E-ISSN : 2746-2331
P-ISSN : 2746-234X

ANALISIS KOMPONEN DAN PRINSIP INFRASTRUKTUR TEKNOLOGI INFORMASI BERBASIS STANDAR DAN FRAMEWORK INTERNASIONAL

Rahmad Rizky[1)], Muhammad Fikry[2)], Asrianda[3)]

[1,2,3)]Prodi Magister Teknologi Informasi, Universitas Malikussaleh, Indonesia
[1)]rahmadrizky2018@gmail.com
[2)]muh.fikry@unimal.ac.id
[3)]asrianda@unimal.ac.id

Abstract: Information Technology (IT) infrastructure is a fundamental element that supports organizational operations, decision-making processes, and the achievement of strategic objectives, particularly in the context of rapid digital transformation and the increasing complexity of cybersecurity risks. This study aims to analyze the main components and principles of IT infrastructure based on a synthesis of scientific literature and relevant international frameworks. The research employs a Systematic Literature Review (SLR) method by examining national and international journal articles, conference proceedings, research reports, and international standards and frameworks, including COBIT 2019, ITIL 4, ISO/IEC 27001, and the NIST Cybersecurity Framework. The findings indicate that IT infrastructure encompasses not only technical aspects such as hardware and software but also non-technical and strategic aspects, particularly IT governance and information security, which are the most frequently discussed components in the literature. These results emphasize that effective IT infrastructure management is strongly influenced by governance mechanisms, risk control, and the protection of information assets, highlighting the need for a holistic approach that integrates both technical and non-technical dimensions to ensure the reliability, security, and sustainability of IT services.

Keywords: Information Technology Infrastructure, IT Governance, Information Security, International Standards, Systematic Literature Review

Abstrak: Infrastruktur Teknologi Informasi (TI) merupakan elemen fundamental yang mendukung operasional organisasi, pengambilan keputusan, dan pencapaian tujuan strategis, seiring dengan pesatnya perkembangan teknologi digital dan meningkatnya risiko keamanan siber. Penelitian ini bertujuan untuk menganalisis komponen dan prinsip utama infrastruktur TI berdasarkan sintesis literatur ilmiah dan framework internasional yang relevan. Metode yang digunakan adalah *Systematic Literature Review* (SLR) terhadap artikel jurnal nasional dan internasional, prosiding ilmiah, laporan penelitian, serta dokumen standar dan framework internasional, dengan mengacu pada COBIT 2019, ITIL 4, ISO/IEC 27001, dan NIST *Cybersecurity Framework*. Hasil kajian menunjukkan bahwa infrastruktur TI tidak hanya

mencakup aspek teknis seperti perangkat keras dan perangkat lunak, tetapi juga aspek non-teknis yang bersifat strategis, terutama tata kelola TI dan keamanan informasi, yang menjadi komponen paling dominan dalam literatur. Temuan ini menegaskan bahwa keberhasilan pengelolaan infrastruktur TI sangat dipengaruhi oleh mekanisme tata kelola, pengendalian risiko, dan perlindungan aset informasi, sehingga diperlukan pendekatan holistik yang mengintegrasikan aspek teknis dan non-teknis untuk menjamin keandalan, keamanan, dan keberlanjutan layanan TI.

Kata kunci: Infrastruktur Teknologi Informasi, Tata Kelola TI, Keamanan Informasi, Standar Internasional, *Systematic Literature Review*

1. Pendahuluan

Infrastruktur Teknologi Informasi (TI) merupakan fondasi utama dalam mendukung operasional organisasi, pengelolaan data, serta penyediaan layanan TI yang andal. Berbagai penelitian menunjukkan bahwa kualitas dan tingkat kematangan infrastruktur TI memiliki pengaruh langsung terhadap efektivitas layanan TI dan kinerja organisasi secara keseluruhan (Fryonanda dkk., 2019; Pereira dkk., 2021).Infrastruktur TI yang dikelola dengan baik memungkinkan organisasi untuk meningkatkan efisiensi operasional, keandalan sistem, serta kualitas pengambilan keputusan berbasis informasi.

Seiring dengan meningkatnya ketergantungan organisasi terhadap sistem digital, pengelolaan infrastruktur TI menjadi semakin kompleks dan berisiko. Kompleksitas tersebut tidak hanya berasal dari aspek teknis, tetapi juga dipengaruhi oleh lemahnya mekanisme tata kelola, manajemen layanan, dan pengendalian risiko. Kondisi ini berpotensi menyebabkan gangguan layanan, inefisiensi operasional, serta meningkatnya kerentanan terhadap ancaman keamanan informasi (Purwanto & Mardjono, 2021; Santoso, 2025; Sigit Julianto dkk., 2024).

Tata kelola TI dipandang sebagai elemen kunci dalam memastikan keselarasan antara infrastruktur TI dan tujuan strategis organisasi. Dalam literatur, *framework* COBIT banyak digunakan sebagai acuan tata kelola dan manajemen TI karena kemampuannya dalam mendukung penciptaan nilai, pengelolaan risiko, serta optimalisasi sumber daya TI (ISACA, 2019; Pereira dkk., 2021; Purnama & Akbar, 2025).Penggunaan COBIT dalam berbagai

penelitian menunjukkan bahwa tata kelola TI menjadi fondasi penting dalam pengelolaan infrastruktur TI yang efektif dan terkontrol.

Selain tata kelola TI, manajemen layanan TI juga memiliki peran penting dalam menjaga stabilitas dan keberlanjutan infrastruktur TI. Framework ITIL digunakan secara luas sebagai acuan dalam pengelolaan layanan TI dengan menempatkan infrastruktur sebagai pendukung utama siklus hidup layanan. ITIL menekankan penciptaan nilai, peningkatan kualitas layanan, serta efisiensi operasional melalui pengelolaan proses layanan yang terstruktur (Axelos, 2019; Budiman & Lubis, 2025; Zulkarnain dkk., 2024).

Keamanan informasi merupakan aspek yang semakin dominan dalam pengelolaan infrastruktur TI modern. Standar ISO/IEC 27001 dan NIST Cybersecurity Framework banyak digunakan untuk mengelola risiko keamanan siber dan melindungi aset informasi organisasi, khususnya pada sistem dan jaringan yang bersifat kritis (ISO/IEC, 2022; NIST, 2020; Rahman dkk., 2024). Sejumlah penelitian juga menyoroti pentingnya evaluasi dan audit keamanan informasi berbasis framework tersebut guna meningkatkan ketahanan infrastruktur TI terhadap ancaman siber (Fadila dkk., 2023; Sulistyowati dkk., 2020).

Literatur menunjukkan bahwa tidak terdapat satu framework tunggal yang mampu mencakup seluruh aspek pengelolaan infrastruktur TI secara menyeluruh. Oleh karena itu, pendekatan integratif yang mengombinasikan framework tata kelola, manajemen layanan, dan standar keamanan informasi semakin banyak diadopsi untuk memperoleh pengelolaan infrastruktur TI yang holistik dan berkelanjutan (Almeida & Da Silva, 2021; Lokare dkk., 2022; Pereira dkk., 2021).

Meskipun berbagai penelitian telah membahas infrastruktur TI dari sudut pandang yang beragam, kajian yang secara sistematis memetakan komponen dan prinsip infrastruktur TI berdasarkan sintesis berbagai standar dan framework internasional masih relatif terbatas (Rochmania dkk., 2020; Sudanawati Rozas dkk., 2020). Oleh karena itu, penelitian ini bertujuan untuk menganalisis komponen dan prinsip utama infrastruktur Teknologi Informasi melalui pendekatan *Systematic Literature Review* guna menghasilkan

pemetaan konseptual yang komprehensif dan terintegrasi. Penelitian ini memberikan kontribusi dengan menyajikan pemetaan sistematis kajian infrastruktur TI berdasarkan framework dan standar internasional, seperti COBIT, ITIL, ISO/IEC 27001, dan NIST *Cybersecurity Framework*, serta mengidentifikasi *framework* dominan dan komponen infrastruktur TI yang menjadi fokus utama dalam literatur.

2. Kajian Kepustakaan

2.1 Infrastruktur Teknologi Informasi

Infrastruktur Teknologi Informasi didefinisikan sebagai sekumpulan sumber daya teknologi yang digunakan untuk mendukung pemrosesan, penyimpanan, dan distribusi informasi dalam organisasi. Infrastruktur TI mencakup komponen teknis seperti perangkat keras, perangkat lunak, jaringan, serta sistem pendukung yang memungkinkan layanan TI berjalan secara efektif. Sejumlah penelitian menunjukkan bahwa infrastruktur TI berperan sebagai fondasi utama dalam penyediaan layanan TI dan stabilitas operasional organisasi (Fryonanda dkk., 2019; Pereira dkk., 2021).

Dalam konteks organisasi modern, infrastruktur TI tidak lagi dipandang hanya sebagai aset teknis, tetapi sebagai bagian strategis yang berkontribusi terhadap penciptaan nilai dan peningkatan kinerja organisasi. (Pereira dkk., 2021) menegaskan bahwa pengelolaan infrastruktur TI harus dilakukan secara terstruktur dan terintegrasi dengan mekanisme tata kelola yang jelas. Hal ini sejalan dengan temuan (Sudanawati Rozas dkk., 2020) yang menunjukkan bahwa pemanfaatan *framework* internasional menjadi tren utama dalam pengelolaan infrastruktur TI di berbagai sektor.

Seiring dengan meningkatnya kompleksitas sistem dan layanan digital, infrastruktur TI juga semakin rentan terhadap gangguan dan risiko operasional. Oleh karena itu, pengelolaan infrastruktur TI tidak hanya menuntut keandalan teknis, tetapi juga pendekatan manajerial dan kebijakan yang mampu mengendalikan risiko serta menjamin keberlanjutan layanan TI (Purwanto & Mardjono, 2021; Santoso, 2025).

2.2 Tata Kelola Infrastruktur Teknologi Informasi

Tata kelola Teknologi Informasi merupakan kerangka kerja yang digunakan untuk memastikan bahwa pemanfaatan TI selaras dengan tujuan strategis organisasi, memberikan nilai, serta mengendalikan risiko. Dalam literatur, tata kelola TI sering dikaitkan dengan mekanisme pengambilan keputusan, akuntabilitas, dan pengendalian yang mengatur pengelolaan sumber daya TI, termasuk infrastruktur TI (ISACA, 2019; Pereira dkk., 2021).

Framework COBIT banyak digunakan sebagai acuan utama dalam tata kelola dan manajemen TI. COBIT 5 dan COBIT 2019 dirancang untuk membantu organisasi dalam mengelola TI secara end-to-end, dengan penekanan pada penciptaan nilai, optimalisasi risiko, dan pemanfaatan sumber daya yang efektif (ISACA, 2019; Purnama & Akbar, 2025). Sejumlah penelitian empiris menunjukkan bahwa penerapan COBIT berkontribusi terhadap peningkatan kematangan tata kelola infrastruktur TI, baik pada sektor publik maupun sektor bisnis (Christiadi & Sutomo, 2023; Purwanto & Mardjono, 2021).

Selain itu, tata kelola infrastruktur TI juga berkaitan erat dengan evaluasi dan pengukuran kapabilitas pengelolaan TI. Penelitian-penelitian di Indonesia menunjukkan bahwa pengukuran kapabilitas tata kelola TI berbasis COBIT 2019 banyak digunakan untuk menilai kesiapan organisasi dalam mengelola risiko dan keamanan infrastruktur TI. Temuan-temuan tersebut menunjukkan bahwa tata kelola TI merupakan komponen dominan dalam kajian infrastruktur TI dan menjadi faktor kunci keberhasilan pengelolaannya.

2.3 Manajemen Layanan TI dan ITIL 4

Manajemen layanan Teknologi Informasi merupakan pendekatan yang berfokus pada penyediaan layanan TI yang bernilai bagi organisasi dan pemangku kepentingan. Dalam konteks infrastruktur TI, manajemen layanan berperan dalam memastikan bahwa infrastruktur mampu mendukung siklus hidup layanan TI secara konsisten dan berkelanjutan. ITIL digunakan secara luas sebagai *framework* manajemen layanan TI yang menyediakan praktik terbaik dalam pengelolaan layanan berbasis nilai (Axelos, 2019).

ITIL 4 memperkenalkan konsep *Service Value System* yang menempatkan infrastruktur TI sebagai *enabler* utama dalam penciptaan nilai layanan. *Framework* ini menekankan integrasi antara proses, teknologi, dan sumber daya manusia dalam mendukung layanan TI yang adaptif terhadap perubahan kebutuhan organisasi (Axelos, 2019; Budiman & Lubis, 2025).Sejumlah penelitian menunjukkan bahwa penerapan ITIL berkontribusi terhadap peningkatan kualitas layanan TI dan stabilitas infrastruktur pendukungnya (Fryonanda dkk., 2019; Zulkarnain dkk., 2024).

Lebih lanjut, literatur menunjukkan bahwa integrasi ITIL dengan *framework* tata kelola seperti COBIT mampu memperkuat pengelolaan infrastruktur TI secara holistik. Kombinasi COBIT dan ITIL membantu organisasi menghubungkan aspek strategis tata kelola dengan praktik operasional manajemen layanan. Temuan ini menunjukkan bahwa manajemen layanan TI merupakan komponen penting yang melengkapi tata kelola infrastruktur TI.

2.4 Keamanan Informasi dalam Infrastruktur TI

Keamanan informasi merupakan salah satu komponen krusial dalam infrastruktur TI modern. Infrastruktur TI yang tidak dilengkapi dengan mekanisme keamanan yang memadai berpotensi menimbulkan risiko kebocoran data, gangguan layanan, dan kerugian organisasi. Oleh karena itu, berbagai standar dan framework internasional dikembangkan untuk membantu organisasi dalam mengelola risiko keamanan informasi (ISO/IEC, 2022; NIST, 2020).

ISO/IEC 27001 merupakan standar sistem manajemen keamanan informasi yang banyak digunakan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi. Standar ini memberikan kerangka kerja pengendalian keamanan yang terstruktur dan dapat diintegrasikan dengan tata kelola infrastruktur TI organisasi (ISO/IEC, 2022). Selain itu, NIST *Cybersecurity Framework* digunakan secara luas untuk mengelola risiko keamanan siber, khususnya pada infrastruktur kritis dan sistem jaringan (NIST, 2020; Rahman dkk., 2024).

Sejumlah penelitian menunjukkan bahwa evaluasi dan audit keamanan infrastruktur TI sering dilakukan dengan mengombinasikan berbagai framework keamanan, seperti NIST CSF, CIS Controls, dan COBIT 2019. Pendekatan ini digunakan untuk memperoleh gambaran yang lebih komprehensif mengenai kesiapan keamanan organisasi (Fadila dkk., 2023; Sulistyowati dkk., 2020). Selain aspek teknis, (Alshaikh, 2020)menegaskan bahwa budaya keamanan siber dan kesadaran organisasi juga berperan penting dalam meningkatkan efektivitas keamanan infrastruktur TI.

2.5 Sintesis Framework dan Standar Internasional

Literatur menunjukkan bahwa tidak terdapat satu *framework* atau standar tunggal yang mampu mencakup seluruh aspek pengelolaan infrastruktur TI. Masing-masing framework memiliki fokus dan kekuatan yang berbeda, seperti COBIT pada tata kelola, ITIL pada manajemen layanan, serta ISO/IEC 27001 dan NIST CSF pada keamanan informasi (Axelos, 2019; ISACA, 2019; ISO/IEC, 2022; NIST, 2020).

Beberapa studi menekankan pentingnya pendekatan integratif dalam pengelolaan infrastruktur TI. (Almeida & Da Silva, 2021)dalam studi literatur sistematisnya menunjukkan bahwa integrasi framework tata kelola, manajemen layanan, dan keamanan informasi mampu meningkatkan efektivitas pengelolaan TI secara keseluruhan. Hal ini diperkuat oleh (Pereira dkk., 2021)yang menyatakan bahwa tata kelola infrastruktur TI yang efektif memerlukan kombinasi berbagai framework agar mampu menjawab kompleksitas lingkungan TI modern.

Selain itu, penelitian-penelitian terbaru menunjukkan adanya tren peningkatan integrasi framework keamanan siber dan tata kelola TI untuk menghadapi ancaman adaptif. (Lokare dkk., 2022) dan (Mehedi Rahman dkk., t.t.) menunjukkan bahwa pendekatan multi-framework digunakan untuk mengelola risiko dan meningkatkan ketahanan infrastruktur TI. Sintesis berbagai framework dan standar internasional ini menjadi landasan konseptual penting dalam penelitian untuk menganalisis komponen dan prinsip infrastruktur TI secara komprehensif.

3. Metode Penelitian

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode *Systematic Literature Review* (SLR). Metode SLR dipilih karena memungkinkan peneliti untuk mengkaji, mengidentifikasi, dan mensintesis hasil penelitian terdahulu secara sistematis dan terstruktur, khususnya terkait infrastruktur Teknologi Informasi (TI) berbasis framework dan standar internasional. Pendekatan ini sesuai untuk memperoleh gambaran komprehensif mengenai fokus penelitian, kecenderungan penggunaan framework, serta komponen infrastruktur TI yang dominan dalam literatur (Almeida & Da Silva, 2021; Pereira dkk., 2021).

Jenis penelitian yang digunakan bersifat deskriptif-analitis, yaitu penelitian yang bertujuan untuk mendeskripsikan dan menganalisis konsep, prinsip, serta komponen infrastruktur TI sebagaimana dibahas dalam literatur ilmiah. Penelitian ini tidak melibatkan pengumpulan data primer, melainkan memanfaatkan data sekunder yang bersumber dari publikasi ilmiah dan dokumen standar internasional.

Pendekatan SLR dalam penelitian ini digunakan untuk mengintegrasikan berbagai perspektif terkait infrastruktur TI, yang meliputi tata kelola TI, manajemen layanan TI, dan keamanan informasi. Dengan demikian, metode penelitian yang digunakan selaras dengan tujuan penelitian, yaitu menganalisis komponen dan prinsip infrastruktur TI secara holistik berbasis standar internasional.

3.2 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini dibatasi pada kajian infrastruktur Teknologi Informasi dalam konteks pengelolaan organisasi, dengan fokus pada penggunaan framework dan standar internasional. *Framework* dan standar yang menjadi perhatian utama dalam penelitian ini meliputi COBIT (COBIT 5 dan COBIT 2019), ITIL (ITIL V3 dan ITIL 4), ISO/IEC 27001, dan NIST Cybersecurity Framework.

Penelitian ini tidak membahas implementasi teknis secara mendalam pada organisasi tertentu, melainkan menitikberatkan pada analisis konseptual dan sintesis literatur. Fokus utama diarahkan pada identifikasi komponen

infrastruktur TI, peran *framework* internasional, serta kecenderungan topik yang dominan dibahas dalam penelitian sebelumnya.

Dengan pembatasan ruang lingkup tersebut, penelitian ini diharapkan mampu memberikan gambaran yang terfokus namun komprehensif mengenai pengelolaan infrastruktur TI berbasis standar internasional.

3.3 Teknik Analisis Data

Analisis data dalam penelitian ini dilakukan menggunakan analisis tematik dan komparatif. Analisis tematik digunakan untuk mengelompokkan literatur berdasarkan tema utama, seperti infrastruktur TI, tata kelola TI, manajemen layanan TI, dan keamanan informasi. Setiap literatur dianalisis untuk mengidentifikasi fokus penelitian, framework atau standar yang digunakan, serta komponen infrastruktur TI yang dibahas.

Selanjutnya, analisis komparatif dilakukan untuk membandingkan pendekatan antar framework dan standar internasional dalam mengelola infrastruktur TI. Analisis ini bertujuan untuk mengidentifikasi kesamaan, perbedaan, serta kecenderungan penggunaan framework dalam literatur.

Hasil analisis tematik dan komparatif ini kemudian disintesis untuk menghasilkan pemetaan literatur, grafik distribusi *framework*, serta identifikasi komponen infrastruktur TI yang dominan, yang menjadi dasar dalam pembahasan hasil penelitian.

4. Metode Pengumpulan Data

4.1 Sumber Data Penelitian

Sumber data dalam penelitian ini berasal dari data sekunder, yaitu publikasi ilmiah dan dokumen standar internasional yang relevan dengan topik infrastruktur Teknologi Informasi. Data dikumpulkan dari artikel jurnal nasional dan internasional, prosiding ilmiah, report penelitian, serta buku dan dokumen resmi *framework* atau standar internasional.

Dokumen standar dan framework internasional yang digunakan dalam penelitian ini meliputi COBIT 2019, ITIL 4, ISO/IEC 27001, dan NIST *Cybersecurity Framework*, yang secara luas diakui dan digunakan dalam pengelolaan infrastruktur TI. Selain itu, penelitian ini juga memanfaatkan artikel ilmiah yang membahas evaluasi, audit, integrasi, serta perbandingan

framework tersebut dalam konteks infrastruktur TI. Penggunaan berbagai jenis sumber data ini bertujuan untuk memperoleh pandangan yang komprehensif dan representatif terhadap perkembangan kajian infrastruktur TI.

4.2 Teknik Penelusuran Literatur

Penelusuran literatur dilakukan secara sistematis dengan menggunakan kata kunci yang relevan dengan topik penelitian. Kata kunci yang digunakan antara lain IT infrastructure, IT governance, IT service management, information security, COBIT, ITIL, ISO/IEC 27001, dan NIST Cybersecurity Framework. Kata kunci tersebut digunakan untuk menelusuri publikasi ilmiah pada jurnal nasional dan internasional serta repositori publikasi yang kredibel.

Literatur yang diperoleh dari proses penelusuran kemudian dikompilasi dan dikelola menggunakan perangkat lunak manajemen referensi untuk memastikan konsistensi sitasi dan menghindari duplikasi referensi. Tahap ini juga memudahkan proses penyaringan literatur berdasarkan relevansi dan fokus kajian.

Penelusuran literatur dilakukan secara iteratif, yaitu dengan menyesuaikan kata kunci dan sumber pencarian hingga diperoleh literatur yang sesuai dengan ruang lingkup penelitian.

4.3 Kriteria Inklusi dan Eksklusi

Untuk menjaga kualitas dan relevansi data, penelitian ini menerapkan kriteria inklusi dan eksklusi dalam proses pengumpulan data. Kriteria inklusi meliputi:

a. literatur yang membahas infrastruktur TI atau komponennya
b. literatur yang menggunakan atau membahas framework dan standar internasional
c. literatur yang memiliki fokus kajian yang jelas dan relevan, dan
d. literatur yang dipublikasikan pada sumber yang kredibel.

Sementara itu, kriteria eksklusi meliputi:

a. publikasi yang tidak berkaitan dengan infrastruktur TI
b. artikel yang tidak memiliki kejelasan metodologi atau fokus penelitian, dan
c. literatur yang bersifat opini tanpa dasar akademik yang memadai.

Berdasarkan kriteria tersebut, literatur yang terpilih selanjutnya digunakan sebagai data utama dalam analisis dan pemetaan literatur.

4.4 Hasil Pengumpulan Data

Hasil dari proses penelusuran dan seleksi literatur menghasilkan sekumpulan artikel ilmiah dan dokumen standar internasional yang relevan dengan fokus penelitian. Literatur terpilih kemudian dipetakan berdasarkan fokus penelitian, framework atau standar yang digunakan, serta komponen infrastruktur TI yang dibahas.

Hasil pengumpulan data ini menjadi dasar dalam penyusunan tabel pemetaan literatur dan analisis lanjutan pada bab hasil dan pembahasan. Dengan proses pengumpulan data yang sistematis dan terstruktur, penelitian ini diharapkan memiliki tingkat transparansi dan replikasi yang baik.

5. Hasil dan Pembahasan

5.1 Hasil Pemetaan Literatur Infrastruktur Teknologi Informasi

Bab ini menyajikan hasil pemetaan literatur yang diperoleh dari proses *Systematic Literature Review* terhadap 22 publikasi ilmiah yang relevan dengan topik infrastruktur Teknologi Informasi. Pemetaan dilakukan untuk mengidentifikasi fokus penelitian, framework atau standar yang digunakan, serta komponen infrastruktur TI yang dibahas dalam masing-masing literatur. Hasil pemetaan ini menjadi dasar utama dalam analisis distribusi framework dan komponen infrastruktur TI pada subbab selanjutnya.

Tabel 5.1 Pemetaan Literatur Infrastruktur Teknologi Informasi

No	Penulis & Tahun	Jenis Publikasi	Fokus Penelitian	Framework / Standar	Komponen Infrastruktur TI
1	Lokare et al., 2022	Report / Paper	Integrasi framework keamanan siber untuk mitigasi ancaman adaptif	NIST CSF, ISO/IEC 27001, Zero Trust	Keamanan jaringan, sistem deteksi ancaman, data, kontrol akses
2	Rahman et al., 2022	Report / Paper	Metodologi praktis penilaian risiko TI dan	NIST SP 800-30,	Aset TI, risiko, kerentanan, CIA (Confidentiality,

No	Penulis & Tahun	Jenis Publikasi	Fokus Penelitian	Framework / Standar	Komponen Infrastruktur TI
			siber (AssessITS)	COBIT 5, ISO 31000	Integrity, Availability)
3	Sulistyowati et al., 2020	Report / Paper	Perancangan metode penilaian kematangan keamanan siber	NIST CSF, ISO/IEC 27002, COBIT, PCI DSS	Sistem keamanan informasi, tata kelola TI, kontrol keamanan
4	Zulkarnain et al., 2024	Jurnal	Integrasi COBIT 5 dan ITIL V3 untuk peningkatan tata kelola TI dan kesuksesan proyek	COBIT 5, ITIL V3	Layanan TI, manajemen insiden, risiko TI, infrastruktur pendukung
5	Purwanto & Mardjono, 2021	Jurnal	Audit tata kelola TI pada instansi pemerintah	COBIT 5	Infrastruktur TI, pengelolaan data, sistem informasi sektor publik
6	Christiadi & Sutomo, 2023	Jurnal	Pengukuran kapabilitas tata kelola keamanan TI sektor bisnis	COBIT 2019 (APO12, APO13, DSS05)	Endpoint security, kontrol akses, event log, keamanan layanan
7	Purnama & Akbar, 2025	Jurnal	Analisis perbandingan COBIT 5 dan COBIT 2019	COBIT 5, COBIT 2019	Infrastruktur TI organisasi, tata kelola dan manajemen TI

E-ISSN : 2746-2331
P-ISSN : 2746-234X

No	Penulis & Tahun	Jenis Publikasi	Fokus Penelitian	Framework / Standar	Komponen Infrastruktur TI
8	Fadila et al., 2023	Jurnal	Audit keamanan siber pada organisasi	CIS CSC, NIST CSF, COBIT 2019	Keamanan jaringan, kontrol keamanan, sistem informasi
9	Rahman et al., 2024	Report / Paper	Perbandingan framework keamanan jaringan	NIST CSF, CIS Controls, ISO/IEC 27001	Jaringan, sistem keamanan, manajemen risiko
10	Julianto et al., 2024	Report / Paper	Manajemen risiko siber pada instansi pemerintah	NIST CSF, COBIT 2019	Infrastruktur TI instansi, manajemen risiko, keamanan data
11	Fryonanda et al., 2019	Report / Paper	Evaluasi infrastruktur TI dan kepuasan pengguna	COBIT 5, ITIL V3	Infrastruktur TI, layanan TI, sistem informasi
12	Rozas & Rochmania, 2020	Jurnal	Statistik dan tren penggunaan framework TI di Indonesia	COBIT, ITIL, ISO/IEC 27001	Infrastruktur TI organisasi (umum)
13	Santoso, 2025	Jurnal	Evaluasi kematangan tata kelola TI sektor transportasi	COBIT 2019, ISO 31000, ITSM	Infrastruktur TI, layanan TI, cloud, manajemen risiko

No	Penulis & Tahun	Jenis Publikasi	Fokus Penelitian	Framework / Standar	Komponen Infrastruktur TI
14	Rochmania et al., 2020	Jurnal	Tren penggunaan framework TI Indonesia dan internasional	COBIT, ITIL, ISO/IEC 27001	Infrastruktur TI organisasi
15	Budiman & Lubis, 2025	Jurnal	Perbandingan COBIT 2019 dan ITIL 4	COBIT 2019, ITIL 4	Tata kelola TI, manajemen layanan TI
16	Pereira et al., 2021	Jurnal	Systematic Literature Review tata kelola infrastruktur TI	IT Governance Frameworks	Infrastruktur TI enterprise
17	Alshaikh, 2020	Jurnal	Budaya keamanan siber dan perilaku karyawan	Cybersecurity Governance	People, process, technology
18	Almeida & Da Silva, 2021	Jurnal	Governance and management of IT (SLR)	COBIT, ITIL, ISO	Infrastruktur TI dan tata kelola
19	NIST, 2020	Standar	Peningkatan keamanan infrastruktur kritis	NIST CSF 1.1	Infrastruktur kritis, jaringan, sistem TI
20	ISO/IEC, 2022	Standar	Sistem manajemen keamanan informasi	ISO/IEC 27001:2022	Sistem keamanan informasi, data, kontrol akses

E-ISSN : 2746-2331
P-ISSN : 2746-234X

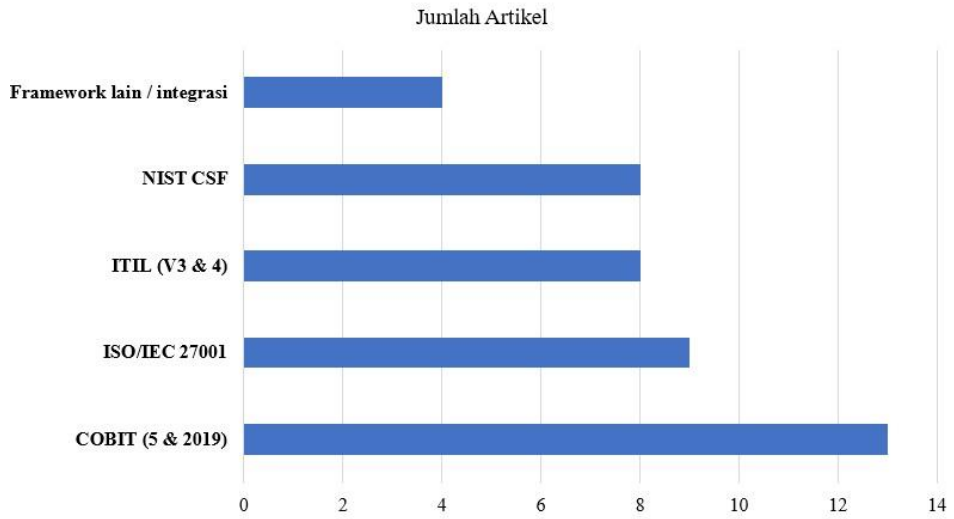
No	Penulis & Tahun	Jenis Publikasi	Fokus Penelitian	Framework / Standar	Komponen Infrastruktur TI
21	ISACA, 2019	Buku / Framework	Tata kelola dan manajemen TI enterprise	COBIT 2019	Infrastruktur TI, governance, risk & compliance
22	Axelos, 2019	Buku / Framework	Manajemen layanan TI modern	ITIL 4	Infrastruktur layanan TI, operasional TI

Tabel 5.1 menyajikan ringkasan literatur yang dianalisis berdasarkan fokus penelitian, framework atau standar yang digunakan, serta komponen infrastruktur TI yang menjadi perhatian utama. Tabel ini menunjukkan bahwa sebagian besar penelitian tidak hanya membahas aspek teknis infrastruktur TI, tetapi juga menekankan aspek tata kelola, manajemen layanan, dan keamanan informasi.

Berdasarkan Tabel 5.1, terlihat bahwa *framework* seperti COBIT, ITIL, ISO/IEC 27001, dan NIST *Cybersecurity Framework* paling sering digunakan dalam kajian infrastruktur TI. Hal ini mengindikasikan bahwa pendekatan pengelolaan infrastruktur TI dalam literatur cenderung mengadopsi *framework* yang berorientasi pada tata kelola, layanan, dan pengendalian risiko, bukan sekadar pengelolaan teknis perangkat keras dan perangkat lunak.

5.2 Analisis Framework dan Standar Internasional yang Digunakan

Setelah dilakukan pemetaan literatur, tahap selanjutnya adalah menganalisis distribusi framework dan standar yang digunakan dalam penelitian terkait infrastruktur TI. Analisis ini bertujuan untuk mengetahui framework yang paling dominan serta kecenderungan penggunaan framework dalam literatur.



Gambar 5.1 Distribusi Framework dalam Literatur Infrastruktur TI

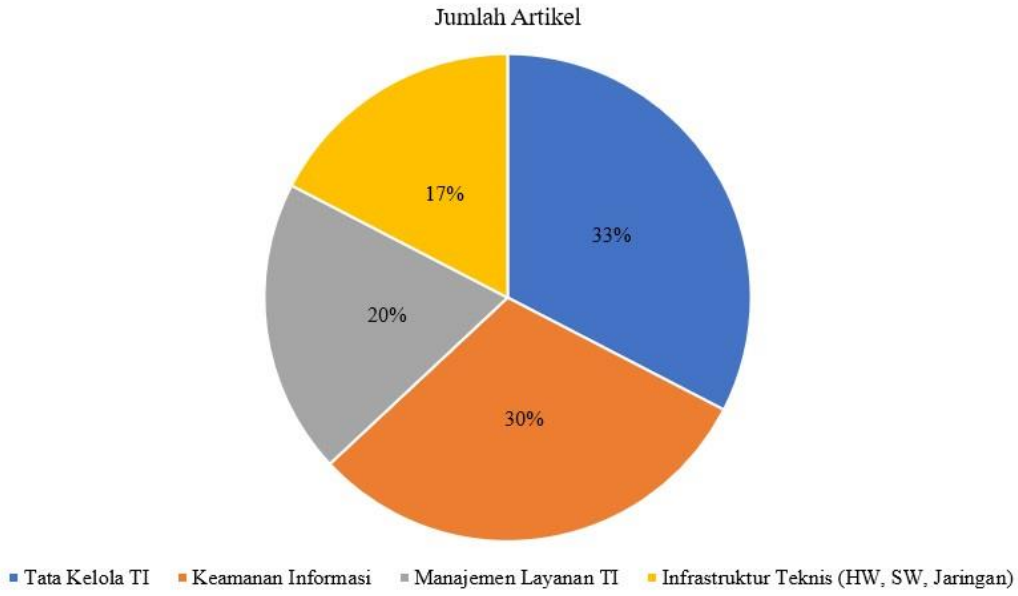
Gambar 5.1 menunjukkan distribusi penggunaan *framework* dan standar dalam 22 literatur yang dianalisis. Data pada grafik diperoleh dari hasil pengkodean literatur, di mana satu literatur dapat menggunakan lebih dari satu framework atau standar. Oleh karena itu, jumlah total pada grafik tidak merepresentasikan jumlah artikel, melainkan frekuensi kemunculan framework.

Berdasarkan Gambar 5.1, framework COBIT merupakan framework yang paling dominan digunakan dalam kajian infrastruktur TI. Hal ini menunjukkan bahwa sebagian besar penelitian memandang pengelolaan infrastruktur TI dari perspektif tata kelola dan pengendalian. Selain itu, ISO/IEC 27001 dan NIST *Cybersecurity Framework* juga menunjukkan tingkat penggunaan yang tinggi, yang mencerminkan meningkatnya fokus penelitian terhadap keamanan informasi dan risiko siber. ITIL digunakan terutama dalam penelitian yang membahas manajemen layanan TI dan operasional infrastruktur.

5.3 Analisis Komponen Infrastruktur Teknologi Informasi

Selain menganalisis distribusi framework, penelitian ini juga mengkaji komponen infrastruktur TI yang paling sering dibahas dalam literatur. Analisis ini penting untuk memahami fokus utama penelitian infrastruktur TI yang berkembang dalam beberapa tahun terakhir.

E-ISSN : 2746-2331
P-ISSN : 2746-234X



Gambar 5.2 Distribusi Komponen Infrastruktur Teknologi Informasi

Gambar 5.2 menyajikan distribusi komponen infrastruktur TI yang dibahas dalam literatur, yang meliputi tata kelola TI, keamanan informasi, manajemen layanan TI, dan infrastruktur teknis seperti perangkat keras, perangkat lunak, dan jaringan. Data grafik diperoleh melalui proses pengelompokan literatur berdasarkan komponen infrastruktur TI yang menjadi fokus pembahasan.

Berdasarkan Gambar 5.2, komponen tata kelola TI dan keamanan informasi merupakan komponen yang paling dominan dibahas dalam literatur. Temuan ini menunjukkan adanya pergeseran fokus penelitian dari aspek teknis infrastruktur TI menuju pendekatan yang lebih strategis dan berbasis pengendalian. Sementara itu, manajemen layanan TI dan infrastruktur teknis tetap menjadi bagian penting, namun tidak menjadi fokus utama dalam sebagian besar penelitian.

5.4 Pembahasan Hasil Penelitian

Hasil penelitian ini menunjukkan bahwa kajian infrastruktur Teknologi Informasi dalam literatur ilmiah semakin menekankan pentingnya tata kelola TI dan keamanan informasi sebagai fondasi utama dalam pengelolaan infrastruktur TI. Dominasi *framework* COBIT dalam literatur mengindikasikan bahwa aspek pengendalian, manajemen risiko, serta

keselarasan TI dengan tujuan strategis organisasi menjadi perhatian utama dalam penelitian dan praktik pengelolaan infrastruktur TI.

Selain itu, tingginya penggunaan standar ISO/IEC 27001 dan NIST *Cybersecurity Framework* menunjukkan bahwa keamanan informasi telah menjadi komponen integral dalam pengelolaan infrastruktur TI modern. Meningkatnya ancaman siber serta tuntutan kepatuhan terhadap regulasi mendorong organisasi untuk mengadopsi pendekatan berbasis standar dalam melindungi aset informasi dan memastikan ketahanan infrastruktur TI, khususnya pada sistem dan jaringan yang bersifat kritis.

Secara keseluruhan, hasil dan pembahasan ini menegaskan bahwa pengelolaan infrastruktur TI yang efektif tidak dapat dilakukan secara parsial. Diperlukan pendekatan terintegrasi yang mencakup tata kelola TI, manajemen layanan TI, dan keamanan informasi secara bersamaan. Temuan ini memberikan dasar konseptual yang kuat bagi pengembangan penelitian lanjutan serta penyusunan rekomendasi praktis dalam pengelolaan infrastruktur TI berbasis standar internasional.

Hasil penelitian ini memberikan implikasi praktis bagi organisasi dalam pengelolaan infrastruktur Teknologi Informasi. Dominasi *framework* tata kelola TI dan keamanan informasi dalam literatur menunjukkan bahwa organisasi perlu memprioritaskan penerapan mekanisme tata kelola, manajemen risiko, dan perlindungan aset informasi secara terstruktur, bukan hanya berfokus pada pengelolaan infrastruktur teknis. Temuan penelitian ini dapat dimanfaatkan oleh praktisi TI sebagai referensi dalam memilih dan mengintegrasikan framework yang sesuai dengan kebutuhan organisasi, seperti menggunakan COBIT untuk penguatan tata kelola dan pengendalian, ITIL untuk pengelolaan layanan TI, serta ISO/IEC 27001 atau NIST Cybersecurity Framework untuk memastikan keamanan informasi dan ketahanan infrastruktur TI secara berkelanjutan.

E-ISSN : 2746-2331
P-ISSN : 2746-234X

6. Kesimpulan

Berdasarkan hasil *Systematic Literature Review* terhadap 22 publikasi ilmiah yang membahas infrastruktur Teknologi Informasi, dapat disimpulkan bahwa pengelolaan infrastruktur TI dalam literatur tidak lagi berfokus pada aspek teknis semata, melainkan berkembang menuju pendekatan yang lebih strategis dan terintegrasi. Penelitian-penelitian yang dianalisis menunjukkan bahwa infrastruktur TI dipandang sebagai aset strategis yang memerlukan tata kelola, manajemen layanan, serta pengendalian risiko yang sistematis.

Hasil pemetaan literatur menunjukkan bahwa framework dan standar internasional seperti COBIT, ITIL, ISO/IEC 27001, dan NIST Cybersecurity Framework merupakan kerangka kerja yang paling dominan digunakan dalam kajian infrastruktur TI. Dominasi framework tersebut mengindikasikan bahwa tata kelola TI, manajemen layanan, dan keamanan informasi menjadi fokus utama dalam pengelolaan infrastruktur TI pada berbagai konteks organisasi.

Selain itu, analisis distribusi komponen infrastruktur TI menunjukkan bahwa tata kelola TI dan keamanan informasi merupakan komponen yang paling banyak dibahas dalam literatur, dibandingkan dengan komponen teknis seperti perangkat keras, perangkat lunak, dan jaringan. Temuan ini menegaskan adanya pergeseran fokus penelitian dari pengelolaan teknis menuju pendekatan berbasis tata kelola dan risiko.

Secara keseluruhan, penelitian ini menyimpulkan bahwa pengelolaan infrastruktur TI yang efektif memerlukan pendekatan holistik dan terintegrasi yang menggabungkan tata kelola TI, manajemen layanan TI, dan keamanan informasi. Kesimpulan ini memberikan dasar konseptual bagi organisasi dalam memilih dan mengintegrasikan *framework* atau standar internasional yang sesuai dengan kebutuhan dan karakteristik pengelolaan infrastruktur TI.

Daftar Pustaka

Almeida, R., & Da Silva, M. M. (2021). Governance and management of IT: A systematic literature review. *Procedia Computer Science*, *181*, 1032–1039. https://doi.org/10.1016/j.procs.2021.01.302

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Axelos. (2019). *ITIL® Foundation: ITIL 4 edition*. TSO (The Stationery Office).

Budiman, A., & Lubis, Y. F. A. (2025). Perbandingan Framework COBIT 2019 dan ITIL 4 dalam Tata Kelola Teknologi Informasi. *Jurnal Ilmu Komputer dan Teknik Informatika*, *1*(2), 52–57. https://doi.org/10.64803/juikti.v1i2.50

Christiadi, R. N., & Sutomo, R. (2023). Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector. *G-Tech: Jurnal Teknologi Terapan*, *7*(4), 1498–1508. https://doi.org/10.33379/gtech.v7i4.3170

Fadila, V., Mutiah, N., Puspita Sari, R., Nawawi, P., Ahmad Yani, J., & - Kalimantan Barat, P. (2023). Audit Keamanan Siber Menggunakan Kerangka Kerja CIS CSC, NIST CSF, dan COBIT 2019 Cyber Security Audit using CIS CSC, NIST CSF and COBIT 2019 Framework. *Journal of Computing Engineering, System and Science)*, *8*(2), 271–283. www.jurnal.unimed.ac.id

Fryonanda, H., Sokoco, H., Nurhadryani, Y., Sistem, J., Fakultas, I., Kreatif, I., Institute, K., Departemen,), Komputer, I., Ilmu, F., Alam, P., & Pertanian Bogor, I. (2019). *Evaluasi Infrastruktur Teknologi Informasi Dengan COBIT 5 dan ITIL V3*.

ISACA. (2019). *COBIT® 2019 framework: Governance and management objectives*. ISACA.

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

Lokare, A., Shripad Bankar, U., & Padmajeet Mhaske JPMC, U. (2022). *Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies*.

Mehedi Rahman, M., Kshetri, N., Abu Sayeed, S., & Masud Rana, M. (t.t.). *AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and Cybersecurity risk assessment*.

NIST. (2020). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. National Institute of Standards and Technology (NIST).

Pereira, R., Santos, M., & Gonçalves, J. (2021). IT infrastructure governance: A systematic literature review. *Journal of Information Systems Engineering and Management*, *6*(1), em0131.

Purnama, D. G., & Akbar, R. I. (2025). Analisis Penerapan Tata Kelola TI menggunakan COBIT 5.0 dan COBIT 2019 Article Info ABSTRAK. *JSAI : Journal Scientific and Applied Informatics*, *08*(2). https://doi.org/10.36085

Purwanto, I., & Mardjono, R. (2021). Cobit 5 dalam Proses Audit Tata kelola Teknologi Informasi pada Dinas Pendidikan Kabupaten Tulang Bawang – Lampung. *Explore: Jurnal Sistem Informasi dan Telematika*, *12*(2), 259. https://doi.org/10.36448/jsit.v12i2.2361

Rahman, R., Ananta, A., Surianti, B., & Artikel, S. (2024). *Technology Sciences Insights Journal Analisis Perbandingan Framework Keamanan Jaringan (NIST CSF, CIS Controls, ISO 27001) INFORMASI ARTIKEL ABSTRAK*.

Rochmania, N., Rozas, I., & Ilham, I. (2020). Tren Penggunaan Framework COBIT, ITIL, dan ISO 27001 Pada Rentang Tahun 2014-2018 di Indonesia. *Edumatic: Jurnal Pendidikan Informatika*, *4*(2), 10–19. https://doi.org/10.29408/edumatic.v4i2.2249

Santoso, H. (2025). *Hal Kata kunci: COBIT 2019, IT governance, IT maturity level*. *5*(6). https://doi.org/10.52436/1.jpti.775

Sigit Julianto, A., Hikmah, I. R., & Yasa, R. N. (2024). *Cyber-Risk Management Menggunakan NIST Cybersecurity Framework (CSF) dan COBIT 2019 pada Instansi XYZ*.

Sudanawati Rozas, I., Rochmania, N., & Studi Sistem Informasi UIN Sunan Ampel Surabaya, P. (2020). Statistik Penelitian Berbasis Kerangka Kerja COBIT, ITIL, dan ISO 27001 di Indonesia. Dalam *JIFTI-Jurnal Ilmiah Teknologi Informasi dan Robotika* (Vol. 2).

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). *Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS*.

Zulkarnain, Z., Lorenz, C., Taai, D., Elia, E., Wenky, W., Wilson, W., & Estrada, Y. (2024). Peran COBIT 5 dan ITIL V3 Dalam Meningkatkan Tata Kelola TI dan Kesuksesan Proyek Sistem Informasi. *Jurnal Minfo Polgan*, *13*(1), 588–599. https://doi.org/10.33395/jmp.v13i1.13748