BAB I
PENDAHULUAN

1.1 Latar Belakang

Integrasi teknologi informasi dan komunikasi telah berevolusi menjadi faktor penentu keberhasilan strategis perusahaan di berbagai sektor. Awalnya, pemanfaatan teknologi hanya terbatas pada kebutuhan administrasi. Namun, seiring dengan perkembangan ilmu pengetahuan dan teknologi, perannya meluas secara signifikan, tidak hanya mendukung operasional, tetapi juga mencakup fungsi pengambilan keputusan, pengelolaan data, serta peningkatan efisiensi yang vital bagi kelangsungan perusahaan. Untuk mewujudkan peran krusial ini, diperlukan dukungan infrastruktur dan layanan TI yang andal dan terintegrasi. Komponen ini mencakup perangkat keras, perangkat lunak, basis data, aplikasi, sistem komunikasi, dan secara khusus jaringan. Jaringan memiliki fungsi sebagai media komunikasi sentral antar sistem, unit kerja, dan pelanggan[1]. Dengan demikian, kerentanan atau gangguan pada jaringan berisiko melumpuhkan operasional, menurunkan kualitas layanan, dan secara signifikan mengikis kepercayaan pelanggan[2].

Risiko ini berpotensi mengancam organisasi di sektor bisnis yang mengandalkan teknologi informasi terintegrasi, termasuk PT Capella Medan, sebuah perusahaan yang berperan sebagai *dealer* resmi merek dagang *Daihatsu, Kubota*, dan *UD Trucks* dari Astra yang beroperasi di wilayah Sumatera dan Aceh. Perusahaan ini membutuhkan jaringan yang stabil untuk mendukung aktivitas administrasi, layanan pelanggan, koordinasi antar cabang, dan distribusi informasi. Namun, operasi perusahaan kerap terhambat oleh berbagai kendala jaringan, termasuk *downtime* yang mengganggu proses administrasi, transaksi penjualan, pelaporan, serta komunikasi internal dan eksternal. Pengelolaan risiko jaringan juga masih bersifat reaktif, dilakukan setelah terjadinya gangguan tanpa adanya kerangka kerja yang sistematis, pemetaan risiko yang jelas, maupun mekanisme pencegahan terencana. Akibatnya, risiko gangguan jaringan sulit dikendalikan dan menghambat pencapaian tujuan bisnis.

Kondisi tersebut menunjukkan perlunya penerapan manajemen risiko teknologi informasi yang terstruktur agar potensi gangguan dapat diidentifikasi, dievaluasi, dan dikendalikan secara sistematis[3]. Tanpa mekanisme yang terstruktur, perusahaan akan kesulitan melakukan deteksi dini, penanganan insiden, maupun pemulihan layanan ketika terjadi *downtime*. Oleh karena itu, pendekatan manajemen risiko menjadi dasar penting

untuk dilakukan audit teknologi informasi terhadap pengendalian dan kesiapan layanan jaringan. Audit yang tepat dapat mencegah terjadinya gangguan yang berdampak pada keberlangungan operasional, kerugian finansial, serta penurunan kualitas layanan organisasi[4].

Untuk menilai sejauh mana pengelolaan risiko telah berjalan, diperlukan pendekatan audit berbasis kerangka kerja yang terstandar. Berbagai kerangka kerja internasional pun dikembangkan sebagai acuan, masing-masing dengan fokus berbeda sesuai tujuan pengelolaan dan pengendalian teknologi informasi. *Information Technology Infrastructure Library (*ITIL*)* menitikberatkan pada *service management* dan tata kelola. *International Organization for Standardization (*ISO*)/ International Electrotechnical Commission (IEC) 27001* berfokus pada perlindungan data dan pengendalian akses terhadap aset informasi. *National Institute of Standards and Technology (NIST)* melengkapi pendekatan tersebut dengan pedoman teknis yang lebih mendalam mengenai manajemen risiko dan penanganan insiden keamanan siber. Sementara itu, *Control Objective for Information Technologies* (COBIT) 2019 menawarkan kerangka kerja tata kelola yang komprehensif dengan mengintegrasikan aspek manajemen layanan, keamanan, dan risiko untuk memastikan keselarasan antara strategi TI dan tujuan bisnis. Keberagaman kerangka kerja ini memberikan fleksibilitas bagi perusahaan dan auditor untuk memilih metodologi audit yang sesuai dengan kebutuhan[5].

Dalam konteks PT Capella Medan, COBIT 2019 dinilai paling relevan karena menyediakan mekanisme evaluasi yang terukur dan berorientasi pada pengelolaan risiko teknologi informasi secara menyeluruh serta dilengkapi dengan *Design Factors*, seperti *Risk Appetite and Tolerance, Enterprise Goals* dan mudah diintegrasikan dengan *framework* lain, seperti ITIL atau ISO/IEC 27001 guna memperkuat aspek operasional maupun keamanan informasi tanpa meninggalkan tata kelola utama[3,6,7]. Relevansi ini mendasari dua kajian terdahulu mengenai audit tata kelola TI di PT Capella Medan. Penelitian pertama pada 2013, menggunakan COBIT 4.1 domain *Plan and Organize* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS), dan *Monitor and Evaluate* (ME) menunjukkan tingkat kematangan tata kelola TI perusahaan masih memerlukan peningkatan signifikan[8]. Melengkapi kajian tersebut, penelitian lanjutan dilakukan pada tahun 2025 menggunakan COBIT 2019 untuk mengevaluasi domain EDM05 *(Ensured Stakeholder Engagement),* APO06 *(Managed Budget and Costs)*, BAI09 *(Managed Assets),* MEA03 *(Managed Compliance with External Requirements)* yang juga mendapatkan kesenjangan cukup besar antara kondisi aktual dengan kondisi ideal[9]. Meskipun demikian, kedua penelitian ini

belum menjadikan aspek risiko gangguan layanan TI sebagai fokus utama kajian, padahal keberlangsungan layanan TI merupakan faktor krusial yang menentukan kelancaran operasional, kualitas layanan, keamanan informasi, dan kepercayaan pemangku kepentingan[8,9].

Di samping itu, kajian pembanding yang melibatkan perusahaan sejenis dan institusi pendidikan menggunakan COBIT 2019 domain APO12 *(Managed Risk)* dan BAI03 *(Managed Solutions Identification and Build)* menunjukkan bahwa tingkat kapabilitas dan kematangan dalam pengelolaan risiko TI masih berada di bawah target yang diharapkan. Temuan ini semakin diperkuat dengan fakta bahwa belum adanya kajian yang secara mendalam dan sistematis membahas pengelolaan risiko terhadap gangguan layanan TI secara spesifik[10,11,12]. Oleh karena itu, hasil perbandingan ini memberikan dasar penting bagi penelitian di PT Capella Medan untuk melakukan audit manajemen risiko gangguan layanan jaringan yang lebih komprehensif, terukur, dan adaptif, guna memastikan ketahanan dan kontinuitas layanan TI perusahaan.

Tahapan awal penelitian di PT Capella Medan dilakukan dengan pelaksanaan wawancara, pemetaan *goals cascade*, dan pengisian *toolkit design factors* COBIT 2019 bersama *IT Section Head* PT Capella Medan. Berdasarkan hasil pemetaan *goals cascade* dan pengisian *design factors*, teridentifikasi bahwa terdapat 2 domain yang menjadi perhatian utama yang memperoleh nilai 100%, yaitu APO12 *(Managed Risk)* dan DSS02 *(Managed Service Requests and Incidents).* Kedua domain ini sama-sama berperan dalam menjaga keandalan layanan teknologi informasi, namun memiliki fokus dan karakteristik yang berbeda. DSS02 *(Managed Service Requests and Incidents)* menitikberatkan pada pengelolaan permintaan layanan dan penanganan insiden secara operasional sehingga bersifat reaktif karena tindakan dilakukan setelah terjadinya gangguan. Sebaliknya, APO12 *(Managed Risk)* berfokus pada pengelolaan risiko melalui proses identifikasi, analisis, dan mitigasi yang terencana sehingga bersifat proaktif dan preventif dalam mencegah terjadinya insiden di masa mendatang[3, 13].

APO12 *(Managed Risk)* merupakan salah satu proses dalam *Align, Plan, and Organize* pada COBIT 2019 yang berfokus pada pengelolaan risiko teknologi informasi secara menyeluruh dan terstruktur. Proses ini mencakup identifikasi risiko, analisis potensi dampak, evaluasi kemungkinan terjadinya risiko, serta perencanaan dan penerapan tindakan mitigasi yang tepat. Dengan pendekatan ini, APO12 *(Managed Risk)* membantu organisasi untuk bersikap proaktif dalam menghadapi ancaman yang dapat mengganggu kelangsungan layanan teknologi informasi. Selain itu, domain ini juga mendorong integrasi manajemen

risiko dengan strategi bisnis perusahaan sehingga setiap keputusan terkait teknologi informasi dapat mendukung tujuan strategis, meningkatkan ketahanan operasional, serta mengurangi potensi akibat insiden yang tidak terduga.

Berdasarkan karakteristik tersebut, domain APO12 *(Managed Risk)* dianggap paling relevan dengan tujuan audit yang berfokus pada peningkatan ketahanan serta pencegahan gangguan jaringan. Pendekatan ini sejalan dengan kebutuhan perusahaan untuk membangun manajemen risiko teknologi informasi yang lebih terstruktur, terukur, dan selaras dengan strategi bisnis guna mendukung keberlanjutan dan stabilitas layanan. Berdasarkan uraian tersebut, penelitian ini mengangkat judul **"Audit Manajemen Risiko Gangguan Layanan Jaringan pada PT Capella Medan Menggunakan *Framework* COBIT 2019 Domain APO12 *(Managed Risk)*".**

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang permasalahan di atas maka perumusan masalah adalah sebagai berikut:

1. Bagaimana tingkat *capability level* dan *maturity level* manajemen risiko gangguan layanan jaringan PT Capella Medan berdasarkan hasil audit menggunakan *framework* COBIT 2019 pada domain APO12 *(Managed Risk)?*
2. Bagaimana hasil *gap analysis* antara *capability level* dan *maturity level* aktual dengan yang diharapkan PT Capella Medan berdasarkan hasil audit ini?
3. Apa saja rekomendasi perbaikan yang sesuai dengan standar COBIT 2019 yang dapat dirumuskan untuk meningkatkan efektivitas manajemen gangguan risiko layanan jaringan di PT Capella Medan?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis *capability level* dan *maturity level* manajemen risiko gangguan layanan jaringan berdasarkan hasil *mapping* dan pengisian *design factors* COBIT 2019 dengan domain APO12 *(Managed Risk)* sebagai fokus utama PT Capella Medan.
2. Mengevaluasi kesenjangan *(gap analysis)* antara kondisi *capability* dan *maturity* saat ini *(as-is*) dengan *capability* dan *maturity* yang diharapkan *(to-be)* dalam pengelolaan risiko gangguan layanan jaringan berdasarkan domain APO12 *(Managed Risk)*.

3. Menyusun rekomendasi strategis berbasis hasil audit COBIT 2019 untuk meningkatkan efektivitas manajemen risiko gangguan layanan jaringan di PT Capella Medan, khususnya pada domain APO12 *(Managed Risk).*

1.4 Manfaat

Berikut merupakan manfaat yang dapat diberikan dari penelitian yang dilakukan:

1. Bagi Penulis
   a. Penelitian ini diharapkan dapat memberikan pemahaman mendalam tentang penerapan audit manajemen risiko gangguan layanan jaringan menggunakan *framework* COBIT 2019, khususnya pada domain APO12 *(Managed Risk).*
   b. Memperluas wawasan mengenai pengukuran tingkat kapabilitas, kematangan, dan kesenjangan *(gap analysis)* dalam pengelolaan risiko gangguan layanan jaringan sebagai bagian dari audit teknologi informasi yang efektif dan berkelanjutan.
2. Bagi Perusahaan
   a. Penelitian ini diharapkan dapat membantu perusahaan dalam mencapai peningkatan kesesuaian antara pengelolaan layanan jaringan dan tujuan strategis perusahaan sehingga pemanfaatan teknologi informasi dapat secara optimal mendukung visi dan misi PT Capella Medan.
   b. Hasil audit ini diharapkan dapat melengkapi laporan audit pada periode sebelumnya yang berfokus pada tata kelola teknologi informasi menggunakan *framework* COBIT 4.1 dan COBIT 2019 dengan terciptanya mekanisme evaluasi berkala yang terstruktur untuk memastikan manajemen risiko layanan teknologi informasi, khususnya pada layanan jaringan.
   c. Rekomendasi yang diberikan diharapkan dapat berkontribusi terhadap peningkatan kemampuan perusahaan dalam mengidentifikasi, menilai, dan mengendalikan risiko gangguan layanan jaringan guna memperkuat ketahanan operasional serta menjaga kontinuitas bisnis di tengah ancaman digital.

1.5 Ruang Lingkup

Agar permasalahan yang diteliti lebih terfokus dan terarah, penelitian ini dibatasi pada beberapa aspek, yaitu

1. Penelitian ini dilaksanakan pada PT Capella Medan berfokus pada manajemen risiko gangguan layanan jaringan teknologi informasi.

2. Metodologi yang digunakan berlandaskan pada kerangka kerja COBIT 2019 domain proses APO12 *(Managed Risk).*
3. Proses audit melibatkan departemen teknologi informasi PT Capella Medan sebagai pemangku kepentingan yang berperan langsung dalam pengelolaan dan pengendalian layanan jaringan.
4. Data penelitian diperoleh melalui analisis serta penyusunan pertanyaan yang mengacu pada pedoman resmi buku COBIT 2019 yang diterbitkan oleh ISACA.
5. Metode pengukuran yang digunakan adalah COBIT *Process Capability Model untuk* menilai tingkat kapabilitas proses serta COBIT *Performance Management* untuk menilai tingkat kematangan.

6. Nilai kesenjangan *(gap analysis)* diperoleh melalui metode perbandingan antara kondisi aktual *(as-is)* dan target yang diharapkan *(to-be).*