Perbandingan Framework COBIT2019 dan TOGAF dalam Manajemen Keamanan Informasi

Fajri Nugraha[1]✉, Billy Hendrik[2]
(1,2) Teknik Informatika, Universitas Putra Indonesia (UPI) YPTK Padang, Indonesia

✉ Corresponding author
[fajrinugraha7@gmail.com]

Abstrak

Manajemen Keamanan Informasi (*Information Security Management*) adalah salah satu aspek penting dalam mendukung organisasi di era digital. Penelitian ini bertujuan untuk mengevaluasi efektivitas, kesesuaian, dan cakupan masing-masing *framework* dalam mendukung standar manajemen keamanan informasi. *Framework* seperti COBIT2019 dan TOGAF menawarkan pendekatan yang berbeda tetapi saling melengkapi untuk penerapan standar keamanan informasi. Analisis tersebut didasarkan pada *literatur review*, tinjauan teori, dan implementasi di berbagai organisasi. Penelitian diharapkan dapat membantu organisasi memilih dan mengintegrasikan *framework* yang paling sesuai dengan kebutuhan dan situasi organisasi. Studi ini juga membantu meningkatkan pemahaman teoritis dan praktis tentang penerapan standar manajemen keamanan informasi berbasis *framework*.

Kata Kunci: *Manajemen Keamanan Informasi*, *COBIT2019*, *TOGAF*, *Literature Review*.

Abstract

Information Security Management is one of the important aspects in supporting organizations in the digital era. This research aims to evaluate the effectiveness, suitability, and coverage of each framework in supporting information security management standards. Frameworks such as COBIT2019 and TOGAF offer different yet complementary approaches for the implementation of information security standards. The analysis is based on literature review, theoretical review, and implementation in various organizations. The research is expected to help organizations choose and integrate the framework that best suits their needs and situations. This study also helps enhance the theoretical and practical understanding of the implementation of framework-based information security management standards.

Keyword: *Information Security Management*, *COBIT2019*, *TOGAF*, *Literature Review*.

PENDAHULUAN

Dalam beberapa tahun terakhir, ancaman terhadap keamanan informasi telah meningkat secara signifikan, terutama dengan berkembangnya teknologi digital dan penggunaan sistem berbasis cloud. Misalnya, laporan dari IBM Security (2022) mencatat bahwa biaya pelanggaran data secara global mencapai rata-rata 4,35 juta dolar AS per insiden. Angka ini menunjukkan betapa pentingnya pengelolaan keamanan informasi yang efektif bagi organisasi dari berbagai sektor.

Perencanaan, pengorganisasian, pengarahan, dan pengendalian sumber daya untuk mencapai tujuan tertentu disebut manajemen. Sebaliknya, keamanan mengacu pada perlindungan terhadap ancaman yang dapat merusak aset atau sumber daya fisik atau digital. Data yang telah diproses sehingga memiliki nilai dan relevansi bagi penggunanya disebut data. Dengan menggabungkan ketiga ide ini, manajemen keamanan informasi muncul, yang bertujuan untuk melindungi data dari ancaman dengan menjaga integritas, kerahasiaan, dan aksesibilitasnya.

Di era digital yang semakin canggih, keamanan informasi telah menjadi elemen penting bagi kelangsungan operasional organisasi. Berbagai risiko muncul dari ancaman siber, pencurian data, dan pelanggaran data, sehingga memerlukan pengelolaan organisasi yang sistematis dan terstruktur. *Framework* tata kelola TI seperti COBIT2019 dan TOGAF telah diadopsi oleh berbagai organisasi

untuk memenuhi kebutuhan keamanan informasi mereka. Menurut ISACA (2019), COBIT2019 memberikan pendekatan berbasis nilai bisnis untuk mengoptimalkan tata kelola TI dan keamanan informasi, dan The Open Group (2018) menyatakan bahwa TOGAF menyediakan arsitektur perusahaan yang mencakup kebijakan keamanan informasi komprehensif suatu organisasi membantu dalam desain.

Berbagai organisasi modern harus mematuhi standar keamanan informasi. ISO/IEC 27001 adalah standar global yang banyak digunakan untuk memastikan pengelolaan keamanan informasi yang sistematis dan terorganisir. ISO/IEC 27001 memberikan pedoman untuk menetapkan, mengimplementasikan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (SMKI). Selain itu, peraturan lokal, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 di Indonesia, mengatur keamanan data elektronik, terutama di sektor publik. Struktur seperti COBIT2019 dan TOGAF didukung oleh standar ini untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi secara optimal.

Berbagai perusahaan besar di Indonesia telah menggunakan *framework* COBIT2019 dan TOGAF untuk meningkatkan tata kelola dan keamanan informasi mereka. PT Telkom Indonesia menggunakan COBIT2019 untuk membuat strategi pengelolaan risiko TI, sementara Bank Indonesia menggunakan TOGAF untuk membuat arsitektur teknologi yang membantu integrasi sistem keuangan nasional. Selain itu, lembaga pemerintah tertentu, seperti Badan Siber dan Sandi Negara (BSSN), menggunakan prinsip-prinsip dari kedua rangka kerja ini untuk memastikan keberlanjutan dan keamanan infrastruktur digital mereka.

Penelitian sebelumnya oleh Johnson dkk. (2020) menunjukkan bahwa *framework* COBIT2019 lebih cocok untuk organisasi yang memerlukan panduan rinci mengenai manajemen risiko dan evaluasi kinerja keamanan informasi. TOGAF kini lebih umum digunakan oleh organisasi yang berfokus pada pengintegrasian perencanaan strategis dan arsitektur TI (Smith & Brown, 2021). Penelitian lebih lanjut yang dilakukan Parinduri dan Hartono (2023) juga menunjukkan bahwa tingkat kinerja organisasi yang menggunakan COBIT2019 masih memerlukan perbaikan dari sisi keamanan informasi. Hal ini menyoroti pentingnya penelitian lebih lanjut mengenai penerapan komprehensif kedua *framework* ini.

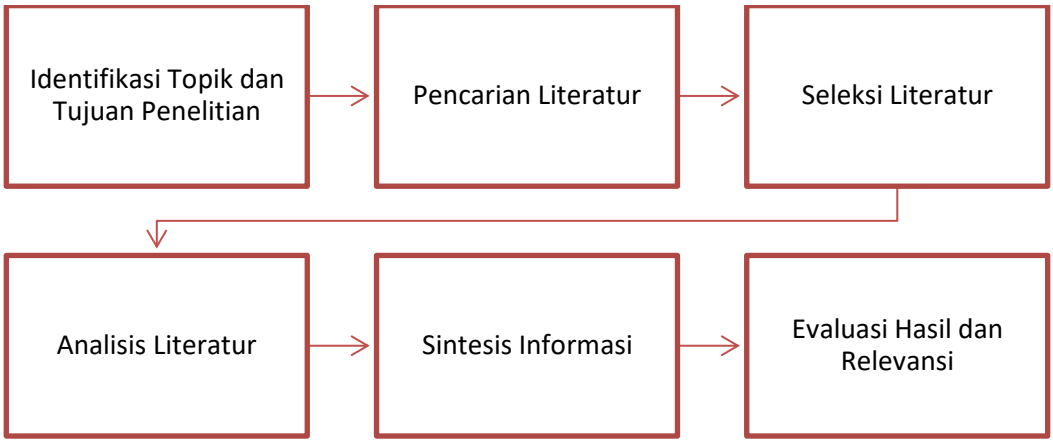
Meskipun COBIT2019 dirancang untuk mendukung manajemen risiko berbasis nilai bisnis dan tata kelola TI, TOGAF lebih fokus pada pengembangan arsitektur perusahaan yang mencakup domain keamanan. Puspitasari dan Achjari (2018) menunjukkan bahwa meskipun integrasi *framework* dalam organisasi pemerintah dapat meningkatkan efisiensi tata kelola TI, pedoman khusus masih diperlukan untuk mengoptimalkan penerapan keamanan informasi.

Meskipun memiliki tujuan yang sama yaitu meningkatkan efektivitas manajemen keamanan informasi, kedua *framework* ini menawarkan pendekatan dan alat yang berbeda dalam penerapannya. Oleh karena itu, penting untuk melakukan penelitian komparatif untuk memahami kekuatan dan kelemahan masing-masing framework dan bagaimana keduanya dapat diintegrasikan untuk menciptakan pendekatan holistik terhadap manajemen keamanan informasi.

Penelitian ini bertujuan untuk mengevaluasi perbedaan utama, kelebihan dan kemungkinan integrasi antara COBIT2019 dan TOGAF dari perspektif manajemen keamanan informasi. Oleh karena itu, penelitian ini diharapkan dapat memberikan panduan yang berguna dalam memilih atau mengadaptasi suatu framework kerja untuk memenuhi kebutuhan suatu organisasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode *literature review*. *Literature review* merupakan metode yang bertujuan untuk mengumpulkan, mengevaluasi, dan mensintesis penelitian yang relevan guna membangun dasar argumen ilmiah (Webster & Watson, 2002). Sumber data yang digunakan antara lain artikel atau jurnal ilmiah yang dikumpulkan dari berbagai sumber, kemudian buku berkaitan dengan topik penelitian. Tujuan dari penelitian ini yaitu untuk membantu mengevaluasi perbedaan utama antara *framework* COBIT2019 dan TOGAF dalam konteks manajemen keamanan informasi, kemudian bertujuan untuk mengidentifikasi keunggulan dan kelemahan masing-masing *framework* berdasarkan *literature review*, kemudian memberikan rekomendasi mengenai integrasi kedua *framework* untuk menciptakan pendekatan yang lebih holistik dalam manajemen keamanan informasi, sehingga organisasi memiliki panduan praktis dalam menentukan *framework* yang tepat sesuai kondisi organisasi.



Gambar 1. Langkah-langkah *Literature Review*

Seperti yang dapat dilihat pada Gambar 1, proses penelitian dibagi menjadi empat tahap, yaitu: 1) Identifikasi Topik dan Tujuan Penelitian; menentukan fokus penelitian pada perbandingan *framework* COBIT2019 dan TOGAF dalam konteks manajemen keamanan informasi. Pada tahap ini, peneliti juga mengidentifikasi kebutuhan akan referensi ilmiah untuk mendukung analisis. 2) Pencarian Literatur: Mengumpulkan artikel, jurnal ilmiah, buku, dan laporan yang relevan menggunakan kata kunci seperti "COBIT2019", "TOGAF", "manajemen keamanan informasi", dan "*framework* tata kelola TI". Pencarian dilakukan melalui database akademik seperti IEEE Xplore, Springer, dan Google Scholar, serta publikasi lokal yang relevan seperti BSSN dan jurnal universitas. 3) Seleksi Literatur: Melakukan seleksi literatur berdasarkan relevansi, kualitas sumber, dan keterkinian. Artikel yang dipilih adalah yang membahas implementasi dan efektivitas kedua *framework* dalam konteks keamanan informasi. Seperti diungkapkan oleh Okoli & Schabram (2010), proses seleksi literatur yang ketat dapat memastikan validitas temuan. 4) Analisis Literatur: Menyusun kategori analisis seperti fokus *framework*, keunggulan, kelemahan, dan contoh implementasi. Setiap sumber dianalisis untuk mengidentifikasi persamaan dan perbedaan antara COBIT2019 dan TOGAF. Menurut Kitchenham (2004), analisis ini penting untuk memahami hubungan antara teori dan praktik. 5) Sintesis Informasi: Mengintegrasikan hasil analisis ke dalam narasi deskriptif dan tabel perbandingan. Pada tahap ini, peneliti menggabungkan wawasan dari berbagai sumber untuk membangun argumen yang mendalam. 6) Evaluasi Hasil dan Relevansi: Mengkaji ulang informasi yang telah disintesis untuk memastikan kesesuaian dengan tujuan penelitian dan validitas temuan. Hal ini juga mencakup pemetaan temuan terhadap *framework* teoritis yang relevan.

Penelitian ini disajikan dalam bentuk narasi deskriptif dan disertai tabel perbandingan yang memberikan gambaran mengenai kedua *framework*. Oleh karena itu, penelitian ini dapat memberikan wawasan yang mendalam dan relevan bagi para praktisi dan peneliti dalam bidang tata kelola keamanan informasi.

HASIL DAN PEMBAHASAN

Manajemen keamanan informasi adalah pendekatan sistematis untuk melindungi data organisasi, infrastruktur TI, dan aset digital dari berbagai ancaman. Hal ini mencakup penetapan kebijakan, prosedur, dan pengendalian teknis untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi. *Framework* seperti COBIT2019 dan TOGAF memberikan panduan khusus untuk membantu organisasi mencapai tujuan tersebut.

Dalam kondisi saat ini, serangan ransomware seperti insiden Colonial Pipeline di Amerika Serikat menunjukkan betapa rentannya infrastruktur penting terhadap serangan siber. Menurut laporan Badan Keamanan Siber dan Infrastruktur (CISA), peretasan ini tidak hanya menyebabkan gangguan pasokan bahan bakar tetapi juga kerugian ekonomi yang signifikan (CISA, 2021). Insiden ini menyoroti pentingnya memiliki *framework* keamanan informasi yang kuat untuk melindungi aset-aset penting.

Selain itu, laporan Badan Siber dan Sandi Negara (BSSN) 2023 menemukan peningkatan tajam serangan phishing terhadap lembaga pendidikan dan keuangan. Serangan-serangan ini sering kali mengeksploitasi kerentanan dalam sistem keamanan informasi yang tidak dikelola dengan baik. Penggunaan *framework* seperti COBIT2019 dapat membantu organisasi mengidentifikasi risiko dan menerapkan kontrol yang tepat untuk memitigasi ancaman ini.

Pelanggaran data besar-besaran yang melibatkan perusahaan teknologi besar, seperti insiden Meta tahun 2022, menyoroti pentingnya arsitektur keamanan yang kuat. *Framework* TOGAF dapat memberikan panduan strategis untuk membangun sistem TI yang lebih terintegrasi dan tahan terhadap ancaman. Penelitian Suryani dan Ramadhan (2021) menunjukkan bahwa pendekatan berbasis arsitektur dapat membuat organisasi lebih tahan terhadap serangan yang kompleks.

Framework ini juga selaras dengan standar keamanan informasi seperti ISO/IEC 27001, yang menetapkan prinsip kerahasiaan, integritas, dan ketersediaan informasi sebagai inti dari manajemen keamanan informasi. Dalam hal ini, COBIT2019 secara khusus membantu organisasi dalam mendesain kontrol operasional dan tata kelola risiko, sementara TOGAF mendukung perancangan arsitektur TI yang komprehensif berdasarkan standar yang telah diterima secara internasional. Relevansi kedua framework ini dengan standar tersebut membantu organisasi mencapai kepatuhan yang tidak hanya meningkatkan keamanan informasi tetapi juga memperkuat kepercayaan mitra bisnis dan pelanggan.

Sebagai contoh, Bank Indonesia menggunakan TOGAF untuk membangun infrastruktur yang mendukung Sistem Pembayaran Nasional, yang secara langsung mengacu pada standar ISO/IEC 27001 untuk pengelolaan risiko keamanan informasi. PT Telkom Indonesia juga menggunakan COBIT2019 untuk mendukung implementasi kontrol yang sesuai dengan peraturan pemerintah terkait perlindungan data elektronik, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 di Indonesia. Implementasi praktis dari framework ini juga dapat ditemukan di Indonesia. PT Telkom Indonesia menggunakan COBIT2019 untuk mengembangkan tata kelola risiko terintegrasi di seluruh area bisnis. *Framework* ini membantu organisasi-organisasi ini mengidentifikasi potensi ancaman dan mengambil tindakan remediasi yang efektif.

Selain itu, penelitian oleh Puspitasari dan Achjari (2018) menunjukkan bahwa implementasi standar manajemen keamanan informasi yang selaras dengan framework seperti COBIT2019 dan TOGAF dapat membantu organisasi tidak hanya dalam pengelolaan risiko, tetapi juga dalam meningkatkan efisiensi operasional melalui pengurangan duplikasi proses dan peningkatan transparansi. Dalam konteks global, framework ini memungkinkan perusahaan untuk menghadapi tantangan yang muncul dari regulasi seperti GDPR di Eropa dan standar serupa lainnya.

Studi yang dilakukan Dewi dan Achjari (2021) menyoroti bahwa *framework* COBIT2019 dapat meningkatkan efisiensi operasional dengan meningkatkan proses pengambilan keputusan berbasis risiko. Namun studi ini juga menunjukkan bahwa penerapan *framework* ini memerlukan investasi sumber daya manusia dan teknis yang signifikan. Hal serupa juga terlihat pada implementasi TOGAF. Dalam TOGAF, kompleksitas desain arsitektur seringkali menjadi tantangan bagi organisasi yang tidak memiliki sumber daya teknis yang memadai.

Hasil analisis menunjukkan bahwa baik COBIT2019 maupun TOGAF memiliki kekuatan dan kelemahan dalam mendukung manajemen keamanan informasi. COBIT2019 unggul dalam memberikan panduan rinci untuk tata kelola TI, khususnya dalam pengelolaan risiko dan pengukuran kinerja keamanan. Domain seperti EDM03 (Ensured Risk Optimization) dan DSS05 (Managed Security Services) memberikan pedoman terperinci yang membantu organisasi mengelola keamanan informasi secara operasional. Namun, penelitian oleh Parinduri dan Hartono (2023) menunjukkan bahwa implementasi COBIT2019 sering kali menghadapi tantangan dalam mencapai tingkat kapabilitas yang optimal, terutama pada organisasi dengan sumber daya yang terbatas.

TOGAF, di sisi lain, menawarkan pendekatan konseptual yang kuat melalui metode ADM (Architecture Development Method). Pendekatan ini membantu organisasi dalam merancang arsitektur TI yang mencakup kebijakan keamanan sejak tahap perencanaan hingga implementasi. Smith dan Brown (2021) mencatat bahwa TOGAF sangat efektif untuk organisasi yang membutuhkan integrasi antara berbagai domain TI, termasuk keamanan, data, dan teknologi. Namun, kelemahan utama TOGAF adalah kurangnya panduan spesifik untuk implementasi operasional, yang membuatnya memerlukan integrasi dengan *framework* lain seperti COBIT2019. Perbandingan singkat mengenai kedua *framework* ini dapat dilihat pada tabel.1 sebagai berikut:

Tabel 1. Perbandingan Berdasarkan Studi Terdahulu

Sumber	Keunggulan COBIT2019	Keunggulan TOGAF	Kelemahan
Parinduri & Hartono (2023)	Tata kelola risiko yang rinci	Integrasi arsitektur perusahaan	Memerlukan SDM yang terlatih
Smith & Brown (2021)	Operasionalisasi keamanan informasi	Strategi holistik untuk perencanaan	Kurangnya panduan untuk operasional
Puspitasari & Achjari (2018)	Efektivitas untuk instansi pemerintah	Fleksibilitas dalam desain arsitektur	Sulit diterapkan dalam organisasi kecil
Dewi & Achjari (2021)	Optimisasi risiko keamanan	Perancangan arsitektur skala besar	Membutuhkan waktu implementasi panjang
Johnson et al. (2020)	Fokus pada pengukuran kinerja	Integrasi lintas domain TI	Membutuhkan investasi besar

Integrasi kedua *framework* ini dapat menciptakan pendekatan yang lebih holistik untuk manajemen keamanan informasi. COBIT2019 dapat digunakan untuk mengidentifikasi risiko dan menetapkan kontrol operasional, sementara TOGAF menyediakan kerangka kerja strategis untuk mendukung keputusan arsitektur yang melibatkan berbagai domain TI. Contoh implementasi di PT Telkom Indonesia dan Bank Indonesia menunjukkan bahwa adopsi *framework* ini dapat membantu organisasi menghadapi tantangan keamanan informasi yang semakin kompleks. Penelitian ini juga mengidentifikasi beberapa tantangan dalam implementasi *framework*, seperti kebutuhan akan sumber daya manusia yang terlatih, investasi teknologi yang besar, dan waktu yang dibutuhkan untuk mencapai hasil yang optimal. Oleh karena itu, organisasi perlu mempertimbangkan kapasitas internal mereka sebelum memilih atau mengintegrasikan *framework* ini.

Dengan mempertimbangkan situasi terkini, kasus serangan siber, dan implementasi *framework*, jelas bahwa pengadopsian COBIT2019 dan TOGAF dapat membantu organisasi dalam menghadapi tantangan keamanan informasi di era digital. Penggunaan kedua *framework* ini secara sinergis memungkinkan organisasi untuk mengatasi kelemahan masing-masing *framework* dan menciptakan pendekatan yang lebih holistik untuk tata kelola keamanan informasi.

SIMPULAN

Berdasarkan kajian literatur, dapat disimpulkan bahwa baik COBIT2019 maupun TOGAF memiliki keunggulan unik yang dapat disesuaikan dengan kebutuhan organisasi. COBIT2019 unggul dalam memberikan panduan operasional dan pengukuran kinerja, sementara TOGAF menyediakan metodologi yang terstruktur untuk merancang arsitektur keamanan. Integrasi kedua *framework* ini dapat memberikan manfaat yang signifikan bagi organisasi yang ingin mengoptimalkan manajemen keamanan informasi mereka. Sebagai penutup, penelitian ini memberikan panduan berharga bagi organisasi, peneliti, dan praktisi untuk memahami dan mengimplementasikan *framework* COBIT2019 dan TOGAF. Ke depannya, pengembangan *framework* yang lebih adaptif dan studi lanjutan mengenai integrasi kedua pendekatan ini diharapkan dapat memberikan kontribusi signifikan terhadap peningkatan manajemen keamanan informasi secara global.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada semua pijak yang telah membantu kami menyusun artikel ini. Kami juga mengucapkan terima kasih kepada para peneliti sebelumnya yang telah memberikan inspirasi melalui penelitian mereka yang menyeluruh. Kami juga menghargai peran institusi akademik dan profesional yang memberikan akses ke database ilmiah dan literatur. Kami berharap artikel ini akan memberikan kontribusi yang untuk kemajuan ilmu pengetahuan, khususnya dalam bidang tata kelola teknologi informasi dan keamanan informasi. Kami berharap organisasi, peneliti, dan praktisi yang ingin meningkatkan pemahaman mereka tentang penerapan *framework* COBIT2019 dan TOGAF dapat menggunakannya sebagai referensi.

DAFTAR PUSTAKA

Amstrong, P., & Levis, R. (2020). Strategic security governance frameworks: A comparative study of COBIT and TOGAF. *Cybersecurity Journal*, *15*(2), 101–115.

Clarkson, P. (2021). The role of COBIT and TOGAF in enhancing organizational resilience. *Journal of Information Security and Applications*, *58*, 102–117.

Dewi, G. K., & Achjari, D. (2021). Analisis keamanan sistem informasi Universitas X. *ABIS: Accounting and Business Information Systems Journal*, *9*(1), 1–14.

Green, D. (2021). Aligning business goals with security architecture: A guide to TOGAF and COBIT. *Business IT Review*, *33*(1), 55–72.

Hidayat, A., & Pratama, Y. (2022). Evaluasi framework COBIT dalam meningkatkan keamanan informasi di perusahaan multinasional. *Jurnal Teknologi Informasi*, *12*(3), 78–88.

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

IT Governance Institute. (2021). *Integrating COBIT with enterprise frameworks*. ITGI Press.

Johnson, M., Smith, R., & Taylor, L. (2020). Comparative analysis of COBIT 2019 and TOGAF in information security management. *Journal of Information Systems Management*, *37*(4), 245–256.

Kitchenham, B. (2004). *Procedures for performing systematic reviews*. Keele University Technical Report.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Journal of Information Technology*, *28*(1), 5–28.

Parinduri, A. F. K., & Hartono, J. (2023). Evaluasi penerapan tata kelola teknologi informasi (TI) menggunakan framework COBIT 2019 (studi kasus pada Perguruan Tinggi Harapan Maju). *ABIS: Accounting and Business Information Systems Journal*, *11*(3), 225–239.

Puspitasari, E. Y., & Achjari, D. (2018). Evaluasi perencanaan manajemen teknologi informasi dengan pendekatan COBIT 5 framework (studi pada Dinas Komunikasi dan Informatika Kabupaten Pringsewu). *ABIS: Accounting and Business Information Systems Journal*, *6*(3), 1–15.

Rahayu, S., & Ahmad, T. (2022). Optimalisasi tata kelola TI dengan COBIT dan TOGAF. *Jurnal Sistem dan Teknologi Informasi*, *8*(4), 200–210.

Smith, J., & Brown, P. (2021). Integrating TOGAF and COBIT 2019 for holistic security governance. *International Journal of IT Governance and Security*, *12*(1), 34–47.

Suryani, E., & Ramadhan, R. (2021). Arsitektur TI untuk penguatan keamanan informasi menggunakan TOGAF. *Jurnal Rekayasa Sistem Informasi*, *5*(2), 101–115.

Telkom Indonesia. (2022). Perancangan tata kelola teknologi informasi berbasis COBIT 2019. *Jurnal Teknik Informatika*, *14*(3), 22–34.

The Open Group. (2018). *TOGAF and risk management: Case studies*. The Open Group Publications.

The Open Group. (2018). *TOGAF® standard, version 9.2*. The Open Group.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.

White, R. (2020). *Enterprise architecture and information security: Practical insights from TOGAF and COBIT integration*. Springer Press.

Wilson, J. (2022). COBIT 2019 and TOGAF synergy for cybersecurity implementation. *Technology and Policy Journal*, *9*(3), 44–59.