:

1. APO12.01 Menghimpun data
2. APO12.02 Menelaah risiko
3. APO12.03 Memelihara *risk profile*
4. APO12.04 Menjelaskan risiko
5. APO12.05 Menentukan dokumentasi tindakan *risk management*
6. APO12.06 Merespon risiko

3.1.1.2 APO13 *Managed Security*

Dalam sub-domain ini mendefinisikan, mengoperasikan dan memantau sistem informasi yang ada dalam rangka manajemen keamanan informasi. Sehingga pada bagian ini dikelompokkan ke dalam 3 proses yaitu:

1. APO13.01 Menyusun dan menjaga Sistem Manajemen Keamanan Informasi (SMKI) mencakup kebijakan, tolak ukur, serta pedoman guna memastikan keamanan informasi dikelola secara terstruktur dan berkelanjutan.
2. APO13.02 Merancang serta menjalankan rencana mitigasi risiko keamanan informasi yang selaras dengan profil risiko dan strategi

organisasi, guna meminimalkan dampak ancaman terhadap aset informasi.

3. APO13.03 Melaksanakan pemantauan dan evaluasi terhadap kerangka pengawasan terintegrasi (Integrated Model for Supervision/IMS) untuk memastikan efektivitas pengendalian keamanan informasi serta kepatuhan terhadap kebijakan yang telah ditetapkan.

3.1.1.3 DSS05 *Managed Security Services*

Dalam sub-domain ini menjaga tingkat risiko keamanan informasi yang terdapat pada sistem informasi mereka sesuai dengan kebijakan keamanan yang telah ditentukan. Sehingga pada bagian ini dikelompokkan ke dalam 7 proses:

1. DSS0S.01 Perlindungan terhadap ancaman *malicious software*
2. DSS05.02 Pengelolaan keamanan jaringan dan konektivitas
3. DSS05.03 pengelolaan keamanan titik akhir
4. DSS05.04 Pengelolaan identifikasi pengguna dan logical access
5. DSS05.05 Pengelolaan akses fisik ke *IT assets*
6. DSS05.06 Pengelolaan berkas penting (terbatas) dan perangkat luaran
7. DSS05.07 Pemantauan prasarana untuk kejadian terkait keamanan

3.1.1.4 Pertimbangan Domain APO07 (*Managed Human Resources*)

Dalam tahap observasi awal, ditemukan bahwa salah satu akar permasalahan insiden keamanan informasi di LAZIS Sabilillah Malang adalah perilaku SDM yang kurang tepat, seperti membuka tautan tidak terpercaya, menginstal perangkat lunak ilegal, dan mengunduh file dari sumber yang tidak terpercaya. Perilaku ini sebagian besar dilakukan oleh pegawai non-divisi TI yang tetap menjadi pengguna aktif sistem informasi organisasi.

Secara prinsip, perilaku tersebut memiliki relevansi dengan domain APO07 (*Managed Human Resources*) dalam COBIT 2019, yang mengatur perencanaan, pengelolaan, dan pengembangan seluruh SDM yang terlibat dalam tata kelola dan layanan TI, termasuk pengguna non-teknis. APO07

mencakup aspek penetapan peran, pelatihan, dan peningkatan kesadaran keamanan informasi (*security awareness*) untuk memastikan semua pihak memahami tanggung jawab mereka dalam menjaga keamanan sistem. Meskipun demikian, penelitian ini memutuskan untuk tidak menjadikan APO07 sebagai domain prioritas dengan pertimbangan:

1. Fokus Penelitian pada Pengendalian Teknis dan Manajemen Risiko

   Tujuan utama penelitian adalah memperkuat tata kelola keamanan informasi melalui pengelolaan risiko (APO12), pengendalian keamanan (APO13), dan layanan keamanan (DSS05), yang secara langsung berhubungan dengan pencegahan dan mitigasi insiden teknis seperti serangan *ransomware*.

2. Integrasi Aspek SDM ke dalam Domain Keamanan

   Faktor perilaku SDM tetap diakomodasi melalui kontrol dan prosedur pada domain APO13 dan DSS05. Misalnya, kebijakan penggunaan perangkat, pembatasan hak akses, dan pelatihan keamanan siber dimasukkan sebagai bagian dari SOP di kedua domain tersebut. Dengan cara ini, aspek manajemen SDM yang relevan tetap diperhatikan tanpa melakukan analisis capability level APO07 secara penuh.

Dengan pendekatan ini, penelitian tetap fokus pada domain yang memiliki dampak langsung terhadap peningkatan postur keamanan teknis organisasi, sambil memastikan faktor manusia yang menjadi salah satu penyebab insiden tetap tertangani melalui kontrol pendukung di dalam implementasi domain prioritas.

3.1.2 Penyesuaian Kerangka COBIT 2019 dengan *Design Factor*

Dalam kerangka kerja COBIT 2019, terdapat 11 *Design Factor* yang berperan sebagai pedoman dalam merancang solusi tata kelola dan manajemen Teknologi Informasi (TI) yang disesuaikan dengan karakteristik masing-masing organisasi. Faktor-faktor ini membantu dalam menyesuaikan pemilihan serta penerapan *Governance and Management Objectives*, dengan mempertimbangkan konteks, kebutuhan, dan prioritas strategis organisasi. Namun, dalam penelitian ini hanya digunakan 7 dari 11 *Design Factors*, yaitu:

1. Strategi Perusahaan
2. Tujuan Perusahaan

3. Profil Risiko
4. Isu Terkait TI
5. Lanskap Ancaman
6. Persyaratan Kepatuhan
7. Peran TI

Pembatasan ini diambil berdasarkan pertimbangan metodologis dan kontekstual, dengan beberapa alasan berikut:

Pertama, dari sisi relevansi terhadap kondisi organisasi. LAZIS Sabilillah Malang merupakan organisasi nirlaba yang memiliki struktur dan kompleksitas manajemen TI yang relatif tidak terlalu rumit. Oleh karena itu, beberapa *Design Factor* lain seperti *Technology Adoption Strategy, Industry Sector*, dan *Role of IT* dinilai terlalu umum atau tidak memberikan dampak signifikan terhadap proses penilaian dan perancangan tata kelola keamanan informasi dalam konteks organisasi ini.

Kedua, penyesuaian terhadap fokus kajian penelitian. Sebagaimana tujuan utama dari studi ini ialah untuk menganalisis serta mengimplementasikan sub-domain APO12, APO13, dan DSS05. Ketiga sub-domain tersebut memiliki fokus utama pada pengelolaan risiko dan keamanan sistem informasi. Oleh sebab itu, hanya *Design Factor* yang secara langsung berkaitan dengan isu risiko, ancaman, layanan TI, serta arah strategi organisasi yang digunakan sebagai acuan.

Ketiga, untuk menjaga efisiensi ruang lingkup penelitian. Mengikutsertakan semua 11 *Design Factors* akan memperluas cakupan analisis dan menambah kompleksitas yang tidak diperlukan. Dengan membatasi pada 7 faktor yang dianggap paling relevan, penelitian ini dapat tetap fokus dan efisien, serta menghasilkan rekomendasi yang lebih konkret, aplikatif, dan sesuai dengan kondisi aktual di lapangan.

Keempat, panduan resmi dari ISACA juga menyatakan bahwa penggunaan Design Factor bersifat fleksibel dan disesuaikan dengan kebutuhan masing-masing organisasi (Rafeq, 2019). Dalam situs resminya, dijelaskan bahwa:

"Further, it is not necessary to use all the design factors, only what is required by the particular enterprise. The design factors are not prescriptive but are generally applicable"

Dengan demikian, pemilihan 7 Design Factors dalam penelitian ini merupakan pendekatan yang sesuai dengan prinsip-prinsip COBIT 2019, serta mempertimbangkan kebutuhan organisasi secara praktis dan akademis. Pendekatan ini diharapkan dapat menghasilkan analisis yang lebih tepat sasaran dan mendukung penguatan sistem keamanan informasi di LAZIS Sabilillah Malang secara efektif.

3.2 Analisis

Dalam tata kelola Teknologi Informasi (TI), terdapat tiga jenis asesmen yang umum dilakukan, yaitu asesmen capability level, maturity level, dan gap analysis. Asesmen capability level bertujuan untuk mengevaluasi sejauh mana setiap proses dalam domain objektif tertentu telah dilaksanakan, sementara asesmen maturity level menilai tingkat kematangan dari area fokus atau domain objektif secara keseluruhan., dan asesmen pada *gap analysis* adalah metode mengidentifikasi kesenjangan (*gap*) antara kondisi saat ini (*as-is*) dari sistem TKTI organisasi dengan kondisi yang diinginkan (to-be) (Herianto & Wasilah, 2022).

3.2.1 Penilaian Kondisi Saat Ini dan Kondisi yang Diharapkan

Analisis tingkat kematangan tata kelola keamanan sistem informasi pada LAZIS Sabilillah Malang dilakukan untuk mengetahui sejauh mana tingkat kapabilitas (*capability level*) masing-masing proses dalam domain COBIT 2019 yang menjadi fokus penelitian, yaitu APO12, APO13, dan DSS05. Penilaian dilakukan berdasarkan hasil data yang diperoleh melalui kuesioner skala Likert dan wawancara mendalam kepada empat narasumber utama yang berperan dalam pengelolaan sistem informasi, yaitu Konsultan IT, Manajer Divisi IT Media, Staf IT, dan Manajer Operasional.

Analisis dilakukan terhadap setiap sub-proses dalam domain APO12, APO13, dan DSS05 dengan tujuan untuk mengetahui *capability*

level yang saat ini dicapai (*as-is*) oleh organisasi. Setiap sub-proses dinilai berdasarkan pemenuhan atribut proses sesuai dengan skala tingkat kapabilitas COBIT 2019, mulai dari Level 0 (*Incomplete*) hingga Level 5 (*Optimizing*). Hasil penilaian kondisi saat ini kemudian dirata-rata untuk memperoleh nilai keseluruhan tingkat kapabilitas dari masing-masing sub-domain.

Selain melakukan analisis terhadap kondisi saat ini, peneliti juga melakukan penilaian terhadap kondisi yang diharapkan (*to-be*) oleh organisasi. Harapan ini didasarkan pada wawasan dari Konsultan IT dan hasil interpretasi dari kebutuhan organisasi terhadap penguatan pengelolaan keamanan informasi. Penilaian kondisi yang diharapkan bertujuan sebagai acuan strategis dalam mengembangkan tata kelola TI di masa mendatang.

Kondisi yang diharapkan mencerminkan tingkat kapabilitas yang ideal bagi LAZIS Sabilillah Malang agar dapat mencapai pengelolaan keamanan informasi yang memadai, terstruktur, dan sesuai standar. Dalam hal ini, sebagian besar proses ditargetkan untuk mencapai Level 3 hingga Level 4, yang mencerminkan bahwa proses sudah terdokumentasi dengan lengkap, dilakukan secara konsisten, serta dimonitor secara berkala.

Perbandingan antara *as-is* dan *to-be* menghasilkan analisis kesenjangan (*gap analysis*) yang menjadi dasar dalam penyusunan rekomendasi implementasi dan dokumen SOP. Analisis kesenjangan ini juga digunakan untuk mengidentifikasi proses-proses yang bersifat urgent dan possible untuk segera ditingkatkan berdasarkan kondisi nyata organisasi, yang telah dipetakan berdasarkan masukan dari Konsultan IT.

3.2.2 Analisis Tingkat Kemampuan

Analisis Tingkat Kemampuan atau biasa disebut *Capability Level Analysis* dalam COBIT 2019 adalah penilaian tentang seberapa optimal suatu proses dilakukan dan dijalankan, berdasarkan skema *Capability Maturity Model Integration* (CMMI) yang berkisar dari tingkat 0 hingga 5 sebagaimana yang sudah dijelaskan pada Tabel 2.2. Setiap level mewakili

tingkat kemampuan proses yang berbeda. Tingkat kematangan (maturity level) dimulai dari level 1 yang menunjukkan bahwa proses masih dijalankan secara ad-hoc atau tidak terstruktur. Pada level 2, proses sudah dapat diulang dan dijalankan secara konsisten meskipun belum sepenuhnya terdokumentasi. Level 3 menggambarkan bahwa proses telah distandarisasi dan diterapkan secara menyeluruh di seluruh organisasi, menandakan pendekatan yang lebih proaktif. Selanjutnya, level 4 menunjukkan bahwa proses telah dikelola dan dipantau secara kuantitatif berdasarkan data dan indikator kinerja. Sedangkan pada level 5, proses telah dioptimalkan dan mengalami perbaikan secara berkelanjutan guna mencapai efisiensi dan efektivitas yang lebih tinggi.

Tabel 3. 1 *Capability Level*

Capability Level	**Status**
Lv. 0	Tidak lengkap (*Incomplete*)
Lv. 1	Dilakukan (*Performed*)
Lv. 2	Dikelola (*Managed*)
Lv. 3	Mapan (*Established*)
Lv. 4	Dapat diprediksi (*Predictable*)
Lv. 5	Mengoptimalkan (*Optimizing*)

Analisis ini membantu organisasi memahami kemampuan proses mereka saat ini, mengidentifikasi apa saja yang perlu untuk dioptimalkan, dan menyelaraskan proses mereka dengan tujuan strategis untuk meningkatkan kinerja dan efisiensi (ISACA, 2019b). Proses analisis kesenjangan dilakukan dengan menghitung prosentase keberhasilan dengan menggunakan persamaan 3.1 berikut:

$$\text{Rumus Capability Level } (CLi) = \frac{R1+R2}{\Sigma R} X\ 100\%$$

Persamaan 3.1

Keterangan:

CLi = Nilai tingkat kapabilitas

R1 = Nilai tingkat kapabilitas dari Responden 1

R2 = Nilai tingkat kapabilitas dari Responden 2

ΣR = Total jumlah Responden

3.2.3 Analisis Tingkat Kematangan

Analisis *maturity level* digunakan untuk mengevaluasi seberapa matang domain tata kelola TI secara keseluruhan. COBIT 2019 mendefinisikan maturity level dalam rentang 0–5 yang menggambarkan tingkat kematangan proses dalam suatu organisasi. Maturity level memberikan gambaran lebih luas daripada capability level karena menilai bukan hanya implementasi proses, melainkan budaya, integrasi antar proses, keberlanjutan, dan pengukuran kinerja jangka panjang. Adapun penjelasan level-level *maturity* dijelaskan dalam bentuk tabel berikut:

Tabel 3. 2 Tingkat Kematangan

Tingkat Kematangan	Penjelasan
Level 0 (*Incomplete*)	Proses tidak ada atau tidak dapat diidentifikasi.
Level 1 (*Initial*)	Proses dilakukan tidak konsisten, sangat bergantung pada individu.
Level 2 (*Managed*)	Proses sudah dijalankan, namun belum terdokumentasi secara formal.
Level 3 (*Defined*)	Proses telah ditetapkan secara formal dan standar diberlakukan di seluruh organisasi.
Level 4 (*Quantitatively Managed*)	Proses dikelola secara kuantitatif dan terukur.
Level 5 (*Optimizing*)	Proses terus-menerus diperbaiki berdasarkan data kinerja.

Penilaian *maturity level* pada penelitian ini yaitu dengan menggabungkan jawaban responden dalam kuesioner dan penjelasan responden pada tahap wawancara untuk memahami tingkat integrasi, perencanaan strategis, dan pengawasan proses dalam domain APO12, APO13, dan DSS05. Hasil penilaian akan digunakan sebagai dasar dalam merancang perencanaan perbaikan dan pengembangan sistem tata kelola keamanan informasi di masa mendatang.

3.2.4 Analisis Kesenjangan

Analisis kesenjangan (*Gap Analysis*) merupakan alat strategis yang digunakan untuk mengidentifikasi perbedaan antara kondisi proses, kapabilitas, atau kinerja organisasi saat ini dengan kondisi ideal atau yang ditargetkan di masa mendatang. Tujuan utamanya adalah untuk mengatasi kesenjangan ini guna mencapai hasil yang diinginkan (ISACA, 2019b).

Tabel 3. 3 Contoh Gap

Objective	***Process***	***Capability Level***	***Expected Level***
APO12	*Managed Risk*	1	4
APO13	*Managed Security*	2	4
DSS05	*Managed Security Services*	3	4

Pengukuran analisis kesenjangan dapat dilakukan dengan mengurangkan tingkat kapabilitas yang diinginkan (target kapabilitas) dengan capaian kapabilitas saat ini (Hidayah et al., 2024). Sebagaimana dalam persamaan 3.2 berikut ini:

Gap = Nilai yang diharapkan (*to-be*) – Nilai yang diperoleh (*as-is*)

Persamaan 3.2