BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi (TI) dengan perkembangannya yang pesat berdampak terhadap perilaku manusia untuk mengadopsi teknologi informasi itu sendiri guna memberikan manfaat dan efisiensi aktivitas mereka. Sudah bukan hal baru bahwa hampir semua bidang yang menjalankan proses bisnis berupa perusahaan profit maupun *non-profit*, organisasi, bahkan pemerintahan bergantung pada keberadaan teknologi informasi. TI telah mengilhami rekayasa ulang proses bisnis tradisional untuk bertransformasi menjadi lebih efisien, meningkatkan komunikasi di dalam perusahaan, antar perusahaan, serta antar pelanggan dan pemasoknya (Hall, 2008). Metodologi dan tata kelola yang baik merupakan suatu prasyarat yang menjadi kewajiban dalam pengelolaan sebuah sistem yang baik. Dengan tata kelola yang baik, maka sistem informasi yang *accountable* serta *sustainable* dapat tercapai bagi badan pemerintah dan dapat memberikan manfaat kepada publik seluas-luasnya (Ibrachim et al., 2012).

Data dan informasi merupakan objek utama yang tidak dapat dipisahkan dan merupakan sumber daya krusial yang perlu diperhatikan. Menurut (Rosmiati & Riadi, 2016) informasi menjadi suatu aset yang sangat penting dan berharga bagi keberlanjutan organisasi. Sangat pentingnya nilai sebuah informasi menyebabkan sering kali informasi hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi (Sarno & Iffano, 2009). Namun, banyaknya

informasi akan berbanding lurus dengan tingginya ancaman keamanan informasi *(information security)*. Keamanan informasi adalah perlindungan informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalkan risiko bisnis, memaksimalkan laba investasi dan peluang bisnis (Hassanzadeh et al., 2013). Kerentanan informasi terhadap ancaman menjadi masalah kompleks bagi perusahaan, organisasi, hingga pemerintahan. Kelemahan sekecil apa pun pada sistem keamanan informasi dapat memberikan dampak negatif terhadap pencapaian tujuan organisasi secara luas (Lenawati et al., 2017). Perusahaan perlu memastikan untuk dapat mengatasi kendala terkait aspek-aspek keamanan informasi. Tiga aspek tersebut dimaksudkan untuk melindungi keamanan informasi organisasi yaitu kerahasiaanya *(Confidentiality)*, menjaga keasliannya *(Integrity)*, dan menjamin ketersediaannya saat dibutuhkan *(Availability)* yang kemudian disebut CIA (Apriandari & Sasongko, 2018). Jika sebuah organisasi gagal memenuhi satu pun aspek dari CIA, keakuratan dan ketersediaan informasi dalam organisasi akan dipertanyakan, pengguna akan kehilangan kepercayaan pada informasi tersebut, dan kelangsungan bisnis organisasi akan sangat terpengaruh. Mengingat pentingnya peran keamanan informasi, instansi, khususnya instansi pemerintah yang menangani masalah informasi harus secara berkala meninjau tata kelola, menilai dan mengaudit aspek keamanannya.

Kesuksesan proses bisnis perusahaan yang unggul dari kompetitor dalam mengadopsi manfaat teknologi informasi tidak lepas dari adanya Tata Kelola TI *(IT Governance)*. Tata kelola TI didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengendalikan suatu perusahaan untuk mencapai tujuan bisnisnya dengan menambahkan nilai dan menyeimbangkan risiko yang terkait

dengan mengelola proses TI. Tidak hanya proses, tetapi juga memastikan bahwa proses tersebut diikuti oleh sumber daya TI yang memberikan dukungan optimal untuk pencapaian tujuan bisnis (Sarno, 2009). Tata Kelola TI merupakan bagian terintegrasi antara teknologi informasi dan manajemen organisasi, termasuk kepemimpinan, struktur organisasi, dan proses untuk memastikan penggunaan teknologi informasi secara optimal (Putra, 2019). Peningkatan kualitas sistem informasi pada lingkup organisasi swasta maupun pemerintah merupakan upaya terwujudnya tata kelola perusahaan yang baik *(Good Corporate Governance)* (Lenawati et al., 2017).

Untuk mengetahui kinerja pencapaian TI terhadap tujuan organisasi maka dibutuhkan audit tata kelola TI. Kegiatan audit memberikan informasi yang membantu organisasi mengelola risiko dan mengkonfirmasi alokasi sumber daya terkait TI yang efisien dalam mencapai tujuan TI dan tujuan bisnis (Gantz & Maske, 2014). Fungsi audit internal pada suatu organisasi harus secara periodik menilai tingkat efektivitas kontrol internal, termasuk kontrol keamanan informasi (Steinbart et al., 2012). Dalam lingkup sistem informasi, audit sistem informasi dilakukan dengan mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan bahwa sistem informasi dan sumber daya yang terkait memberikan perlindungan secara memadai terhadap aset-aset, dapat memelihara integritas data dan sistem serta mampu menyediakan informasi yang dibutuhkan pihak manajemen sesuai dengan pemenuhannya terhadap tujuan bisnis perusahaan (Sarno, 2009).

Lebih mengerucut lagi terdapat istilah audit keamanan sistem informasi. Menurut Ahmad (2012) yang lalu dikutip (Gunawan & Tjahjadi, 2021), audit keamanan merupakan proses di mana terdapat dasar kebijakan atau standar

keamanan untuk memutuskan kondisi dalam adanya perlindungan, dan untuk memeriksa apakah perlindungan terlaksana dengan baik. Berdasarkan buku (Ibrachim et al., 2012) tujuan utama dari audit keamanan, diantaranya adalah: a) Memeriksa kesesuaian dari mulai kebijakan, bakuan, pedoman, dan prosedur keamanan yang ada; b) Mengidentifikasi kekurangan dan memeriksa efektivitas dari kebijakan, bakuan, pedoman, dan prosedur keamanan yang ada ; c) Mengidentifikasi dan memahami kelemahan *(vulnerability)* yang ada; d) Mengkaji kendala keamanan yang ada terhadap permasalahan operasional, administrasi, dan manajerial, dan memastikan kesesuaian dengan bakuan keamanan minimum; e) Memberikan rekomendasi dan aksi perbaikan atau koreksi untuk peningkatan. Manajemen keamanan informasi merupakan bagian dari keseluruhan sistem manajemen organisasi, yang berdasarkan pendekatan risiko bisnis untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan suatu keamanan informasi (Fauzi, 2018).

Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Kediri adalah Satuan Kerja Perangkat Daerah (SKPD) yang merupakan unsur pelaksana urusan Pemerintahan Daerah di bidang Komunikasi dan Informatika, urusan Pemerintahan Daerah di bidang Persandian dan urusan Pemerintahaan Daerah di bidang Statistik. Diskominfo Kabupaten Kediri berdiri atas dasar hukum Peraturan Bupati Kediri Nomor 31 Tahun 2022 tentang kedudukan, susunan organisasi, uraian tugas dan fungsi serta tata kerja Dinas Komunikasi dan Informatika Kabupaten Kediri. Penerapan TIK di lingkungan pemerintahan kerap dikaitkan dengan istilah *e-Government*. Dengan adanya *e-Government* diharapkan kualitas kinerja pemerintah dalam pelayanan masyarakat dapat lebih meningkat (Riesta, 2022). Begitu halnya

dengan Pemerintah Kabupaten Kediri menerapkan konsep *e-Government* yang dikembangkan oleh Diskominfo Kabupaten Kediri.

Sistem Manajemen Keamanan Informasi (SMKI) diimplementasikan untuk melindungi aset informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimal kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi, dan peluang usaha (Fauzi, 2018). Sesuai Peraturan Bupati Nomor 33 Tahun 2019 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) Kabupaten Kediri juga menyebutkan bahwa "Setiap SKPD harus menerapkan Keamanan SPBE". Untuk pemeliharaan dan peningkatan keamanan informasi, Diskominfo Kabupaten Kediri melaksanakan diskusi secara rutin dan berkala 2 kali dalam setahun namun pendokumentasian hanya sebatas notulensi. Penelitian sebelumnya (Wulandari, 2017) yang telah melakukan evaluasi pada Diskominfo Kabupaten Kediri menggunakan indeks Keamanan Informasi mendapatkan hasil evaluasi terhadap tingkat kelengkapan penerapan standar ISO 27001 memperoleh skor "163" yang berada dalam area berwarna "Merah" dan dikategorikan sebagai "Tidak Layak" untuk menerapkan sertifikasi SNI ISO 27001:2013.

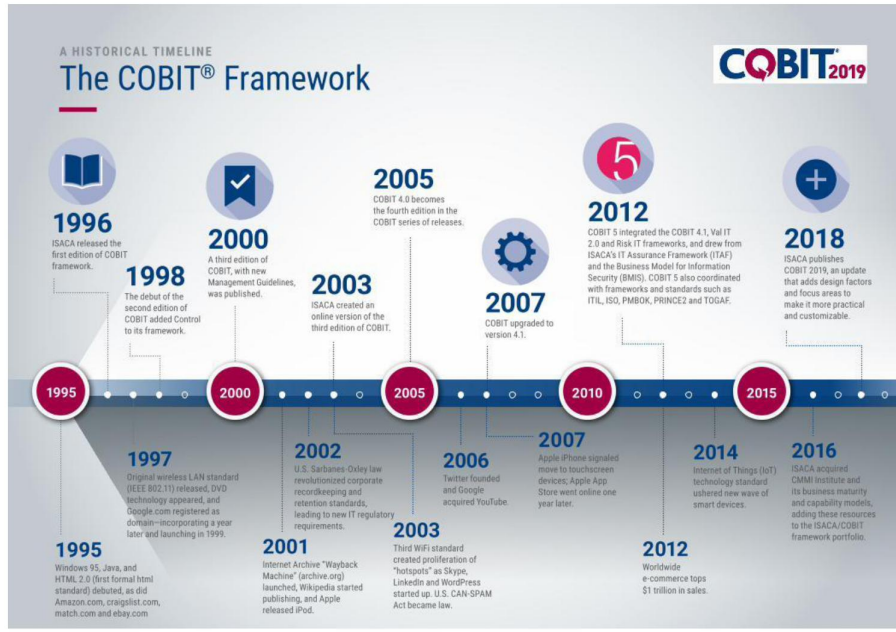
Berdasarkan Peraturan Bupati Kediri Nomor 31 Tahun 2022 tentang kedudukan, susunan organisasi, uraian tugas dan fungsi serta tata kerja menyatakan bahwa Diskominfo Kabupaten Kediri sebagai wali data memiliki kewenangan merencanakan, merancang, membangun, mengembangkan, mengoperasikan, dan mengevaluasi SPBE. Bidang Aplikasi Informatika memiliki wewenang untuk penyelenggaraan urusan layanan infrastuktur dasar *data center, disaster recovery center* & TIK, layanan keamanan informasi *e-Government*, layanan manajemen data dan informasi *e-Government*, hingga penyelenggaraan *Government Chief*

Information Officer (GCIO) Pemerintah Kabupaten. Selain itu, Diskominfo Kabupaten Kediri pernah mengalami gangguan jaringan pada kantor kecamatan menimbulkan kendala pada layanan informasi maupun terhadap proses pelaksanaan pelaporan yang mengancam keamanan data seperti yang disebutkan oleh Bapak Arik selaku analis tata kelola keamanan siber (bukti pada lampiran 1) yang dikuatkan keterangan pada Buku 1 Kondisi Eksiting dan Analis GAP SPBE Pemerintah Kabupaten Kediri (bukti pada lampiran 2). Sebagai tindakan preventif, diperlukan sebuah pengukuran tingkat kapabilitas manajemen keamanan informasi pada Diskominfo Kabupaten Kediri.

Pengukuran tingkat kapabilitas harus memiliki acuan *best practice* yaitu sebuah proses yang telah berhasil digunakan oleh perusahaan dan dapat menjadi contoh yang baik dari implementasi serupa di perusahaan lain. Pihak Diskominfo Kabupaten Kediri berminat menerapkan kerangka kerja yang dapat membantu melibatkan kepentingan manajemen dalam mengambil keputusan dalam organisasi sekaligus layanan yang disampaikan dapat terjamin (bukti lampiran 1). Tidak ada acuan baku mengenai standar yang harus digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan sistem informasi (Sarno & Iffano, 2009). Beberapa *best practice* seperti COBIT dan ISO/IEC 27001 dapat digunakan sebagai landasan untuk pengembangan proses keamanan informasi yang baik (Sheikhpour & Modiri, 2012). ISO/IEC 27001 hanya fokus pada keamanan informasi tetapi ketika membahas kontrol pada ISO/IEC 27001 maka sudah mencakup sebagian besar COBIT terutama proses DSS05 – Manajemen Kemanan Layanan. Meskipun COBIT tidak memiliki pesyaratan keamanan informasi sedetail ISO 27001 namun COBIT mencakup topik manajemen TI yang jauh lebih luas dan biasanya

digunakan sebagai bagian dari sistem manajemen organisasi secara keseluruhan. Sehingga dalam pengukuran tingkat kapabilitas keamanan informasi pada studi kasus ini, digunakan kerangka kerja tata kelola TI yaitu COBIT 5.

COBIT *(Control Objective for Information and Related Technology)* yang dibuat oleh *Information System Audit and Control Association* (ISACA) merupakan kerangka panduan tata kelola TI dan atau bisa juga disebut sebagai *toolset* pendukung yang bisa digunakan untuk menjembatani *gap* antara kebutuhan dan langkah teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi. COBIT memungkinkan pengembangan kebijakan yang jelas dan sangat baik digunakan untuk TI kontrol seluruh organisasi, membantu meningkatkan kualitas dan nilai serta menyederhanakan pelaksanaan alur proses sebuah organisasi dari sisi penerapan TI (ITGID, 2016a). COBIT yang dikembangkan oleh ISACA telah ada semenjak 1996 dan telah berkembang dengan menambahkan berbagai fitur dan kontrol baru sampai perkembangan menjadi COBIT 5 yang selanjutnya dikeluarkanlah versi terbaru yaitu COBIT 2019 seperti pada gambar 1.1. COBIT 5 hanya menggunakan *capability level* tetapi pada COBIT 2019 adanya penambahan menjadi *capability level* dan *maturity level*. Dari segi kelebihan COBIT 5 lebih banyak digunakan sedangkan dari kekurangannya tidak bersifat fleksibel sedangkan COBIT 2019 kelebihannya lebih bersifat fleksibel dan kekurangannya prinsip dan detail domainnya lebih banyak sehingga akan lebih sulit dalam implementasi (Syuhada, 2021).



Gambar 1.1 Sejarah COBIT Berdasarkan Waktu (ISACA, 2018)

COBIT 5 sendiri adalah *a set of best practice* bagi pengelolaan teknologi informasi *(IT management)* yang secara lengkap terdiri dari*: executive summary, framework, control objectives, audit guidelines, implementation tool set* serta *management guidelines* yang sangat berguna untuk proses sistem informasi strategis (ITGID, 2016b). COBIT 5 memberikan layanan kerangka kerja secara komprehensif untuk membantu mengatur dan manajemen TI dalam sebuah perusahaan mencapai tujuan yang diharapkan. COBIT 5 memiliki sifat umum dan dapat digunakan untuk semua instansi, baik komersial maupun sektor publik. Bahkan COBIT 5 memiliki sebuah produk yang khusus berfokus pada keamanan informasi yaitu COBIT 5 *for Information Security* (ISACA, 2012b). Meskipun telah diterbitkan versi terbaru yaitu COBIT 2019 seperti yang disebutkan sebelumnya namun penelitian terkait COBIT 2019 sangat terbatas sehingga diputuskan menggunakan kerangka kerja COBIT 5 pada studi kasus ini.

Selain itu, COBIT 5 merupakan kerangka kerja untuk manajemen, yang mampu mencakup aspek teknis maupun non teknis, mengelola semua yang berkaitan dengan teknologi informasi mulai dari pemenuhan kebutuhan para *stakeholder* terhadap teknologi informasi. COBIT 5 memiliki prinsip dasar untuk tata kelola dan manajemen TI (Sinaga et al., 2021). Kelebihan lain COBIT 5 yaitu adanya metrik, acuan dan pelaksanaan audit, serta adanya tata kelola dan manajemen yang menyeluruh (Aritonag et al., 2018) dan dapat diterapkan COBIT 5 bersifat generik dan berguna untuk perusahaan dari semua ukuran, baik komersial, nirlaba atau di sektor publik (ISACA, 2012a). Sehingga judul penelitian yang diajukan adalah **"Pengukuran Tingkat Kapabilitas Manajemen Keamanan Informasi Menggunakan Kerangka Kerja COBIT 5"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah dalam skripsi ini adalah bagaimana evaluasi pengukuran tingkat kapabilitas manajemen keamanan informasi SPBE pada Dinas Komunikasi dan Informatika Kabupaten Kediri menggunakan kerangka kerja COBIT 5?

1.3 Batasan Masalah

Beberapa batasan masalah pada skripsi ini adalah sebagai berikut:

a. Pengukuran tingkat kapabilitas keamanan informasi ini dilaksanakan di Dinas Komunikasi dan Informatika Kabupaten Kediri yang beralamat di Jl. Sekartaji No. 2, Kabupaten Kediri.
b. *Framework* yang digunakan adalah COBIT 5.

c. Pengukuran tingkat kapabilitas fokus proses pada APO13 dan DSS05.
d. Langkah-langkah untuk pengukuran tingkat kapabilitas *(Capability Level)* dalam skripsi ini menggunakan *Assessment Process Activities* COBIT 5.
e. Skripsi ini tidak membahas manajemen risiko.
f. Hasil skripsi ini terdiri dari tingkat kapabilitas, analisa *gap* level, dan saran perbaikan berdasarkan temuan.

1.4 Tujuan Penelitian

Adapun tujuan skripsi ini adalah untuk mengetahui tingkat kapabilitas manajemen keamanan informasi SPBE Dinas Komunikasi dan Informatika Kabupaten Kediri sebagai evaluasi berdasarkan kerangka kerja COBIT 5.

1.5 Manfaat

Adapun manfaat yang dapat diambil dari hasil penelitian ini adalah:

1. Bagi dunia akademis, hasil dari penelitian ini diharapkan dapat digunakan sebagai referensi penelitian dalam mengukur tingkat kapabilitas sesuai dengan COBIT 5 untuk penelitian selanjutnya terkait manajemen keamanan informasi. Sekaligus menjadi acuan untuk penelitian lebih baik dan terbaru.
2. Bagi Dinas Komunikasi dan Informatika Kabupaten Kediri, penelitian ini diharapkan dapat digunakan sebagai gambaran tingkat kapabilitas dari manajemen keamanan informasi saat ini sehingga menjadi referensi evaluasi bagi instansi. Kemudian mendapatkan temuan yang dapat digunakan sebagai pertimbangan dalam pengambilan keputusan. Sehingga saat dilakukan evaluasi oleh lembaga resmi dapat mendapatkan hasil yang baik.

1.6 Relevansi Audit Sistem Informasi dengan Sistem Informasi

Audit didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (*audit*) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (Meyliana et al., 2020). Sedangkan definisi sistem informasi secara teknis merupakan serangkaian komponen yang saling berhubungan yang mengumpulkan, menyimpan, memproses, dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan pengawasan di sebuah organisasi. Sistem informasi juga membantu manajer dan karyawan dalam menganalisis masalah, menggambarkan hal-hal yang rumit, juga menciptakan produk atau inovasi baru. Sistem informasi berisi informasi-informasi penting berupa, orang, tempat/lokasi, dan hal-hal penting lainnya yang berkaitan dengan organisasi dan lingkungan luar organisasi tersebut (Laudon & Laudon, 2019). Dalam lingkup sistem informasi, audit sistem informasi dilakukan dengan mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan bahwa sistem informasi dan sumber daya yang terkait memberikan perlindungan secara memadai terhadap aset-aset, dapat memelihara integritas data dan sistem serta mampu menyediakan informasi yang dibutuhkan pihak manajemen sesuai dengan pemenuhannya terhadap tujuan bisnis perusahaan (Sarno, 2009). Audit sistem informasi digunakan untuk mengidentifikasi semua

kontrol yang mengatur sistem informasi individual dan menilai efektivitasnya (Laudon & Laudon, 2019).

Relevansi antara audit sistem informasi dengan sistem informasi juga telah dijelaskan dalam kurikulum AISINDO (Asosiasi Sistem Informasi Indonesia) pada poin 7 yang menjelaskan bahwa "Disiplin ilmu Sistem Informasi mempelajari berbagai aspek mencakup Perencanaan Sistem Informasi, Perancangan Sistem Informasi, Pembangunan Sistem Informasi, Operasional Sistem Informasi, Evaluasi Atau Audit Sistem Informasi, Faktor-Faktor Yang Menyebabkan Sebuah SI/TI Dapat Diterima Target Penggunanya (*Adoption/Diffusion*), Bagaimana Sebuah SI/TI Digunakan Target Penggunanya (*Domestication*), Dan Bagaimana Pengaruh/Dampak Penggunaan Sebuah SI/TI (*Impacts* Atau *Post Adoption Stage*)" (AISINDO, 2018).

Sedangkan COBIT 5 *(Control Objective for Information and Related Technology)* yang dibuat oleh *Information System Audit and Control Association* (ISACA) merupakan kerangka panduan tata kelola TI dan atau bisa juga disebut sebagai *toolset* pendukung yang bisa digunakan untuk menjembatani *gap* antara kebutuhan dan langkah teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi. COBIT memungkinkan pengembangan kebijakan yang jelas dan sangat baik digunakan untuk TI kontrol seluruh organisasi, membantu meningkatkan kualitas dan nilai serta menyederhanakan pelaksanaan alur proses sebuah organisasi dari sisi penerapan TI (ITGID, 2016a). Secara keseluruhan, COBIT 5 menyediakan kerangka kerja yang terstruktur dan komprehensif untuk mengelola dan mengatur sistem informasi. Relevansinya terletak pada kemampuannya untuk membantu organisasi menyelaraskan TI dengan tujuan

bisnis, membangun kontrol dan proses yang efektif, mengelola risiko, mengukur kinerja, dan mengintegrasikan dengan standar lain yang relevan. Dengan mengadopsi COBIT 5, organisasi dapat meningkatkan nilai, keandalan, dan keamanan sistem informasi (ISACA, 2012a).

1.7 Sistematika Penulisan

Sistematika penulisan bertujuan untuk mengarahkan sekaligus menjadi acuan dalam penyusunan laporan skripsi agar sesuai dengan tujuan penulisan laporan skripsi yang diharapkan. Laporan skripsi terbagi menjadi 5 bab yaitu:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, relevansi audit sistem informasi dengan sistem informasi dan sistematika penulisan yang digunakan dalam penyusunan laporan skripsi ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang informasi umum dari tempat studi kasus yaitu Dinas Komunikasi dan Informatika Kabupaten Kediri, dan memuat penjabaran mengenai teori-teori dasar yang dipergunakan dalam penyusunan laporan skripsi ini yang diambil dari berbagai sumber literatur dan kajian-kajian sebelumnya.

BAB III METODOLOGI PENELITIAN

Bab ini berisi metode penelitian secara runtut dan sistematis sebagai acuan agar tujuan dari penelitian ini dapat tercapai.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil yang lebih terperinci sekaligus pembahasan dari tiap-tiap tahapan dimulai dari *initiation, planning the assessment, briefing, data collection, data validation, process attribute level,* dan *reporting the result.*

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Bab ini berisi daftar rujukan pustaka yang mendukung penyusunan skripsi ini. Studi pustaka didapat dari berbagai sumber seperti buku, jurnal, dan internet.

LAMPIRAN

Lampiran terdapat beberapa dokumen pendukung untuk melengkapi penyusunan laporan skripsi ini.