BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

PT XYZ adalah Penyedia Layanan Internet (ISP) Indonesia yang didedikasikan untuk menyediakan koneksi internet berkualitas tinggi dan terjangkau. Misi mereka menekankan pada memberikan manfaat dan kepuasan kepada pelanggan melalui layanan internet yang andal dan hemat biaya. PT XYZ bertujuan untuk mengembangkan bisnisnya dengan tetap menjaga kualitas koneksinya untuk menjamin kepuasan pelanggan. Perusahaan juga memiliki visi untuk menjadi berkah bagi seluruh pemangku kepentingan, termasuk pelanggan, investor, dan karyawan, yang mencerminkan komitmen mereka terhadap tanggung jawab sosial dan kesejahteraan masyarakat.

PT XYZ menawarkan beragam paket internet yang disesuaikan dengan kebutuhan berbeda dengan gratis 31 hari pertama. Paket-paket internet PT XYZ hadir dengan data tak terbatas, tanpa denda keterlambatan pembayaran, dan dukungan layanan pelanggan melalui WhatsApp, memastikan pengalaman yang lancar dan ramah pengguna. Fokus perusahaan dalam menyediakan akses internet yang stabil dan tanpa batas 24/7 menyoroti komitmen mereka terhadap keandalan dan kepuasan pelanggan.

Selain layanan internetnya, PT XYZ memiliki dukungan pelanggan dan layanan konsultasi aktif. PT XYZ menawarkan waktu respons yang cepat untuk menangani keluhan dan memberikan solusi terbaik untuk masalah akses internet. Sistem pembayaran tetap prabayar mereka memungkinkan pelanggan mengelola pengeluaran mereka dengan mudah, menjadikan layanan mereka nyaman dan hemat biaya. Memiliki cabang-cabang di pulau Jawa dan Sumatera, PT XYZ memiliki posisi yang baik untuk melayani masyarakat lokal dengan solusi internet berkualitas tinggi, sehingga berkontribusi terhadap konektivitas dan pertumbuhan digital di wilayah-wilayah tersebut.

1.2 Latar Belakang Penelitian

Salah satu infrastruktur besar pertama yang dibangun manusia untuk komunikasi internasional adalah jaringan telepon. Memasuki abad ke-20, tepatnya antara tahun 1910-1920, perkembangan teknologi informasi dan komunikasi ditandai dengan peluncuran transmisi suara tanpa kabel melalui siaran radio AM yang pertama. Perkembangan pesat komunikasi suara tanpa kabel ini diikuti oleh peluncuran transmisi audio-visual tanpa kabel, yang pertama kali muncul sebagai siaran televisi pada tahun 1940-an (Admin BKPSDM, 2022). Asal usul internet sendiri dimulai pada akhir tahun 1960-an sebagai inisiatif pertahanan militer AS selama Perang Dingin yang dimulai dengan konsep ARPA tentang "jaringan intergalaksi" dan berkembang dengan peralihan paket Donald Davies, yang memungkinkan data dikirim dalam bentuk paket. Pesan ARPANET pertama dikirimkan pada tahun 1969. Selama tahun 1970an dan 1980an, jaringan berkembang, menggabungkan protokol TCP/IP Vinton Cerf, yang memungkinkan jaringan yang berbeda untuk berkomunikasi. Pada tahun 1991, Tim Berners-Lee memperkenalkan *World Wide Web*, menciptakan jaringan informasi yang saling terhubung. Pada tahun 1990-an muncul *browser* yang mudah digunakan seperti Mosaic, yang mengarah pada komersialisasi internet. Pada tahun 2000-an, platform media sosial muncul, dan pada tahun 2020-an, sistem AI yang canggih terintegrasi, menjadikan internet penting dalam kehidupan sehari-hari (History.com, 2024).

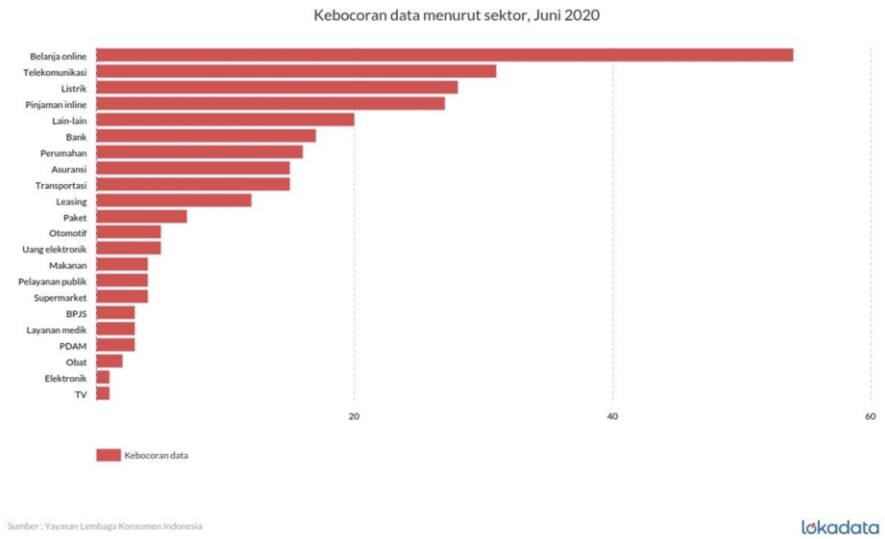
Setelah perkembangan industri telekomunikasi khususnya internet di dunia, pada tahun 1985 hingga 1993 di Indonesia perkembangan telekomunikasi semakin intensif seiring dengan pertumbuhan ekonomi dan meningkatnya permintaan sambungan telepon, sehingga menyebabkan evolusi telepon umum dalam beberapa variasi teknologi. Di Indonesia, evolusi industri telekomunikasi dimulai dengan ponsel 1G analog pada era 1990-an, yang kemudian berkembang pesat seiring dengan perubahan ukuran perangkat menjadi lebih kecil dan ringan. Tahun 2000 menjadi titik balik dengan lonjakan signifikan jumlah pelanggan, yang terus meningkat hingga ledakan penggunaan layanan 3G pada tahun 2006 setelah tiga operator mendapatkan izin. Regulasi pemerintah pada tahun 2007 membatasi operasi jaringan pada frekuensi 1900 MHz, namun ini tidak menghentikan

perkembangan yang telah memasuki era 4G dengan peluncuran oleh Internux pada tahun 2013, dan akhirnya 5G yang beroperasi secara komersial di seluruh negeri pada tahun 2021 (Balai Monitor Spektrum Frekuensi Radio Kelas I Semarang, 2023). Evolusi internet di Indonesia dimulai pada tahun 1980an dimana pengenalan jaringan komputer ke lima universitas perintis menandai dimulainya era digital baru meskipun terdapat tantangan yang ditimbulkan oleh infrastruktur yang tidak memadai. Popularitas radio amatir pada tahun 1986 membuka saluran komunikasi baru, yang mengarah pada penciptaan milis (*mailing* list) oleh pelajar Indonesia di luar negeri, yang memainkan peran penting dalam sejarah internet di negara ini. Pada awal tahun 1990-an, Onno W. Purbo melakukan eksperimen komunikasi gelombang radio yang inovatif antara Indonesia dan Kanada, yang membuka jalan bagi peluncuran ISP (*internet service* provider) Indonesia pada tahun 1994 dan *Radio Pocket* pada tahun-tahun berikutnya. Pada tahun 2000an terjadi kebangkitan milis pendidikan seperti Jaringan Informasi Sekolah, *booming* blog pada tahun 2003, dan munculnya media sosial pada tahun 2004, yang selanjutnya membentuk lanskap digital Indonesia (Kurikulum.id, 2020). Berdasarkan data Survei Susenas 2022 oleh Badan Pusat Statistik (2023), 66,48% masyarakat Indonesia mengakses internet pada tahun 2022, naik dari 62,10% pada tahun 2021. Tingginya penggunaan internet ini mencerminkan lingkungan keterbukaan informasi dan penerimaan masyarakat terhadap kemajuan teknologi telekomunikasi. Besarnya jumlah pengguna internet di Indonesia tidak lepas dari pesatnya pertumbuhan penggunaan telepon seluler.

Industri telekomunikasi di Indonesia banyak menjadi pemberitaan karena dugaan kebocoran data. Berdasarkan grafik pada Gambar 1.1 di bawah, kasus pembobolan data dalam sektor telekomunikasi berada dalam peringkat dua terbanyak. Tingginya angka pembobolan data di industri telekomunikasi tentu saja menimbulkan kekhawatiran terhadap keamanan data pribadi pengguna. Masyarakat khawatir data pribadinya akan disalahgunakan untuk kegiatan kriminal atau tindakan melanggar hukum lainnya oleh pihak yang tidak bertanggung jawab. Contoh kasus pelanggaran keamanan dalam industri telekomunikasi salah satunya terjadi pencurian data yang melibatkan dua teknisi internal di Lampung. Dua teknisi

yang diidentifikasi ditangkap oleh Bareskrim Polda Metro setelah diduga mencuri dan menjual data internet hingga meraup keuntungan sebesar Rp1,3 miliar. Pencurian itu terbongkar setelah adanya laporan dari manajemen yang kemudian dilanjutkan dengan penyelidikan dan pemasangan kamera CCTV di ruang kendali. Dari rekaman tersebut terungkap bahwa dua pelaku telah menyambung kembali sembilan sirkuit jaringan internet secara ilegal dan menjual data tersebut ke publik. Selain itu, tiga pelaku lainnya ditangkap atas peran mereka dalam penjualan paket internet curian itu. Pencurian itu diduga terjadi antara 1 Juli 2022 hingga 6 April 2024 (Purna Jaya & Susanti, 2024). Pasca laporan pembobolan data yang melibatkan beberapa oknum internal perusahaan ISP, industri telekomunikasi juga kembali dihebohkan dengan pencurian kabel fiber optik yang melibatkan empat bersaudara pelaku pencurian kabel fiber optik di Tasikmalaya. Empat tersangka yang diidentifikasi terlibat dalam pencurian di tujuh lokasi berbeda yang mengakibatkan kerugian hingga ratusan juta rupiah. Dalang pencurian yang bekerja di sebuah perusahaan pemasangan jaringan fiber optik, menggunakan pengetahuannya untuk mengatur pencurian tersebut. Kelompok ini mencuri kabel tidak hanya dari tempat penyimpanan tetapi juga dari lokasi pemasangan. Mereka tertangkap setelah mencuri kabel fiber optik sepanjang 4.000 meter senilai 28 juta rupiah. Penyelidikan lebih lanjut mengungkap bahwa mereka telah melakukan pencurian di enam lokasi lain, dengan satu insiden di Cihideung yang mengakibatkan kerugian sebesar 41 juta rupiah. Polisi terus melanjutkan penyelidikan untuk mendapatkan kembali kabel yang dicuri dan menangkap para pembeli, yang diyakini sebagai penyedia layanan internet ilegal di Bandung (Amiruddin, 2023). Ancaman yang tidak disengaja juga turut memberikan perhatian serius pada keamanan informasi industri telekomunikasi. Pada 1 Januari 2024, terjadi kebakaran di ruang baterai gedung transmisi salah satu ISP di Semarang yang mengakibatkan hilangnya sinyal sementara di sebagian wilayah Jawa Tengah dan Daerah Istimewa Yogyakarta. Kebakaran yang terjadi sekitar pukul 09.00 WIB tersebut berhasil dipadamkan oleh pemadam kebakaran setempat pada pukul 11.00 WIB. Kebakaran diduga disebabkan oleh korsleting listrik. Kejadian tersebut menyebabkan gangguan yang meluas, banyak pengguna

melaporkan tidak ada sinyal di ponsel mereka dan menyampaikan kekhawatiran mereka di media sosial. Perusahaan ISP tersebut segera mengatasi masalah tersebut, dan pada pukul 11.50 WIB, sinyal mulai pulih di beberapa wilayah (detikJateng, 2024). Ancaman tidak disengaja seperti ancaman lingkungan juga turut menjadi perhatian serius keamanan informasi. Pada tanggal 28 September 2018, OpenSignal mengukur dampak pada ketersediaan layanan jaringan akibat gempa bumi berkekuatan 7,5 skala Richter dan tsunami susulan di Palu, Sulawesi. OpenSignal mencatat penurunan signifikan yang membutuhkan waktu hampir dua minggu untuk pulih. Penurunan terburuk terjadi pada tanggal 30 September, ketika ketersediaan jaringan turun hampir 60%. Hal ini menunjukkan bahwa kerusakan pada menara seluler bukanlah satu-satunya masalah; pemulihan jaringan yang lambat juga disebabkan oleh meningkatnya beban dari lebih banyak pengguna yang terhubung ke lebih sedikit lokasi seluler yang beroperasi. Analisis ini menyoroti tantangan yang dihadapi operator jaringan dalam memulihkan layanan setelah bencana alam, seperti yang terlihat pada gempa bumi di Sulawesi (Rizzato, 2018). Berikut merupakan grafik sektor-sektor industri dengan kebocoran data terbanyak:



Gambar 1.1 Kebocoran data menurut sektor

Sumber: (Hidayah, 2020)

Pembobolan data ini menyoroti pentingnya keamanan fisik dalam melindungi data. Pendekatan komprehensif sangat penting, dengan fokus pada pengamanan infrastruktur, pengendalian akses terhadap fasilitas, pengujian

langkah-langkah keamanan, pengelolaan risiko seperti pencurian dan bencana alam, serta evaluasi kebijakan dan pelatihan. Langkah-langkah tersebut sangat penting untuk melindungi informasi pelanggan dan memitigasi risiko pelanggaran data. Keamanan fisik yang efektif tidak hanya mencakup perlindungan perangkat keras dan server tetapi juga penerapan kontrol akses yang ketat dan penilaian kerentanan rutin untuk mencegah potensi ancaman. Selain itu, strategi manajemen risiko yang kuat dan evaluasi kebijakan yang menyeluruh berkontribusi terhadap postur keamanan yang tangguh. Analisis risiko merupakan teknik penting yang dapat membantu organisasi mengidentifikasi risiko yang dihadapi aset mereka dan menentukan langkah-langkah keamanan yang harus diterapkan untuk memitigasi kemungkinan ancaman tersebut dan/atau potensi dampaknya. Metodologi ini dapat digunakan untuk mengevaluasi risiko yang terkait dengan berbagai aset dan menentukan kontrol keamanan yang tepat yang harus diterapkan untuk meminimalkan kemungkinan terjadinya risiko tersebut. Dengan menggunakan analisis risiko, organisasi dapat lebih memahami risiko yang mereka hadapi dan mengambil langkah-langkah untuk melindungi aset mereka dari potensi ancaman (Insua dkk., 2021). ISO 27001:2022 merupakan standar internasional yang menetapkan persyaratan untuk menetapkan, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi. Salah satu aspek manajemen keamanan informasi adalah perlindungan aset, seperti *software*, *hardware*, *network*, *personnel, site,* dan *organization* dari akses tidak sah, kerusakan, atau pencurian. Standar ini memberikan daftar pengendalian keamanan fisik pada Annex A bagian 7 atau pengendalian fisik.

Pengendalian fisik menjadi salah satu aspek keamanan informasi yang bertujuan untuk mencegah akses fisik, kerusakan, dan gangguan yang tidak sah terhadap lokasi dan aset informasi organisasi. Pengendalian fisik dapat mencakup kunci, pagar, penjaga, alarm, kamera, dan perangkat lain yang melindungi keamanan fisik sistem informasi dan data. Kantor pusat PT XYZ sebagai penyedia layanan internet, mengoperasikan 12 titik operasi atau cabang yang dipantau dan dikonfigurasi oleh pusat kendali jaringan (NOC) di kantor pusat. NOC bertanggung jawab atas pemantauan sistem dan penanganan awal gangguan sebelum tim teknis

melakukan kunjungan ke lokasi pelanggan jika diperlukan. Aset-aset dalam kantor pusat PT XYZ seperti *server, biling equipment, monitoring system* sebagai alat operasional perusahaan yang memiliki nilai informasi tinggi vital keberadaannya dalam memastikan kelancaran pelayanan perusahaan terhadap para pelanggan. Penulis dan peneliti melakukan wawancara dalam PT XYZ dan mengkonfirmasi beberapa hal terkait keamanan pengendalian fisik di PT XYZ. Dari wawancara tersebut didapatkan informasi bahwa dalam aspek pengendalian fisik, masih terdapat celah keamanan informasi pada PT XYZ diantaranya belum semua tempat memiliki parameter keamanan untuk melindungi aset-aset di dalamnya, tidak melakukan audit rutin proses manajemen kunci untuk mengelola kunci fisik atau informasi otentikasi, tidak mengunci dan memeriksa secara teratur area aman yang kosong dan lain-lain. Penelitian analisis risiko keamanan aset di kantor pusat PT XYZ yang belum memiliki sistem manajemen keamanan informasi diharapkan dapat melindungi data sensitif, memastikan kepatuhan terhadap peraturan, dan mengidentifikasi serta memitigasi potensi risiko. Menurut Siregar & Neaxie (2014), memastikan keamanan sumber daya sistem informasi sangatlah penting. Organisasi harus menerapkan Sistem Manajemen Keamanan Informasi (ISMS) untuk mengelola aset informasi mereka secara efektif. ISMS terdiri dari serangkaian kebijakan yang ditetapkan oleh organisasi untuk mendefinisikan, membangun, mengembangkan, dan memelihara keamanan sistem komputer mereka, termasuk sumber daya perangkat keras dan perangkat lunak. Dengan sistem informasi yang terjaga keamanannya, manajemen institusi dapat membuat keputusan dengan lebih mudah. Informasi yang salah dapat berdampak buruk pada aktivitas dan tujuan institusi. Mengelola keamanan informasi melibatkan risiko dari ancaman internal dan eksternal yang dapat merugikan institusi (Maingak et al., 2018). Oleh karena itu, penting bagi organisasi untuk melakukan penilaian risiko dan menerapkan tindakan pengendalian fisik yang tepat untuk memitigasi risiko dan melindungi aset informasinya (Rohman dkk., 2020).

Penelitian ini bertujuan untuk mengukur tingkat kematangan keamanan informasi perusahaan dalam domain pengendalian fisik, mengidentifikasi kerentanan dan ancaman terhadap aset-aset perusahaan, menganalisis dampaknya,

melakukan penilaian risiko, mengkaji penanganan dan mitigasi risiko, serta memberikan rekomendasi kontrol untuk mengatasi tingkat risiko. Penelitian ini menggunakan data primer yang diperoleh dari kuesioner dan wawancara, serta data sekunder yang diperoleh dari dokumentasi perusahaan. Penelitian ini menerapkan standar internasional ISO 27001:2022 untuk memberikan pendekatan yang lebih komprehensif terhadap keamanan informasi.

1.3 Perumusan Masalah

Perkembangan industri telekomunikasi di Indonesia dari 1985 hingga 1993 meningkat seiring pertumbuhan ekonomi dan permintaan telepon, memicu evolusi teknologi telepon umum dan seluler. Dari ponsel 1G analog pada 1990-an hingga lonjakan pelanggan pada 2000 dan ledakan 3G pada 2006, telekomunikasi terus berkembang hingga era 4G pada 2013 dan 5G pada 2021 (Balai Monitor Spektrum Frekuensi Radio Kelas I Semarang, 2023). Evolusi internet dimulai pada 1980-an dengan jaringan komputer di universitas, radio amatir pada 1986, dan ISP pertama pada 1994. Tahun 2000-an melihat kebangkitan milis pendidikan, booming blog pada 2003, dan media sosial pada 2004 (Kurikulum.id, 2020). Pada 2022, 66,48% masyarakat Indonesia mengakses internet, naik dari 62,10% pada 2021, mencerminkan tingginya penggunaan internet dan telepon seluler (Badan Pusat Statistik, 2023).

Industri telekomunikasi di Indonesia mengalami tingkat pembobolan data terbanyak kedua dibandingkan industri lain. Peningkatan kasus kebocoran data, menimbulkan kekhawatiran masyarakat terkait keamanan data pribadi. Salah satu kasus melibatkan dua teknisi internal di Lampung yang mencuri dan menjual data internet secara ilegal dengan keuntungan Rp1,3 miliar (Purna Jaya & Susanti, 2024), serta kasus pencurian kabel fiber optik oleh empat tersangka di Tasikmalaya, menyebabkan kerugian hingga ratusan juta rupiah (Amiruddin, 2023). Selain itu, ancaman tak disengaja seperti kebakaran di ruang baterai ISP di Semarang (detikJateng, 2024) dan gempa bumi di Palu pada 2018 juga memperburuk keamanan dan ketersediaan jaringan telekomunikasi (Rizzato, 2018).

Penelitian ini bertujuan untuk mengidentifikasi kerentanan dan ancaman terhadap aset perusahaan, menganalisis dampaknya, melakukan penilaian risiko,

mengkaji penanganan dan mitigasi risiko, serta memberikan rekomendasi kontrol untuk mengatasi tingkat risiko dengan fokus pada aset-aset pendukung perusahaan seperti *software, hardware, network,* dan *personnel*. Penelitian ini menggunakan data primer yang diperoleh dari kuesioner dan wawancara, serta data sekunder dari dokumentasi perusahaan. Penelitian ini menerapkan standar internasional ISO 27001:2022 untuk pendekatan keamanan informasi yang lebih komprehensif.

Berikut adalah pertanyaan penelitian terkait rumusan masalah:

1. Bagaimana tingkat kematangan keamanan informasi yang diterapkan oleh perusahaan saat ini?
2. Apa saja risiko yang ada pada aset-aset perusahaan saat ini?
3. Bagaimana cara mengendalikan dan meminimalisir dampak risiko pada aset-aset perusahaan?

1.4 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah diatas, tujuan-tujuan penelitian dapat dirumuskan menjadi:

1. Mengetahui tingkat kematangan keamanan informasi yang diterapkan oleh perusahaan saat ini.
2. Mengetahui risiko yang ada pada aset-aset perusahaan saat ini.
3. Memberikan cara mengendalikan dan meminimalisir dampak risiko pada aset-aset perusahaan.

1.5 Manfaat Penelitian

1.5.1 Aspek Teoritis

Penelitian ini memberikan kontribusi teoritis dengan mengembangkan kerangka kerja untuk manajemen keamanan informasi berdasarkan standar ISO 27001. Penelitian ini juga mengaplikasikan kerangka kerja tersebut pada studi kasus di perusahaan telekomunikasi di Indonesia, dan mengukur tingkat kematangan dan tingkat risiko aset yang ada. Penelitian ini juga memberikan rekomendasi kontrol yang sesuai untuk mengurangi tingkat risiko dan meningkatkan kinerja aset sistem teknologi informasi (Legowo & Juhartoyo, 2022).

1.5.2 Aspek Praktis

Penelitian ini memberikan manfaat praktis dengan memberikan panduan bagi perusahaan telekomunikasi dan organisasi lain yang ingin menerapkan manajemen keamanan informasi berdasarkan standar ISO 27001. Penelitian ini juga memberikan informasi mengenai aset, kerentanan, ancaman, dampak, dan risiko yang terkait dengan aset sistem teknologi informasi, serta cara mengukur dan mengevaluasinya. Penelitian ini juga memberikan saran untuk meningkatkan kesadaran dan kompetensi sumber daya manusia dalam hal sistem keamanan informasi (Legowo & Juhartoyo, 2022).

1.6 Sistematika Penulisan Tugas Akhir

BAB I PENDAHULUAN

Bab ini merupakan penjelasan secara umum, ringkas dan padat yang menggambarkan dengan tepat isi penelitian. Isi bab ini meliputi: Gambaran Umum Objek Penelitian, Latar Belakang Penelitian, Perumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan Tugas Akhir.

BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori dari umum sampai ke khusus, disertai penelitian terdahulu dan dilanjutkan dengan kerangka pemikiran penelitian yang diakhiri dengan hipotesis jika diperlukan.

BAB III METODE PENELITIAN

Bab ini menegaskan pendekatan, metode, dan teknik yang digunakan untuk mengumpulkan dan menganalisis temuan yang dapat menjawab masalah penelitian. Bab ini meliputi uraian tentang: Jenis Penelitian, Operasionalisasi Variabel, Populasi dan Sampel (untuk kuantitatif) / Situasi Sosial (untuk kualitatif), Pengumpulan Data, Uji Validitas dan Reliabilitas, serta Teknik Analisi Data.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian dan pembahasan diuraikan secara sistematis sesuai dengan pembahasan masalah serta tujuan penelitian dan disajikan dalam sub judul tersendiri. Bab ini berisi dua bagian: bagian pertama menyajikan hasil penelitian dan bagian kedua menyajikan pembahasan atau analisis dari hasil penelitian. Setiap aspek pembahasannya dimulai dari hasil analisis data, kemudian diinterpretasikan dan selanjutnya diikuti oleh kesimpulan kesimpulan. Dalam pembahasan sebaiknya dibandingkan dengan penelitian-penelitian sebelumnya atau landasan teoritis yang relevan.

BAB V KESIMPULAN DAN SARAN

Kesimpulan merupakan jawaban dari pertanyaan penelitian, kemudian menjadi saran yang berkaitan dengan manfaat penelitian.