BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Pada bab ini dilakukan kajian-kajian *literatur review* terkait topik permasalahan penelitian ini dengan mengeksplorasi *repository* jurnal-jurnal seperti *sciencedirect*, *IEEExplore* dan *Google Scholar*. Dari banyak review pada penelitian-penelitian dari para peneliti sebelumnya menghasilkan ringkasan sepuluh tinjauan pustaka yang memiliki pembahasan paling terkait dengan penelitian ini. Guna memperkuat posisi penelitian ini, dirancang kajian seperti ditunjukkan pada tabel 2.1

Tabel 2.1 *State of The Art* Penelitian

No	Sitasi	Judul, Penulis dan Tahun	Tujuan Permasalahan	Metodologi	Hasil	Catatan
1	(Nawir dkk., 2022)	Integrasi *Framework* ISO 27001 dan COBIT 2019 pada Keamanan Informasi Smart *Tourism* PT. YoY Manajemen Internasional (Muhammad Nawir, Irfan AP, Farid)	Memberikan gambaran tentang penggunaan kombinasi ISO 27001 dan COBIT 2019, dengan fokus pada pemetaan objektif proses dan klausul	Pemetaan objektif dilakukan dengan menyelaraskan visi misi organisasi dengan *enterprise goal* COBIT 2019 dan objektif APO13 (*Managed Security*).	Pemilihan klausul ISO 27001 ditentukan berdasarkan objektif proses APO13 pada COBIT 2019.	Teknik pemetaan yang digunakan berhasil menunjukkan hubungan yang jelas antara klausul dan objektif, sehingga pemilihan klausul lebih terarah dan terstruktur.

Tabel 2.1 *State of The Art* Penelitian (Lanjutan)

No	Sitasi	Judul, Penulis dan Tahun	Tujuan Permasalahan	Metodologi	Hasil	Catatan
2	(Sidik, 2023)	Audit Sistem Informasi Berbasis COBIT 2019 Menggunakan Standar ISO (Sidik, 2023)	Mengembangkan audit manajemen keamanan TI dengan ISO 27001:2005, serta mengevaluasi dan menyajikan instrumen audit.	Pendekatan kualitatif dengan langkah-langkah audit: perencanaan persiapan, pelaksanaan dan pelaporan audit.	Hasil inspeksi menunjukkan rata-rata 65%, dengan temuan penting yang perlu diperbaiki.	Audit menggunakan ISO 27001 untuk menilai tingkat maturitas yang tercapai setelah mengadopsi COBIT 2019
3	(King, 2017)	*Examine The Relationship Between Information Technology Governance, Control Objectives For Information And Related Technologies*, ISO 27001/27002, *And Risk Management* (King, 2017)	Mengkaji keterkaitan antara COBIT 5, ISO 27001/27002, dan Manajemen Risiko TI serta mengeksplorasi bagaimana mereka dapat digabungkan dalam tata kelola SI/TI.	Pendekatan survei dengan 210 responden profesional IT (manajer dan eksekutif) menggunakan *Survey Monkey* dan analisis statistik dengan SPSS serta regresi *linear multiple*.	¾ responden percaya bahwa ISO 27001/27002, Manajemen Risiko TI, dan COBIT 5 dapat diadopsi bersama dalam organisasi dan dapat diselaraskan untuk tata kelola SI/TI yang baik.	Penelitian menunjukkan keselarasan antara ketiga standar ini dalam mencapai tata kelola SI/TI yang baik, memungkinkan untuk diintegrasikan bersama.

Tabel 2.1 *State of The Art* Penelitian (Lanjutan)

No	Sitasi	Judul, Penulis dan Tahun	Tujuan Permasalahan	Metodologi	Hasil	Catatan
4	(Shraim, 2020)	*Quality Standards in Online Education: The ISO/IEC 40180 Framework* (Shraim, 2020)	Meningkatkan kualitas pendidikan *online* (QOE) dengan menggunakan ISO/IEC 40180 sebagai kerangka kerja.	Analisis terhadap 72 publikasi antara tahun 2000 dan 2019 untuk mengevaluasi kualitas pendidikan *online* (QOE).	ISO/IEC 40180 dianggap solusi yang tepat untuk kualitas pendidikan *online*, meskipun belum ada kerangka kualitas holistik.	Kerangka kerja ISO/IEC 40180 perlu diintegrasikan dengan standar nasional pendidikan, seperti ISO 21001.
5	(Prapena & Pamuji, 2020)	*Information System Security Analysis of XYZ Company Using COBIT5 Framework and* ISO 27001:2013 (Prapena & Pamuji, 2020)	Mengkaji evaluasi sistem informasi / teknologi informasi (SI/TI) dengan menggunakan COBIT 5 dan ISO 27001 untuk mencari *gap analysis.*	Audit bertahap dimulai dengan ISO 27001, kemudian COBIT 5, untuk mengidentifikasi *gap* antara kondisi saat ini dan posisi yang diinginkan.	*Gap analysis* menunjukkan perbedaan kecil antara kondisi saat ini dan target, serta rekomendasi perbaikan untuk meningkatkan tata kelola.	Audit dilakukan dengan ISO 27001 terlebih dahulu, diikuti dengan COBIT 5 untuk meningkatkan tata kelola SI/TI.
6	(Yasin dkk., 2020)	*Designing Information Security*	Mengatasi kesulitan dalam	Pemetaan antara kedua	ISO 27001 dijadikan acuan	Tanpa teori acuan yang jelas dalam

Tabel 2.1 *State of The Art* Penelitian (Lanjutan)

No	Sitasi	Judul, Penulis dan Tahun	Tujuan Permasalahan	Metodologi	Hasil	Catatan
		Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)	menggabungkan dua *framework* ITG (ISO 27001 dan COBIT 2019) untuk mendesain rekomendasi tata kelola SI/TI.	*framework* dilakukan dengan menjadikan ISO 27001 sebagai acuan utama, dan COBIT 2019 sebagai turunan.	utama, dengan klausul-klausulnya dipetakan ke dalam domain COBIT 2019.	pemetaan, proses ini bisa menjadi bias dan subjektif.
7	(Tohet & Cahyono, 2020)	Peningkatan Mutu Perguruan Tinggi Pesantren Melalui ISO 21001 (Tohet & Cahyono, 2020)	Menilai dan mengevaluasi *gap* dalam organisasi dengan menggunakan alat bantu eksternal selain ISO 21001.	Dibutuhkan *tools* atau teknik analisis tambahan di luar ISO 21001 untuk mengidentifikasi *gap* yang ada.	*Tools* yang digunakan menggambarkan perbandingan antara kondisi saat ini dan target, dengan referensi ke level-level pada CMMI COBIT 2019.	Alat atau teknik yang digunakan berasal dari luar ISO 21001, karena ISO 21001 tidak menyediakan *toolkit* bawaan untuk *gap analysis.*
8	(Bawono dkk., 2020)	*Analysis Correlation of the Implementat*	Menganalisis perbedaan tiap domain dan klausul pada	Uji korelasi terhadap beberapa variabel:	COBIT 5 menunjukkan hasil terbaik	Penelitian menunjukkan bahwa COBIT 5

Tabel 2.1 *State of The Art* Penelitian (Lanjutan)

No	Sitasi	Judul, Penulis dan Tahun	Tujuan Permasalahan	Metodologi	Hasil	Catatan
		ion Framework COBIT 5, ITIL V3, and ISO 27001 for ISO 10002 Customer Satisfaction (Bawono dkk., 2020)	*framework* ITG COBIT 5, ITIL, ISO 27001, dan ISO 10002 terkait kepuasan pelanggan.	*customer-oriented service, service operation incident management, information security incident management, dan customer satisfaction.*	pada semua variabel yang diuji, dengan nilai rata-rata tertinggi untuk tiap variabel.	dapat mewakili semua standar yang ada dan memberikan hasil terbaik untuk setiap variabel.
9	(Rohayati & Delvika, 2020)	*Preparation for the Implementation of ISO 21001: 2018 using Assistance Program: Case study of Telkom Vocational High School* (Rohayati & Delvika, 2020)	Mengukur dan merencanakan persiapan implementasi ISO 21001 untuk manajemen pendidikan di *Telkom Vocational High School.*	Persiapan dan perencanaan strategi dilakukan dengan bantuan ahli, serta pengukuran tingkat kapabilitas saat ini melalui wawancara dan kuesioner.	Setelah diukur, kondisi saat ini dipetakan dan diselaraskan dengan ISO 21001. Terdapat 3 klausul yang menunjukkan kapabilitas rendah.	Penelitian ini menunjukkan bahwa ISO 21001 memiliki tingkat capaian yang tinggi dalam manajemen pendidikan, meskipun ada beberapa klausul dengan kapabilitas rendah.
10	(Yadav dkk., 2021)	*Quality System Certificatio*	Memberikan gambaran mengenai	Analisis deskriptif perbandinga	ISO 21001 menunjukkan	ISO 21001 memiliki capaian

Tabel 2.1 *State of The Art* Penelitian (Lanjutan)

No	Sitasi	Judul, Penulis dan Tahun	Tujuan Permasalahan	Metodologi	Hasil	Catatan
		ns in Education Sector (Yadav *dkk.*, 2021)	standarisasi internasional yang relevan dengan manajemen pendidikan.	n antara ISO 9001 dan ISO 21001, termasuk fase PDCA, *scope*, dan keunggulan terkait akreditasi institusi pendidikan.	kemandiri an institusi dari segi pendanaan dibanding ISO 9001, namun biayanya lebih tinggi.	tinggi dalam manajemen pendidikan, tetapi memerlukan biaya lebih tinggi bagi institusi yang menginginka n sertifikasi ini.

Berdasarkan *literatur review* yang dilakukan pada tabel 2.1, terdapat 10 paper relevan terkait penelitian ini. *Gap* penelitian paling mendasar adalah riset menjadi dasar panduan bagi peneliti dan audit SI/TI lainnya dalam melakukan pengelolaan tata kelola SI/TI dan juga keamanan informasi dan komunikasinya dalam bidang manajemen organisasi pendidikan. Selain itu dalam dunia pendidikan, khususnya pendidikan tinggi, ISO 21001 yang merupakan standarisasi internasional dibidang manajemen organisasi pendidikan, dapat dikolaborasikan dengan alat audit SI/TI, yang dalam riset ini dilakukan pemilihan antara ISO 27001 atau COBIT 2019 oleh karena itu peneliti mengusulkan penelitian ini. Skenario penelitian ini akan memilih domain dan klausul mana yang harus dipilih untuk dilakukan olah data, sehingga tidak semua domain dan klausul alat audit digunakan. Dari 65 *paper* yang di *review*, yang kemudian berhasil dibuat *resume* perbedaan mendasar antara ISO 27001 dan COBIT 2019 terhadap korelasi dengan ISO 21001, ditunjukkan pada tabel 2.2 dan 2.3. Berdasarkan komparasi model evaluasi (tabel 2.2), ISO 21001 dan 27001 memiliki banyak korelasi dikarenakan merupakan 1 keluarga ISO, dikembangkan oleh ISO/IEC.

Tabel 2. 2 Komparasi Berdasarkan Model Evaluasi

No	Indikator Kunci	ISO 21001	ISO 27001	COBIT 2019	Keterangan
1	Pengembang	ISO/IEC	ISO/IEC	ISACA	ISO 21001 dan ISO 27001 dikembangkan oleh ISO/IEC, sedangkan COBIT 2019 dikembangkan oleh ISACA.
2	Jenis Model	Standarisasi internasional; ISO 20000 *Family*	Standarisasi internasional; ISO 20000 *Family* (ISF)	Kerangka kerja audit (ITG)	ISO 27001 merupakan bagian dari ISF, sedangkan COBIT 2019 merupakan ITG.
3	Fokus Bidang	Manajemen sistem pendidikan	Manajemen sistem keamanan teknologi dan informasi	Manajemen tata kelola SI/TI	Masing-masing memiliki fokus yang sangat berbeda dalam evaluasinya.
4	Fokus Domain dan Klausul	11 lausul: 1. *Introduction* 2. *Scope* 3. *Normative references* 4. *Terms and definitions* 5. *Context of organization* 6. *Leadership* 7. *Planning* 8. *Support* 9. *Operation* 10. *Performance evaluation* 11. *Improvement*	11 Klausul: 1. *Introduction* 2. *Scope* 3. *Normative references* 4. *Terms and definitions* 5. *Context of organization* 6. *Leadership* 7. *Planning* 8. *Support* 9. *Operation* 10. *Performance evaluation* 11. *Improvement*	6 Domain: 1. *Governance and Management Objective (GMO)* 2. *Evaluate, Direct, and Monitor (EDM)* 3. *Align, Plan and Organize (APO)* 4. *Build, Acquire, and Implement (BAI)* 5. *Deliver, Service, and Support (DSS)* 6. *Monitor, Evaluate, and Assess (MEA)*	ISO 21001 dan ISO 27001 memiliki klausul yang serupa karena keduanya dikembangkan oleh ISO/IEC, namun COBIT 2019 memiliki domain yang berbeda.

Tabel 2. 2 Komparasi Berdasarkan Model Evaluasi (Lanjutan)

No	Indikator Kunci	ISO 21001	ISO 27001	COBIT 2019	Keterangan
5	*Annex* dan Proses	1. *Additional requirements for early childhood education* 2. *Principles for an EOMS* 3. *Classification of interested parties in educational organizations* 4. *Guidelines for communication with interested parties* 5. *Health and safety considerations for educational organizations*	1. *Security policy* 2. *Organization of information policy* 3. *Asset management* 4. *Human resources security* 5. *Physical and environmental security* 6. *Communications and operations management* 7. *Information security incident management* 8. *Business continuity management* 9. *Compliance*	1. *Governance Objectives: GMO1 to GMO10* 2. *Evaluate, Direct, and Monitor (EDM01 - EDM05)* 3. *Align, Plan, and Organize (APO01 - APO05)* 4. *Build, Acquire, and Implement (BAI01 - BAI05)* 5. *Deliver, Service, and Support (DSS01 - DSS05)* 6. *Monitor, Evaluate, and Assess (MEA01 - MEA05*)	Setiap model audit memiliki *annex* yang berbeda sesuai dengan fokus dan tujuan implementasinya.
6	Metodologi Implementasi	PDCA	PDCA	Tidak ada, fleksibel	ISO 21001 dan ISO 27001 menggunakan PDCA, sedangkan COBIT 2019 lebih fleksibel dalam metodologi implementasi.
7	Model Pengukuran Kapabilitas	*Gap Analysis* – Prosentase nilai	*Gap Analysis* – Prosentase nilai	*Gap Analysis* - CMMI (*Capability Maturity Model Index*); skala 0-5	ISO 21001 dan ISO 27001 menggunakan *Gap Analysis*, hasil prosentase nilai, sedangkan COBIT 2019 menggunakan CMMI skala 0-5.

Kolom bagian ISO 21001 berwarna abu-abu merupakan kunci indikator pembanding dan pencari korelasi antara ISO 27001 dan COBIT 2019, bagi kedua kolom tersebut jika terdapat kesamaan akan diberi warna abu-abu. Tabel 2.2 ditunjukkan bahwa terdapat persamaan pada komparasi tiap alat audit, seperti yang ditunjukkan pada blok warna abu-abu, dimana persamaan tersebut karena ISO 27001 dan ISO 21001 merupakan produk ISO *Family*.

Tabel 2. 3 Komparasi *Framework*

No	Fokus Permasalahan	ISO 21001	ISO 27001	COBIT 2019
1.	Pengelolaan Pendidikan	Fokus pada manajemen sistem pendidikan. Dapat berkolaborasi dengan ISO 27001 untuk evaluasi kualitas pendidikan dan keamanan sistem informasi.	Tidak fokus pada pengelolaan pendidikan, tapi dapat digunakan untuk mendukung keamanan TI dalam institusi pendidikan.	Tidak fokus pada pendidikan, namun bisa digunakan untuk evaluasi tata kelola TI secara menyeluruh di institusi pendidikan.
2.	Pengelolaan Teknologi Informasi dan Komunikasi	Tidak berfokus pada TI dan komunikasi. Fokus pada kualitas pendidikan.	Fokus pada keamanan TI, termasuk kebijakan dan kontrol terhadap sistem informasi.	Evaluasi lengkap tata kelola TI di sebuah institusi, mencakup manajemen risiko, pengelolaan sumber daya, dan kontrol TI.

Secara komparasi berdasarkan fokus bidang tabel 2.3, COBIT 2019 dapat melahap semua sisi pengelolaan SI/TI dimana saja diimplementasikan termasuk dalam ranah bidang institusi pendidikan, berbeda dengan ISO 27001 yang hanya berfokus pada keamanan informasi dan komunikasinya saja. Padahal didalam

bidang pendidikan, tingkat keberhasilan dan kualitas layanan pendidikan, tidak hanya berfokus pada keamanan informasinya saja. Menggali lebih dalam terkait *framework* yang digunakan dalam penelitian ini yaitu ISO 27001 dan COBIT 2019, dimana dikaji lingkup *expertise* permasalahan apa yang biasanya dikaji, teknikal dan detail evaluasi hingga hasil evaluasi. ISO 27001 merupakan sebuah *framework* ISF yang dapat digunakan untuk menekan manajemen resiko IT (Fathurohman & Witjaksono, 2020), mengevaluasi tingkat keamanan sistem informasi dengan menambahkan alat ukur eksternal diluar *framework*, misalnya: indeks KAMI (Soesanto, dkk., 2023; Kornelia & Irawan, 2021; Rais dkk, 2024), mengukur tingkat kematangan sebuah sistem keamanan informasi, dengan mengkombinasikan dengan ISF lain, misal: ISO 27002 sistem informasi khususnya dalam aplikasi pemerintahan (Herikson & Pamuji, 2020). Sedangkan COBIT 2019 merupakan sebuah *framework* ITG yang dapat digunakan untuk mengaudit sebuah tata kelola teknologi informasi (Sakron dkk, 2023; Widarja & 2023; Ishlahuddin dkk., 2020) baik di lingkup swasta maupun pemerintah, dengan tujuan untuk mendapat masukan perbaikan bagi tata kelola SI/TI itu sendiri dari *gap analysis* yang ada, selain itu digunakan untuk mengevaluasi standar keamanan informasi sebuah sistem atau tata kelola SI/TI (Algiffary dkk., 2023; Anam dkk., 2023; Prasetyo & Sitokdana, 2021). ITG COBIT 2019 sendiri memiliki domain yang mendukung keamanan informasi, meskipun tidak sejelas dan sedetail milik ISO *Series*, selain itu juga untuk pengukuran dan evaluasi sebuah tata kelola pelayanan di bidang SI/TI (Haay & Sitokdana, 2022; Samsinar & Sinaga, 2022), mendapatkan sejumlah rekomendasi perbaikan guna peningkatan dan mendukung strategi bisnis perusahaan (Darmawan & Wijaya, 2022).

Ketika ISF dan ITG tersebut diterapkan terkait kasus permasalahan yang telah ditentukan, seperti yang banyak dipaparkan pada paragraf awal, maka dipetakanlah proses yang berkaitan dan berelasi dengan poin yang akan dievaluasi dari organisasi oleh *auditor* (Prapenan & Pamuji, 2020). Konsep pemetaan ini penting, terlebih apabila di dalam melakukan evaluasi baik keamanan informasi atau tata kelola SI/Tinya digunakan lebih dari 1 *framework* (Rais dkk., 2024), makadari itu dibutuhkan sebuah bagan pemetaan. Jika digunakan kombinasi

framework, dalam mengatasi sebuah permasalahan evaluasi, maka konsep pemetaan tersebut juga dapat dilakukan pada level pemilihan prioritas *framework* (Serrado, 2020). Selain itu auditor atau peneliti dapat menggunakan sumber yang sudah seperti penelitian relevan, dokumentasi audit dalam menentukan domain dan proses maupun klausul pada ISF atau ITG (Andry dkk., 2019), selanjutnya juga terdapat *Goal Cascade* (Sipayung & Yunis, 2022; Martinus dkk., 2021), yakni dengan mengidentifikasi tujuan dan kebutuhan dari organisasi yang akan diaudit. *Goal cascade* sendiri merupakan standar identifikasi yangada dalam COBIT 2019. Teknik lainnya adalah dengan mengadopsi desain faktor, didalam desain faktor terdapat langkah-langkah yang menuntun auditor dalam menentukan proses yang akan dikaji (Sipayung & Yunis, 2022; Ajismanto & Surahmat,2021; Tulus & Tanaamah, 2023; Viamianni dkk, 2023).

Dalam konteks ISF ISO 27001 terdapat alat yang digunakan untuk audit keamanan informasi yaitu Indeks KAMI (Pratiwi & Wulandari, 2021), *tools* tersebut telah mengadopsi ISO 27001, dalam alat tersebut, auditor hanya tinggal memberikan jawaban yang diminta saja, dimana berfokus pada klausul yang telah ditetapkan, sehingga *auditor* tidak perlu melakukan pemilihan proses dan klausul (Soesanto, dkk., 2023). Namun juga terdapat *riset* yang mengadopsi semua klausul (Alexei, 2021), dimana dalam hal ini adalah evaluasi menggunakan ISO 27001, meskipun dalam auditnya, beberapa klausul yang diadopsi, belum semua diterapkan Dalam menilai dan mengevaluasi sebuah sistem (Sofianda dkk., 2023), diperlukan justifikasi pada tahapan akhir, hal ini bertujuan untuk mendapatkan hasil dalam bentuk pemeringkatan dan perbaikan apa saja yang diperlukan untuk mencapai hasil yang lebih baik lagi, dalam audit SI/TI hal ini dinamakan pengukuran tingkat kapabilitas dan *gap analysis* (Purnama dkk., 2020), hal ini juga biasa disebut sebagai pengukuran tingkat kematangan (Nugraha & Syaidah, 2022), dimana pada COBIT 2019, nilai rentang skor kematangan dan kapabilitas level sama (Samsinar & Sinaga, 2022).

Hal tersebut digunakan ketika auditor menggunakan COBIT 2019, berbeda dengan ISO 27001, hasil akhir dari ISF tersebut hanya menunjukkan prosentase kondisi saat ini dari setiap klausul yang telah ditetapkan, sesuai dengan kondisi

organisasi atau sistem keamanan yang di evaluasi (Legowo & Juhartoyo, 2022). Baik ISF maupun ITG dapat dikombinasikan dengan sebuah teknik atau analisis lainnya, untuk mendukung atau meningkatkan hasil dari *framework* yang digunakan, contohnya adalah tambahan penggunaan analisis *Balanced Score Card* (BSC) bersamaan dengan ITG, hal ini bertujuan agar selain mendapatkan informasi tingkatan kapabilitas, rekomendasi perbaikan, namun juga sebuah analisis strategi. BSC sendiri mengacu kepada analisis SWOT untuk menentukan strategi organisasi (Pradipta & Manuputty, 2022). Dalam praktek perhitungan, tingkat kapabilitas dan rekomendasi dari adanya *gap analysis* tersebut dilakukan tiap proses (Amalia dkk., 2018). Audit perlu dilakukan juga *collecting data* ke *auditee*, target level kapabilitas yang dikejar oleh organisasi, hal inilah yang akan membuat *gap* antar target dengan kondisi saat ini.

2.2 Dasar Teori

2.2.1 Tata Kelola SI/TI

Tata kelola SI/TI (Sistem Informasi / Teknologi Informasi) merupakan optimalisasi strategi untuk mengurangi hambatan dan meningkatkan kesesuaian implementasi teknologi informasi dengan tujuan perusahaan atau organisasi (Darmawan & Wijaya, 2022). Dalam merancang dan mendesain tata kelola SI/TI dnegan baik dan tepat pada tujuan organisasi, maka akan dapat membantu organisasi agar dapat bersaing dengan kompetitornya. Semakin besar dan kompleks sebuah organisasi perusahaan, ditambah dengan semakin banyaknya SDM (sumber daya manusia) dan operasional yang dilakukan, maka diperlukan tata kelola SI/TI yang baik, terutama apabila pelayanan organisasi didasarkan pada berbasis Teknologi Informasi. Penggunaan kerangka kerja tata kelola SI/TI atau IT *Governance* (ITG) sangat diperlukan dalam hal ini. Standarisasi seperti keamanan dan manajemen informasi dapat di *benchmark* berdasarkan *framework* yang digunakan. Oleh karena itu dalam konteks tata kelola SI/TI, permasalahan yang sering ada, tidak hanya pada desain arsitektur saja, namun juga evaluasi, audit dan *assessment* (Shantika dkk., 2022). Komponen penilaian tata kelola didasarkan pada domain *framework* yang digunakan, terdiri dari tingkat maturitas dan target

maturitas (Satyareni & Mahanani, 2014). Nilai ini didapatkan dari analisis data dan pengujian hasil responden dari *stakeholders* terkait yang berperan sebagai pemangku kepentingan organisasi. Seperti yang telah dijelaskan pada bab sebelumnya, terdapat banyak ITG yangdapat digunakan sebagai acuan dasar *assessment* dan audit seperti: ITIL, ISO, COBIT, COSO dan sebagainya.

Untuk justifikasi hasil pengukuran akan digunakan *Maturity Model Level* yang terdiri dari level 0 - 5 , terdiri sebagai berikut:

1. *Level 0* = *Non Exsistent*; Situasi sebuah organisasi mengabaikan Teknologi Informasi yang diadopsinya.
2. *Level 1* = *Initial* atau *Ad Hoc;* Situasi sebuah organisasi menerapkan Teknologi Informasi yang dibutuhkan tanpa ada perencanaan sebelumnya.
3. *Level 2* = *Repeatable But Intuitive*; Situasi sebuah organisasi secara berkelanjutan namun tidak konsisten telah menerapkan tata kelola SI/TI, tidak terdefinisi secara jelas dan terdokumentasi.
4. *Level 3* = *Defined Process*; Situasi sebuah organisasi telah melakukan sosialisasi kepada semua level manajemen organisasi terkait layanan tata kelola SI/TI, namun dalam prakteknya tidak terdapat *supervise* dalam menerapkan regulasi sosialisasi tersebut
5. *Level 4* = *Managed and Measurable*; Situasi sebuah organisasi memiliki indikator yang telah dirancang secara kuantitatif untuk melakukan *benchmark* tata kelola SI/TI, disertai fasilitas untuk melakukan *monitoring* dan evaluasi prosedur yang sedang berjalan.
6. *Level 5* = *Optimized;* Situasi sebuah organisasi secara aktif melakukan implementasi layanan tata kelola SI/TI secara baik, berkesinambungan dan memantau evaluasi dengan baik.

Model ini membantu organisasi mengidentifikasi posisi mereka pada skala kematangan tata kelola Sistem Informasi dan Teknologi Informasi (SI/TI). Dengan menggunakan enam level kematangan. Hasil evaluasi menjadi acuan strategis bagi organisasi untuk merencanakan perbaikan berkelanjutan, memastikan pengelolaan SI/TI yang lebih efektif dan relevan dengan kebutuhan organisasi.

2.2.2 Audit Sistem Informasi

Audit Sistem Informasi merupakan sebuah kegiatan *assessment* dan evaluasi layanan, infrastruktur dan fasilitas tata kelola Teknologi Informasi, untuk mengetahui seberapa efektif, efiesien dan optimal sebuah sistem yang sedang berjalan dapat menjamin keberdaya gunaannya dalam mencapai tujuan organisasi (Amirudin dkk., 2023). Auditor yang menjalankan proses serangkaian audit pada dasarkan akan menggunakan kerangka kerja untuk memastikan proses auditing menggunakan indikator-indikator yang terstandarisasi. Dalam praktek, indikator-indikator pada sistem yang diaudit mengacu kepada kerangka kerja yang diadopsi, memiliki banyak proses, seperti: proses manajemen resiko, manajemen strategi, manajemen keamanan informasi, manajemen *asset*, manajemen operasi, pengadaan asuransi tata kelola dan sebagainya. Dari banyak proses dan domain yang ada dalam sebuah kerangka kerja, auditor atau peneliti haruslah memahami latar belakang organisasi untuk memastikan dan memilih proses dari domain-domain yang sesuai. Pemilihan domain ini akan berkaitan dengan topik permasalahan pada audit sistem informasi yang dilakukan, misal: audit sumber daya TI, dalam proses ini, auditor melakukan *assessment* sumber daya TI, seperti: perangkat keras, perangkat lunak dan infrastruktur.

2.2.3 COBIT 2019

COBIT *(Control Objective for Information and related technology)* merupakan sebuah kerangka kerja yang ditujukan untuk *assessment* tata kelola SI/TI baik untuk perusahaan maupun organisasi (Zuraidah & Sulthon, 2022). COBIT sebagai standarisasi tata kelola SI/TI diterbitkan oleh *IT Governance Institute* (ITGI), merupakan bagian dari ISACA, suatu organisasi profesi internasional pada bidang Teknologi Informasi yang berbasis di Amerika (Susanto, 2018). COBIT pertama kali diperkenalkan pada tahun 1996 dengan versi 1 yang sangat menekankan pada bidang audit. Selanjutnya, versi COBIT 2 diluncurkan pada tahun 1998 dengan penekanan pada tahap kontrol. Pada tahun 2003, COBIT 3 diperkenalkan yang lebih berorientasi kepada aspek manajemen. Tahun 2005 melihat kelahiran COBIT 4 yang berfokus pada tata kelola TI. Pada tahun 2007,

COBIT mengalami *upgrade* menjadi versi 4.1 dengan perbedaan utama yaitu penekanan pada nilai dan risiko TI. Selanjutnya, pada tahun 2012, muncul COBIT versi 5 yang secara jelas memisahkan fokus antara tata kelola dan manajemen TI. Terakhir, pada tahun 2018, diluncurkan COBIT 2019, sebuah pembaruan yang memperkenalkan faktor desain yang lebih kuat dan menitik beratkan pada area yang lebih praktis dan lebih dapat disesuaikan sesuai kebutuhan spesifik. Domain dan proses yang ada pada COBIT 2019 ditunjukkan pada tabel 2.4 (Oktarina, 2022).

Tabel 2.4 Acuan domain dan penjelasan pada *framework* COBIT 2019

No	Domain	Penjelasan
EDM - *Evaluate, Direct, and Monitor* (Evaluasi, Mengarahkan, dan Memantau)		
1	EDM01	Memastikan Penyusunan dan Pemeliharaan Kerangka Tata Kelola
2	EDM02	Memastikan Pengantaran Manfaat
3	EDM03	Memastikan Optimisasi Risiko
4	EDM04	Memastikan Optimisasi Sumber Daya
5	EDM05	Memastikan Transparansi Pemangku Kepentingan
APO - *Align, Plan, and Organize* (Menyelaraskan, Merencanakan, dan Mengorganisir)		
6	APO01	Mengelola Kerangka Kerja Manajemen TI
7	APO02	Mengelola Strategi
8	APO03	Mengelola Arsitektur Perusahaan
9	APO04	Mengelola Inovasi
10	APO05	Mengelola Portofolio
11	APO06	Mengelola Anggaran dan Biaya
12	APO07	Mengelola Sumber Daya Manusia
13	APO08	Mengelola Kualitas
14	APO09	Mengelola Risiko
15	APO10	Mengelola Proyek
16	APO11	Mengelola Kontrak dan Pemasok
17	APO12	Mengelola Hubungan Pemangku Kepentingan
18	APO13	Mengelola Keamanan

Tabel 2.4 Acuan domain dan penjelasan pada *framework* COBIT 2019 (Lanjutan)

Tabel 2.4 Acuan domain dan penjelasan pada *framework* COBIT 2019 (Lanjutan)

No	Domain	Penjelasan
BAI - *Build, Acquire, and Implement* (Membangun, Memperoleh, dan Melaksanakan)		
20	BAI01	Mengelola Program dan Proyek
21	BAI02	Mengelola Definisi Persyaratan
22	BAI03	Mengelola Identifikasi dan Pembangunan Solusi
23	BAI04	Mengelola Ketersediaan dan Kapasitas
MEA - *Monitor, Evaluate, and Assess* (Memantau, Menilai, dan Menilai)		
24	BAI05	Mengelola Pemberdayaan Perubahan Organisasi
25	BAI06	Mengelola Perubahan
26	BAI07	Mengelola Penerimaan Perubahan dan Transisi
27	BAI08	Mengelola Pengetahuan
28	BAI09	Mengelola Aset
29	BAI10	Mengelola Konfigurasi
30	BAI11	Mengelola Data
DSS - Deliver, Service, and Support (Mengantarkan, Memberikan Layanan, dan Mendukung)		
31	DSS01	Mengelola Operasi
32	DSS02	Mengelola Permintaan Layanan dan Insiden
33	DSS03	Mengelola Masalah
34	DSS04	Mengelola Kelangsungan
35	DSS05	Mengelola Layanan Keamanan
36	DSS06	Mengelola Kontrol Proses Bisnis
MEA - *Monitor, Evaluate, and Assess* (Memantau, Menilai, dan Menilai)		
37	MEA01	Memantau, Menilai, Menilai Kinerja dan Kesesuaian
38	MEA02	Memantau, Menilai, dan Menilai Sistem Pengendalian Internal
39	MEA03	Memantau, Menilai, dan Menilai Kepatuhan dengan Persyaratan Eksternal
40	MEA04	Memberikan Jaminan Tata Kelola

Tabel 2.4 menjelaskan domain dalam COBIT 2019, yaitu EDM (evaluasi dan pemantauan tata kelola TI), APO (perencanaan dan penyelarasan strategi TI), BAI (pengembangan dan implementasi solusi TI), DSS (pengantaran layanan TI), dan MEA (pemantauan serta penilaian kinerja dan kepatuhan TI). *Framework* ini membantu organisasi mengelola tata kelola TI secara efektif.

2.2.4 ISO 27001

ISO *(International The Organization for Standarization)* merupakan sebuah organisasi yang berlokasi di Jenewa, dan merupakan organisasi LSM (Lembaga Swadaya Masyarakat), organisasi ini menetapkan standarisasi yang ditujukan untuk kepentingan pemerintahaan, organisasi, bisnis dan perusahaan (Oktarina, 2022). Klausul pada ISO 27001 ini dipaparkan pada tabel 2.5

Tabel 2. 5 Acuan klausul dan namanya pada framework ISO 27001

No Klausul	Nama Klausul
5	Kebijakan keamanan informasi
6	Organisasi keamanan informasi
7	Keamanan SDM
8	Manajemen *asset*
9	Kontrol akses
10	Kriptografi
11	Keamanan fisik dan lingkungan
12	Keamanan operasi
13	Keamanan komunikasi
14	Akuisisi sistem, pengembangan dan pemeliharaan
15	Hubungan pemasok
16	Manajemen insiden keamanan informasi
17	Aspek keamanan informasi manajemen kesinambungan bisinis
18	Pemenuhan

Pada Tabel 2.5 mencakup klausul-klausul penting dalam standar keamanan informasi, mulai dari kebijakan keamanan (Klausul 5), organisasi keamanan (Klausul 6), dan keamanan SDM (Klausul 7), hingga manajemen aset (Klausul 8) dan kontrol akses (Klausul 9). Selain itu, klausa lainnya mencakup kriptografi, keamanan fisik dan lingkungan, keamanan operasi, komunikasi, serta pengembangan sistem. Aspek seperti hubungan pemasok, manajemen insiden keamanan, kesinambungan bisnis, dan kepatuhan juga diatur, menjadikan kerangka ini komprehensif untuk melindungi aset informasi organisasi.

2.2.5 ISO 21001

ISO 21001 merupakan standarisasi internasional untuk manajemen organisasi pendidikan. ISO 21001 dapat diimplementasikan pada tingkat PAUD, Pendidikan Dasar, Pendidikan Menengah dan Pendidikan Tinggi baik Vokasi maupun Nonvokasi (Maulana, 2019). Standarisasi tersebut akan berfokus bagaimana mengevaluasi dan meningkatkan standar kualitas manajemen pelayanan pendidikan. Adapun klausul-klausul yang ada dalam ISO tersebut ditunjukkan pada tabel 2.6.

Tabel 2. 6 Acuan klausul dan nama klausul pada *framework* ISO 21001

No Klausul	Nama Klausul
1	Ruang lingkup
2	Acuan normatif
3	Istilah dan definisi
4	Konteks organisasi
5	Kepemimpinan
6	Perencanaan
7	Dukungan
8	Operasi
9	Evaluasi kerja
10	Peningkatan

Tabel 2.6 menjelaskan klausa utama dalam standar manajemen yang mencakup berbagai aspek penting. Klausul 1 menetapkan ruang lingkup standar, diikuti oleh Klausul 2 yang berisi acuan normatif, serta Klausul 3 yang menjelaskan istilah dan definisi yang digunakan. Klausul 4 membahas konteks organisasi, sementara Klausul 5 menekankan pentingnya kepemimpinan dalam implementasi standar. Klausul 6 hingga Klausul 8 mencakup perencanaan, dukungan, dan operasi sebagai langkah implementasi. Selanjutnya, Klausul 9 membahas evaluasi kinerja untuk menilai efektivitas, dan Klausul 10 menyoroti upaya peningkatan berkelanjutan dalam manajemen organisasi. Struktur ini memberikan panduan komprehensif untuk memastikan keberhasilan sistem manajemen.

2.2.6 KMO *(Kayser Meyer Oikin)*

Uji KMO atau *Kaiser Meyer Oikin*, merupakan uji statistik yang digunakan untuk mengevaluasi angka kecukupan sampling sebuah variabel (Muin dkk, 2020). Dengan menggunakan uji KMO, dapat diketahui sebuah variabel dikatakan memiliki data yang cukup untuk olah data selanjutnya atau tidak. Sebuah data dikatakan lolos uji KMO jika nilainya >=0.6. Formula pada Uji KMO ditunjukkan pada formula no1.

$$\mathbf{KMO} = \frac{\sum\sum \mathbf{r_{ij}^2}}{\sum\sum \mathbf{r_{ij}^2} + \sum\sum \mathbf{u_{ij}^2}} \qquad (1)$$

Dengan:

r_{ij} = Koefisien korelasi sederhana antara pasangan variabel *i* dan *j*

q_{ij} = Koefisien korelasi parsial antara pasangan variabel *i* dan *j*

Pada formula diatas, diketahui sebuah *dataset*, maka dilakukan perhitungan korelasi sederhana $\sum\sum r^2$ dan hitung korelasi parsial $\sum\sum q^2$, misal diketahui sebuah data dan dihitung korelasi sederhana 150, dan korelasi parsial 50, maka dengan menggunakan formula 1 didapatkan hasil 0.75, data tersebut lulus uji KMO karena >0.6.

2.2.7 Realibilitas dan Validitas

Uji Reabilitas dan Validitas digunakan untuk mengukur sejauh mana kehandalan instrumentasi kuesioner yang telah dibuat. Ketika melakukan olah data, 2 alat uji ini akan dilakukan secara berpasangan untuk melihat kehandalan kuesioner. 2 uji tersebut sebenarnya memiliki tujuan yang berbeda, jika uji Reabilitas digunakan untuk melihat sejauh mana kuesioner yang dibuat dapat dihandalkan, maka uji Validitas adalah untuk melihat sejauh mana instrumen dapat mengukur faktornya (Amanda dkk, 2019). Berikut formula yang digunakan untuk uji Reabilitas (ditunjukkan pada formula no 2) dan Validitas (ditunjukkan pada formula no 3).

$$\alpha = \frac{N}{N-1} . (1 - \frac{\sum s_i^2}{s_t^2}) \qquad (2)$$

Dengan:

α = koefisien *alpha*

N = jumlah pertanyaan

s_i^2 = variansi dari setiap pertanyaan

s_t^2 = variansi total

$$r_{xy} = \frac{N \sum XY - (\sum X)(\sum Y)}{\sqrt{[N \sum X^2 - (\sum X)^2][N \sum Y^2 - (\sum Y)^2]}} \qquad (3)$$

Dengan:

r = koefisien relasi *pearson*

Xi = skor individu untuk tiap pertanyaan Y = Total skor

$\bar{X}$ = Rata – rata skor untuk tiap pertanyaan

$\bar{Y}$ = Rata – rata dari total skor

∑ = Penjumlahan untuk semua responden

Semisal diketahui jumlah data adalah 3 *record*, dan nilai variansi setiap data adalah 1.2, 1.1 dan 1.3, maka nilai totalnya adalah 3.6, sedangkan nilai variansi secara keseluruhan adalah 4.5, maka dilakukan perhitungan dengan formula 2 dengan hasil 0.3, nilai tersebut memiliki reabilitas yang rendah. Sedangkan, uji validitas mengacu kepada nilai e*stimate* setiap item > 0.30 (misalnya pada aplikasi JASP) dan nilai *p value* setiap item >0.05 maka dikatakan *valid*.

2.2.8 PLS-SEM *(Partial Least Square-Structural Equation Modelling)*

Uji PLS-SEM merupakan uji statistik yang digunakan untuk memeriksa apakah sebuah variabel mempengaruhi variabel lainnya (Abdurrahman dkk, 2022), metode ini merupakan metode yang digunakan untuk pemecahan masalah penelitian sebab akibat. Dengan menggunakan PLS-SEM, sebuah variabel atau variabel laten dapat diamati memiliki korelasi atau tidak dengan variabel laten lainnya, berdasarkan model konseptual yang dibangun. Berikut tahapan-tahapan Uji PLS-SEM:

1. Menentukan variabel laten
2. Merancang model konseptual atau *path diagram*
3. Menghitung nilai dengan formula PLS-SEM:

$$CR = \frac{(\sum \text{loading})^2}{(\sum \text{loading})^2 + \sum \text{varian error}} \qquad (4)$$

Dengan:

CR = *Composite Reliabillity*

Loading = Nilai *Loading Factor*

Misalnya diketahui, terdapat seorang peneliti sedang meneliti pengaruh kepuasan pelanggan terhadap loyalitas pelanggan, skor nilai kepuasan pelanggan adalah [0.80, 0.85, 0.78]. Dengan menggunakan formula 4, dihitung ∑loading = $0.80^2 + 0.85^2 + 0.78^2$ =2027, sedangkan ∑varian error = $(1 - 0.80^2) – (1 - 0.85^2) – (1 - 0.78^2)$ = 0.973, maka nilai *path coefficient* adalah 0.676, ini variabel kepuasan pelanggan terhadap loyalitas pelanggan.

2.2.9 Bootstrapping

Uji *Bootstraping*, adalah uji statistik yang digunakan untuk melihat apakah sebuah variabel laten memiliki nilai signifikan atau tidak, uji *Bootstrap* akan menghitung nilai p *value* atau t *statistic* dari variabel laten pada model konseptual. Berikut langkah – langkah uji Bootstraping:

1. Menggunakan data asli, dilakukan resampling dan mendapatkan data sintetis
2. Menghitung nilai *path coefficient* untuk setiap data resampling
3. Menghitung nilai *t-statistic* atau *p value* dengan formula:

$$\mathbf{t} = \frac{\bar{\beta} - \theta}{\mathbf{SE}_{\mathbf{bootstrap}}} \qquad (5)$$

Dengan:

$\bar{\beta}$ = nilai *path coefficient*

$SE_{bootstrap}$ = standar *error* dari data *bootstrap*

Semisal digunakan studi kasus pada uji PLS-SEM, diketahui nilai *path coefficient* 0.45 dan standar error hasil *bootstrapping* 0.08, maka dengan formula 5 = 5.625, karena lebih besar daripada 1.96 maka hasil tersebut signifikan.