

Literature Review: Evaluasi Keefektifan *Framework* Audit Teknologi Informasi pada Perguruan Tinggi

Ni Kadek Dwi Suryadewi¹, Ida Bagus Gede Manuaba², Lie Jasa³

[Submission: 26-01-2024, Accepted: 30-06-2024]

Abstract— This literature review paper explores the effectiveness of Information Technology (IT) audit frameworks in the context of higher education, with particular emphasis on the role of IT governance in ensuring the optimal utilization of technology resources in higher education. The impact of the rapid development of Information Technology has been significantly felt in various aspects of life, especially in the education sector. This study specifically evaluates a number of commonly used IT audit frameworks, including COBIT, ISO/IEC 27002:2013, COSO, ITIL V3, HCYMAF, TOGAF and CMMI. The research method involves a literature study by collecting data from reliable sources such as Google Scholar, IEEE Xplore, ScienceDirect, ResearchGate, JSTOR, and Wiley Online Library. This research guides the reader through a thorough evaluation of the effectiveness of each audit framework, supported by specific case studies that illustrate their application in the context of higher education. The in-depth analysis covers key factors such as security, efficiency, regulatory compliance, and overall maturity in IT management. This research aims to provide better insight into the importance of selecting an IT audit framework that suits the unique needs of each institution. Therefore, this paper is expected to make a valuable contribution in deepening the understanding of the role of IT audit frameworks in managing and improving the effective use of information technology in higher education.

Intisari— *Paper* tinjauan literatur ini mengeksplorasi efektivitas kerangka kerja audit Teknologi Informasi (TI) dalam konteks pendidikan tinggi, dengan penekanan utama pada peran tata kelola TI dalam memastikan optimalitas pemanfaatan sumber daya teknologi di perguruan tinggi. Dampak dari pesatnya perkembangan Teknologi Informasi telah terasa secara signifikan dalam berbagai aspek kehidupan, terutama di sektor pendidikan. Studi ini secara khusus melakukan evaluasi terhadap sejumlah *framework* audit TI yang umum digunakan, antara lain COBIT, ISO/IEC 27002:2013, COSO, ITIL V3, HCYMAF, TOGAF, dan CMMI. Metode penelitian melibatkan studi kepustakaan dengan mengumpulkan data dari sumber-sumber terpercaya seperti *Google Scholar*, *IEEE Xplore*, *ScienceDirect*, *ResearchGate*, *JSTOR*, dan *Wiley Online Library*. Penelitian ini memberikan panduan kepada pembaca melalui evaluasi menyeluruh terhadap keefektifan dari masing-masing *framework* audit dan didukung oleh studi kasus khusus yang

mengilustrasikan aplikasinya dalam konteks perguruan tinggi. Analisis secara mendalam mencakup faktor-faktor kunci seperti keamanan, efisiensi, kepatuhan regulasi, dan kematangan keseluruhan dalam manajemen TI. Penelitian ini memiliki tujuan untuk memberikan wawasan yang lebih baik mengenai pentingnya pemilihan *framework* audit TI yang sesuai dengan kebutuhan unik dari setiap institusi. Oleh karena itu, *paper* ini diharapkan dapat memberikan kontribusi berharga dalam memperdalam pemahaman tentang peran *framework* audit TI dalam mengelola dan meningkatkan efektivitas penggunaan teknologi informasi di lingkungan pendidikan tinggi.

Kata Kunci— *Literature Review*; Keefektifan; *Framework* Audit; Teknologi Informasi; Perguruan Tinggi.

I. PENDAHULUAN

Teknologi Informasi (TI) merujuk pada berbagai bentuk teknologi yang berperan dalam memproses, menyimpan, mengkomunikasikan, dan menyebarkan informasi untuk mendukung aktivitas manusia. Perkembangan teknologi informasi saat ini telah menghasilkan perubahan yang signifikan dalam kehidupan sehari-hari. Selain itu, TI memainkan peran penting dalam memfasilitasi komunikasi global melalui berbagai platform perangkat lunak seperti email, pesan instan, dan media sosial, memungkinkan koneksi antar individu di berbagai penjuru dunia. Akses mudah ke informasi melalui internet juga mempermudah pencarian berita, pengetahuan, dan sumber daya pendidikan [1].

Pemanfaatan teknologi informasi saat ini membawa tantangan dan peluang yang memerlukan evaluasi serta optimalisasi guna mencapai manfaat maksimalnya. Kemajuan teknologi informasi telah menyeluruh di berbagai aspek kehidupan manusia pada era saat ini, memengaruhi cara kita bekerja, berkomunikasi, belajar, dan berinteraksi, termasuk dalam konteks pendidikan. Oleh karena itu, sektor pendidikan dituntut untuk terus beradaptasi dengan perkembangan teknologi guna meningkatkan kualitas pendidikan, khususnya dalam mengintegrasikan teknologi informasi dan komunikasi ke dalam proses pembelajaran [2].

Pengelolaan teknologi informasi menjadi penting untuk memastikan pemanfaatannya yang optimal. Konsep ini dikenal sebagai tata kelola teknologi informasi, yang jika diterapkan dengan baik, dapat mendukung pencapaian tujuan suatu organisasi [3]. Perguruan tinggi memanfaatkan teknologi informasi dalam berbagai aspek, termasuk penggunaan platform e-learning untuk pembelajaran inovatif, portal mahasiswa untuk akses informasi kampus, dan sistem informasi administratif untuk manajemen akademik dan administrasi kampus secara efisien.

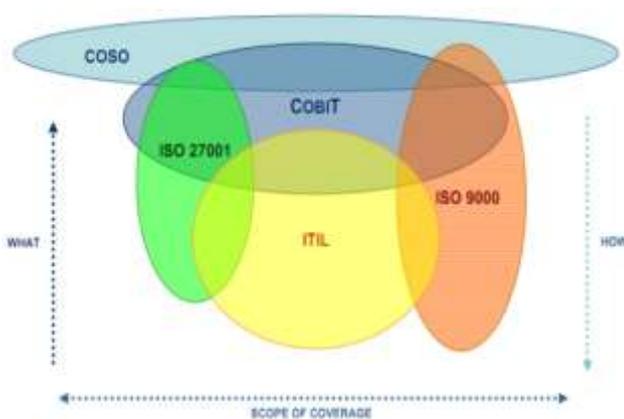
¹Mahasiswa, Program Studi Magister Teknik Elektro Universitas Udayana, Jl. Raya Babahan Kawan, Tabanan, Bali 82152 INDONESIA (telp: 081246397918; e-mail: dwisurya58@gmail.com)

^{2,3}Jurusan Teknik Elektro Fakultas Teknik Universitas Udayana, Jln. Jalan Kampus Bukit Jimbaran 80361 INDONESIA (telp: 0361-703315; fax: 0361-4321; e-mail: ibgmanuaba@gmail.com, liejasa@unud.ac.id)



Demi memastikan keamanan data dan sistem dalam berbagai manfaat penggunaan teknologi informasi, perlu diberikan perhatian khusus. Adopsi kebijakan keamanan teknologi informasi menjadi suatu keharusan, dan implementasinya harus konsisten. Semua pihak yang terlibat dalam penggunaan teknologi informasi perlu mengikuti pelatihan keamanan untuk memahami risiko dan langkah-langkah pencegahannya [4]. Prioritas utama adalah melindungi data sensitif, seperti data mahasiswa dan keuangan, karena keberlanjutan kerahasiaan dan integritas informasi tersebut sangat penting. Pelanggaran keamanan data dapat berakibat serius, seperti pelanggaran privasi, pencurian identitas, kerugian finansial, dan merusak reputasi institusi. Oleh karena itu, audit sistem informasi menjadi semakin penting untuk mengevaluasi pengendalian internal, meminimalisir risiko fraud, dan mendukung kelangsungan operasional perguruan tinggi [3].

Audit adalah proses pengumpulan dan evaluasi bukti terkait informasi untuk menilai kesesuaian informasi dengan kriteria yang telah ditetapkan. Proses ini dilakukan oleh individu yang kompeten di bidangnya [5]. Di sisi lain, audit teknologi informasi merupakan evaluasi dari seluruh kegiatan sistem informasi dalam suatu organisasi untuk menilai efektivitas dan integrasi aset dalam mencapai tujuan organisasional [6]. Walaupun banyak literatur membahas penerapan framework dalam instansi pendidikan, sedikit artikel yang membandingkan jenis-jenis framework tersebut. Oleh karena itu, penelitian ini bertujuan untuk menilai efektivitas framework audit teknologi informasi dalam meningkatkan keamanan sistem informasi dan meningkatkan kepuasan pengguna, terutama di perguruan tinggi. Hasil penelitian ini diharapkan dapat menjadi referensi bagi penelitian berikutnya dalam memilih framework audit TI sesuai gambar 1 yang sesuai dengan kebutuhan. Terdapat beberapa sub bagian dalam penelitian ini yaitu: Bagian 2 menjelaskan mengenai framework audit TI, Bagian 3 memaparkan terkait metode penelitian, Bagian 4 menjelaskan tentang hasil dan pembahasan, dan Bagian 5 memaparkan mengenai kesimpulan dari artikel ini.



Gambar 1 framework audit TI

II. STUDI PUSTAKA

A. Tata Kelola Teknologi Informasi

Tata Kelola Teknologi Informasi merupakan sebuah proses untuk melakukan pemantauan dan pengendalian keputusan kapabilitas teknologi informasi (TI) dalam memastikan *value delivery* (mengirimkan nilai) kepada pemangku kepentingan utama dalam suatu organisasi [7]. Tata kelola TI yang efektif adalah tata kelola yang bisa membantu instansi agar dapat memastikan bahwa penggunaan TI telah mendukung dan selaras dengan tujuan organisasi, mengoptimalkan investasi TI dan melakukan dokumentasi terhadap keseluruhan proses TI pada suatu organisasi.

B. Audit Teknologi Informasi

Audit sistem informasi atau beberapa kalangan menyebut audit teknologi informasi merupakan sebuah proses pengumpulan dan pengevaluasian terhadap serangkaian bukti untuk dapat menentukan apakah suatu sistem aplikasi komputerisasi telah menerapkan sistem pengendalian internal yang memadai. Tujuan dari audit TI ini adalah untuk menilai apakah pengendalian sistem informasi telah dapat memberikan keyakinan yang memadai atas pengamatan asset, integritas data, efektivitas, serta efisiensi [8].

Terdapat beberapa alasan mengapa audit teknologi informasi ini perlu dilakukan, diantaranya adalah kerugian akibat kehilangan data, kesalahan dalam pengambilan keputusan, risiko kebocoran data, penyalahgunaan komputer, kerugian akibat kesalahan proses perhitungan, serta tingginya nilai investasi perangkat keras dan perangkat lunak komputer [9].

C. Framework Audit Teknologi Informasi

Framework Audit Teknologi Informasi merupakan sebuah kerangka kerja atau panduan yang digunakan oleh auditor untuk melakukan penilaian dan mengevaluasi sistem teknologi informasi, infrastruktur teknologi informasi dan prosedur keamanan yang terkait. Terdapat beberapa jenis *framework* atau model standar audit TI [10], diantaranya:

1. ISO/IEC17799, dikembangkan oleh ISO (*The International Organization for Standardizations*) pada tahun 2000 dan IEC (*The International Electro technical*) yang menyediakan suatu kerangka sebagai standar keamanan informasi. Tujuan utama dari penyusunan standar ini adalah penerapan keamanan informasi dalam organisasi [11].
2. ISO/IEC 27001:2013 adalah standar sistem manajemen keamanan informasi yang diterbitkan pada Oktober 2013 sebagai penyempurnaan dari versi 2005. Sebagai bagian dari keluarga standar ISO/IEC 27000, ISO/IEC 27001:2013 memberikan kerangka kerja untuk pengembangan, implementasi, operasional, pemantauan, peninjauan, dan peningkatan Sistem Manajemen Keamanan Informasi (SMKI). Standar ini terdiri dari 10 klausul, 14 domain kontrol keamanan, 35 kontrol objektif, dan 114 kontrol, memberikan pedoman yang komprehensif untuk manajemen keamanan informasi di organisasi [12].
3. ITIL (*The IT Infrastructure Library*), merupakan kerangka kerja umum yang menggambarkan praktik terbaik dalam manajemen layanan TI. Kerangka kerja ini memberikan struktur bagi tata kelola TI, dengan penekanan pada "pembungkusan layanan" dan fokus pada pengukuran terus-menerus serta perbaikan kualitas layanan TI dari perspektif

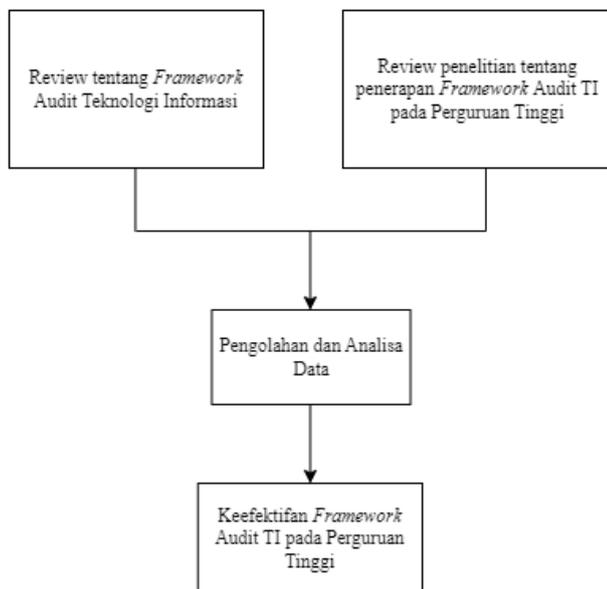
- bisnis dan pelanggan [13]. *Service lifecycle* dalam *Information Technology Infrastructure Library* (ITIL) terdiri atas lima fase domain diantaranya adalah *Domain Service Strategy*, *Domain Service Design*, *Domain Service transition*, *Domain Service Operation* dan *Domain Continual Service Improvement*. *Domain Service Design* adalah fase merumuskan apa yang telah disepakati pada tahap sebelumnya [14]. *Service Transition* merupakan fase pengimplementasian, dan *Service Operation* merupakan fase yang bertumpu pada bagaimana mengelola operasional layanan TI. Fase yang kelima adalah *Continual Service Improvement* digunakan sebagai fase peningkatan pengetahuan dan termasuk mencakup semua fase [15].
4. COSO atau *Committee of Sponsoring Organizations of the Treadway Commission*, dapat diartikan sebagai sebuah badan kolaboratif yang secara khusus fokus pada pemahaman, analisis, dan pengembangan serta penyebaran panduan terkait tata kelola organisasi yang efektif. COSO mengeluarkan suatu kerangka kerja, yaitu COSO ERM, yang terdiri dari delapan komponen utama. Komponen-komponen tersebut mencakup penetapan sasaran, lingkungan pengendalian, identifikasi kejadian, penilaian risiko, tanggapan risiko, aktivitas pengendalian, informasi dan komunikasi, serta pengawasan. Melalui kerangka kerja ini, COSO memberikan landasan yang komprehensif untuk membantu organisasi dalam mengelola risiko, mengoptimalkan pengendalian, dan mencapai tujuan-tujuan yang telah ditetapkan [16].
 5. COBIT, berfungsi sebagai kerangka kerja tata kelola TI yang ditujukan untuk staf layanan TI, manajemen, fungsi audit, dan pemilik proses bisnis. Tujuan utama COBIT 2019 adalah memastikan kerahasiaan, integritas, dan ketersediaan data dan informasi yang kritis dan sensitif. Struktur konseptual ini berasal dari dua prinsip pokok, yakni prinsip yang menjelaskan persyaratan inti dari suatu sistem pengelolaan informasi dan prinsip untuk suatu struktur kerangka pengelolaan yang dapat digunakan untuk merancang sistem pengelolaan bagi suatu perusahaan [17].
 6. CMMI adalah kerangka kerja yang digunakan untuk menilai dan meningkatkan kualitas serta kematangan proses pengembangan perangkat lunak dan sistem dalam sebuah organisasi. Terdiri dari lima tingkat, mulai dari *Level 1 (Initial)* hingga *Level 5 (Optimized)*, CMMI membantu organisasi mengidentifikasi dan meningkatkan kemampuan mereka dalam mengelola dan mengembangkan produk perangkat lunak dan sistem. Melalui penerapan CMMI, organisasi dapat mengukur kematangan proses, mengidentifikasi area perbaikan, dan melakukan perubahan untuk mencapai tingkat kematangan yang lebih tinggi [18].
 7. ISO 20000 adalah standar internasional untuk manajemen layanan TI (ITSM) yang menetapkan praktik terbaik dalam evaluasi efektivitas penyediaan layanan terkelola. Terkait erat dengan ITIL, standar ini melibatkan desain, transisi, pengiriman, dan peningkatan layanan TI. ISO 20000 menekankan pendekatan proses terintegrasi dalam perencanaan, implementasi, operasi, pemantauan, ulasan, pemeliharaan, dan peningkatan *Service Management System* (SMS). Koordinasi yang baik dan penerapan berkelanjutan dari SMS membawa efektivitas dan efisiensi yang lebih besar serta peluang perbaikan terus-menerus. Fokusnya pada operasi proses mensyaratkan koordinasi dan organisasi personal yang efisien. Standar ini bertujuan untuk memastikan penyediaan layanan TI yang terkelola dengan baik, memberikan nilai kepada pelanggan, dan mendukung perbaikan berkelanjutan [19].
 8. TOGAF, yang dikembangkan oleh *The Open Group's Architecture Framework* pada tahun 1995, awalnya bertujuan untuk keamanan Amerika Serikat tetapi sejak itu berkembang menjadi sebuah *framework* yang digunakan di berbagai industri seperti manufaktur, perbankan, dan pendidikan. TOGAF memberikan metode dan alat untuk membangun, merancang, mengimplementasi, dan mengelola arsitektur *enterprise*. Penerapan TOGAF sangat bergantung pada ADM (*Architecture Development Method*), yang digambarkan oleh diagram lingkaran *TOGAF Wheel*, yang menjelaskan beberapa fase kunci dari metode TOGAF ADM [20].
 9. *Holistic Cybersecurity Maturity Assessment Framework* (HCYMAF), adalah suatu panduan evaluasi yang komprehensif untuk menilai tingkat kematangan keamanan siber suatu organisasi. Kerangka kerja ini mencakup identifikasi risiko, perlindungan data, deteksi insiden, respons terhadap serangan, dan pemulihan pasca insiden. Dengan memberikan langkah-langkah sistematis, HCYMAF membantu organisasi mengidentifikasi kelemahan, menerapkan perbaikan, dan meningkatkan ketahanan terhadap ancaman siber, memberikan pendekatan holistik dalam pengelolaan risiko keamanan siber [21].
 10. *CIS Controls*, merupakan kumpulan *best practice* untuk meningkatkan keamanan siber organisasi. Dikembangkan oleh ahli global, kontrol ini memberikan pendekatan yang diprioritaskan untuk mengatasi ancaman umum dan berbahaya. Dengan struktur progresif, setiap kontrol menyediakan rekomendasi tindakan spesifik, mempermudah implementasi dan mengurangi risiko. Diperbarui secara berkala untuk mencerminkan pemahaman terkini tentang ancaman, *CIS Controls* adalah kerangka kerja komprehensif yang dapat diterapkan di berbagai sektor dan ukuran organisasi [22].
 11. *NIST Framework*, adalah panduan yang dikembangkan untuk membantu organisasi dalam mengelola dan mengurangi risiko keamanan Siber. Dengan lima fungsi inti, yaitu Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan, kerangka kerja ini memberikan pendekatan komprehensif untuk memahami dan mengatasi tantangan keamanan Siber. Selain itu, terdapat empat tingkatan untuk menilai tingkat kematangan keamanan Siber suatu organisasi dan memberikan fleksibilitas untuk membuat



profil yang sesuai dengan kebutuhan bisnis dan toleransi risiko. Dengan adopsi luas di berbagai industri, kerangka kerja ini menjadi alat yang berharga untuk meningkatkan ketangguhan keamanan Siber secara global [23]. Framework ini menonjolkan pendekatan fleksibel yang dapat disesuaikan dengan organisasi dari berbagai ukuran dan sektor industri, dengan penekanan pada aplikabilitasnya di sektor-sektor kritis seperti energi, perbankan, komunikasi, dan pertahanan. Departemen Perdagangan Amerika Serikat melalui NIST merilis versi 1.1 dari Cybersecurity Framework untuk meningkatkan ketahanan infrastruktur kritis, dengan fokus perlindungan terhadap keamanan nasional dan ekonomi. Meskipun awalnya ditujukan untuk digunakan oleh agensi federal Amerika Serikat, publikasi khusus NIST telah banyak diadopsi oleh organisasi di seluruh dunia, menunjukkan pengakuan dan aplikabilitas global dari framework tersebut [24].

III. METODOLOGI

Penelitian ini menerapkan metode penelitian studi kepustakaan atau biasa disebut dengan studi literatur (*library research*). Studi literatur dapat dilakukan dengan mengumpulkan referensi yang terdiri dari beberapa penelitian terdahulu yang kemudian dikompilasi untuk menarik sebuah kesimpulan [25]. Dalam penelitian studi literatur memiliki ciri utama yaitu peneliti berhadapan langsung dengan sumber-sumber yang tersedia [26]. Data yang diperoleh didapatkan melalui pengindeks atau mesin pencari seperti Google Scholar, IEEE Xplore, ScienceDirect, ResearchGate, JSTOR, dan Wiley Online Library dari rentang tahun 2019 sampai 2023. Skematik penelitian yang dibahas pada penelitian ini dirancang dengan alur pada Gambar 1.



Gambar 1: Skematik Penelitian

Skematik penelitian ini menjadi pedoman dalam melakukan penelitian ini yang dilakukan melalui beberapa tahapan.

A. Tahapan I

Tahapan pertama dilakukan proses *literature review* tentang *framework* yang digunakan dalam melakukan audit teknologi informasi.

B. Tahapan II

Pada tahapan kedua dilakukan proses pengolahan dan analisa data yang diperoleh dari hasil *literatur review* untuk kemudian dilakukan perbandingan agar dapat diketahui performa dari masing-masing *framework* audit TI yang telah diteliti.

C. Tahapan III

Pada tahapan ketiga ini dilakukan analisa mengenai status penerapan *Framework* audit TI pada Perguruan Tinggi.

IV. HASIL DAN PEMBAHASAN

Berdasarkan hasil dari studi literatur yang diperoleh dari berbagai sumber terkait dengan penelitian terdahulu, maka diperoleh beberapa penelitian yang membahas mengenai penerapan berbagai *framework* audit TI pada Perguruan Tinggi yang dijelaskan sebagai berikut.

Penelitian berjudul *Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu)* mengevaluasi efektivitas *framework* COBIT 2019 dalam meningkatkan tata kelola TI di XYZ-edu. Dengan melakukan serangkaian langkah mulai dari pemetaan tujuan organisasi ke tujuan perusahaan, identifikasi masalah, pengukuran tingkat kematangan, hingga analisis kesenjangan. Penelitian ini memberikan gambaran menyeluruh tentang keadaan tata kelola TI di institusi tersebut. Penggunaan COBIT 2019 sebagai landasan penelitian menjadi langkah kritis karena *framework* ini telah diakui sebagai standar industri yang dapat memberikan panduan yang kuat untuk mengevaluasi dan meningkatkan tata kelola TI. Meskipun *framework* ini membawa nilai positif, hasil penelitian juga menunjukkan tantangan yang dihadapi XYZ-edu dalam mencapai tingkat kematangan yang diinginkan. Kondisi umum menunjukkan tingkat kematangan yang rendah, khususnya dalam area perencanaan, evaluasi, pemantauan, dan dokumentasi kegiatan TI. Analisis kesenjangan menyoroti seberapa besar XYZ-edu harus bergerak untuk mencapai tingkat kematangan yang diinginkan, dan rekomendasi perbaikan selanjutnya memberikan arahan konkret untuk langkah-langkah perbaikan yang dapat diambil. Secara keseluruhan, penelitian ini menyimpulkan bahwa *framework* COBIT 2019 efektif dalam mengidentifikasi kekurangan dan memberikan arahan untuk perbaikan dalam tata kelola TI di XYZ-edu. Namun, tantangan implementasi dan tingkat kematangan yang rendah menunjukkan bahwa perubahan signifikan dan komitmen organisasi diperlukan untuk mencapai tingkat kematangan yang lebih tinggi dan mencapai tujuan tata kelola TI yang diinginkan [27].

Selanjutnya penelitian berjudul *Analysis of Information Technology Governance in The Planning and Organization of E-Learning at Universitas Negeri Malang* yang menggunakan COBIT 4.1 sebagai kerangka kerja untuk mengevaluasi efektivitas implementasi *e-learning* di Universitas Negeri Malang, dengan fokus pada domain perencanaan dan organisasi TI (*Technology Planning and Organization*). Evaluasi tersebut

melibatkan beberapa langkah metodologis, termasuk pengumpulan data melalui wawancara dan kuesioner dengan manajer *e-learning*, dan analisis data menggunakan COBIT 4.1 untuk mengukur tingkat kematangan dalam implementasi berbagai proses. Hasil evaluasi menunjukkan bahwa implementasi *e-learning* di Universitas Negeri Malang, khususnya dalam domain perencanaan dan organisasi TI, masih berada pada tahap awal. Kematangan proses-proses yang terkait, seperti perencanaan strategis TI, arsitektur informasi, dan manajemen investasi TI, umumnya masih rendah. Meskipun beberapa proses mungkin telah dilaksanakan, belum ada kerangka kerja atau kebijakan yang mendukung secara menyeluruh. Dalam menghadapi temuan ini, COBIT 4.1 memberikan panduan yang konkrit dan terstruktur untuk menyusun rekomendasi perbaikan. Rekomendasi tersebut mencakup pengembangan rencana strategis untuk *e-learning*, peningkatan manajemen sumber daya manusia, perbaikan dalam manajemen investasi TI, dan pendefinisian kebijakan dan prosedur yang lebih ketat dalam konteks *e-learning*. Secara keseluruhan, efektivitas COBIT 4.1 dalam penelitian ini terletak pada kemampuannya untuk mengidentifikasi dan mengukur tingkat kematangan implementasi *e-learning*, memberikan panduan konkret untuk perbaikan, dan memberikan dasar yang kuat untuk pengelolaan teknologi informasi yang lebih baik di lingkungan akademis. Dengan mengikuti kerangka kerja ini, Universitas Negeri Malang dapat mengambil langkah-langkah yang terukur dan terarah untuk meningkatkan efektivitas dan keseluruhan kematangan implementasi *e-learning* mereka [28].

Penelitian selanjutnya dengan judul *Audit Information Systems in Digilib University of Uin Sunan Ampel Surabaya Using COBIT Framework 4.1*. Dalam penelitian ini, *framework* COBIT 4.1 telah membuktikan efektivitasnya sebagai alat yang sangat berharga dalam melakukan audit terhadap sistem informasi Digilib di Universitas Islam Negeri Sunan Ampel Surabaya (UINSA). Pertama, COBIT memberikan landasan yang kokoh dengan membagi proses ke dalam domain-domain yang jelas, seperti manajemen kinerja, keamanan sistem, dan pengelolaan investasi TI. Hal ini memungkinkan peneliti untuk fokus pada aspek-aspek kritis yang relevan dengan tujuan penelitian. Panduan yang disediakan oleh COBIT juga membantu peneliti dalam memahami dan mengidentifikasi proses-proses yang membutuhkan perhatian khusus. Kedua, COBIT 4.1 membantu dalam menilai kematangan proses-proses kunci yang ada pada sistem Digilib. Dengan menggunakan *framework* ini, peneliti dapat melakukan evaluasi mendalam terhadap bagaimana proses-proses tersebut dikelola dan sejauh mana tingkat kematangan yang telah dicapai. Hal ini memberikan wawasan yang berharga terkait dengan efisiensi operasional, keamanan, dan kesiapan sistem dalam mencapai tujuan organisasi. Ketiga, COBIT memberikan kerangka kerja yang standar dan terukur untuk merancang rekomendasi perbaikan. Dengan mengacu pada indikator kematangan yang telah ditetapkan, peneliti dapat merancang rekomendasi yang

spesifik dan dapat diukur. COBIT membantu peneliti untuk mengidentifikasi kesenjangan antara kondisi saat ini dan tingkat kematangan yang diinginkan, serta menyusun langkah-langkah konkret untuk mencapainya. Dengan demikian, efektivitas COBIT 4.1 dalam penelitian ini dapat dilihat dari kontribusinya dalam menyediakan landasan yang kuat, menyeluruh, dan terukur untuk melakukan audit dan perbaikan pada sistem informasi Digilib di lingkungan akademik UINSA [29].

Selanjutnya dalam penelitian berjudul *A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom*, efektivitas *framework* yang diusulkan, yaitu *Holistic Cybersecurity Maturity Assessment Framework (HCYMAF)*, sangat mencolok dalam memberikan solusi yang komprehensif dan terukur untuk mengevaluasi kematangan keamanan siber di lembaga pendidikan tinggi (HEIs) di Inggris [30]. Pengintegrasian berbagai model dan standar keamanan siber seperti CMMI, ISO/IEC 27001, CIS Controls, NIST Framework, serta regulasi seperti GDPR, PCI DSS, dan DSPT, memberikan landasan yang solid dan terpadu. HCYMAF mengatasi gap dalam literatur keamanan siber dengan menawarkan pandangan holistik yang mencakup kontrol teknis dan kepatuhan regulasi. Salah satu keunggulan HCYMAF terletak pada kemampuannya untuk memberikan pandangan yang komprehensif terhadap tingkat kematangan keamanan siber di berbagai domain, dengan menggunakan enam tingkatan kematangan yang dapat diukur [31]. Dengan memasukkan perspektif regulasi yang beragam, HCYMAF membantu HEIs dalam memahami dan memenuhi persyaratan hukum dan keamanan yang relevan. Hasil validasi melalui wawancara dan studi kasus dengan ahli keamanan dan *data protection officers* di HEIs menguatkan relevansi dan daya terima *framework* ini dalam konteks praktis. Kemampuannya untuk memberikan laporan otomatis dan representasi grafis terhadap tingkat kematangan serta rekomendasi perbaikan memberikan nilai tambah signifikan dalam mendukung lembaga pendidikan tinggi untuk mengelola dan meningkatkan keamanan siber mereka [32]. Dengan demikian, HCYMAF berhasil menciptakan solusi yang dapat membantu organisasi dalam menghadapi tantangan kompleks keamanan siber dan memastikan kesiapan mereka terhadap ancaman yang berkembang.

Penelitian selanjutnya dengan judul *Managing Cyber Hygiene at a Higher Education Institution in the United States*, yang mengeksplorasi pengelolaan dan evaluasi tingkat kebersihan siber di institusi pendidikan tinggi di Amerika Serikat, khususnya pada *Savannah State University (SSU)*. Dalam konteks ini, *Holistic Cybersecurity Maturity Assessment Framework (HCYMAF)* digunakan sebagai alat utama untuk mengukur dan mengelola kebersihan dan kematangan siber. Penelitian ini menyoroti tantangan dan kebutuhan institusi pendidikan tinggi dalam mengelola kebersihan siber, terutama dalam konteks SSU, dan memberikan rekomendasi spesifik untuk meningkatkan tingkat kematangan keamanan siber. Dengan menggunakan HCYMAF, penelitian ini mencapai



pemahaman mendalam tentang keberhasilan SSU dalam mematuhi standar kebijakan keamanan siber, serta mengidentifikasi peluang perbaikan untuk mencapai kematangan yang lebih tinggi. Hasil penelitian memberikan kontribusi terhadap literatur keamanan siber di pendidikan tinggi dan memberikan landasan bagi institusi pendidikan tinggi lainnya di Amerika Serikat untuk memperbaiki dan meningkatkan efektivitas kebijakan dan praktik keamanan siber mereka [33].

Penelitian berjudul *Audit Keamanan Sistem Informasi Menggunakan ISO/IEC 27002:2013 Pada Universitas XXX*, secara efektif menerapkan *framework* ISO/IEC 27002:2013 untuk mengaudit dan meningkatkan keamanan sistem informasi di Universitas XXX. *Framework* tersebut memberikan landasan yang kuat untuk mengevaluasi sejauh mana universitas telah mengadopsi praktik keamanan informasi yang sesuai. Dengan merinci 14 kontrol keamanan, penelitian ini dapat mengidentifikasi kelemahan konkret dalam implementasi kebijakan keamanan yang masih belum sesuai dengan standar yang ditetapkan. Hal ini memungkinkan peneliti memberikan rekomendasi yang tepat untuk perbaikan, memberikan nilai tambah dalam hal memberikan solusi konkret untuk meningkatkan keamanan sistem informasi di universitas. Rekomendasi hasil penelitian membuktikan bahwa *framework* ISO/IEC 27002:2013 tidak hanya berfungsi sebagai alat evaluasi, tetapi juga sebagai panduan tindakan yang praktis. Dengan menyoroti kontrol keamanan yang perlu diperbaiki, penelitian ini memberikan arah yang jelas untuk langkah-langkah perbaikan yang dapat diambil universitas. Selain itu, *framework* ini membuktikan keandalannya dalam menilai tingkat kematangan keamanan sistem informasi, dengan menetapkan universitas pada tingkat 2 (*managed*). Ini menunjukkan bahwa universitas telah mencapai tingkat pengelolaan yang memadai, tetapi masih memiliki ruang untuk peningkatan yang lebih lanjut. Selanjutnya, implementasi *framework* ini memberikan kontribusi berharga dalam pengembangan pemahaman umum mengenai keamanan informasi di lingkungan pendidikan tinggi. Dengan menonjolkan perbedaan versi standar, penelitian ini membuktikan keunggulan penerapan ISO/IEC 27002:2013 dibandingkan dengan versi sebelumnya. Kesimpulannya, efektivitas *framework* ini terletak pada kemampuannya memberikan gambaran menyeluruh, rekomendasi tindakan konkret, dan pemahaman yang lebih dalam terkait kematangan keamanan sistem informasi di universitas [34].

Penelitian dengan judul *The role of the modern COSO framework in evaluating the internal control system through the mediating role of the internal auditor: (Al-Muthanna State University as a model)*, secara konkret mengeksplorasi bagaimana *framework* COSO modern berperan dalam mengevaluasi sistem pengendalian internal di konteks Al-Muthanna State University. Temuan penelitian menunjukkan bahwa penggunaan COSO sebagai landasan metodologis dalam penilaian sistem pengendalian internal universitas memberikan kontribusi signifikan terhadap peningkatan efektivitas dan efisiensi operasional. Dalam konteks spesifik universitas ini, COSO membantu mengenali area-area di mana pengendalian internal dapat ditingkatkan, serta mengevaluasi kinerja dan efektivitas auditor internal sebagai perantara yang memainkan peran penting dalam mengimplementasikan prinsip-prinsip

COSO. Melalui mediasi auditor internal, implementasi *framework* COSO dapat diintegrasikan secara lebih efektif dalam kebijakan dan praktik internal universitas, meningkatkan pemahaman dan kesesuaian dengan standar kontrol internal yang relevan. Secara keseluruhan, penelitian ini menggambarkan peran krusial COSO dalam konteks evaluasi *internal control system* di Al-Muthanna State University, yang dijelaskan melalui mediator auditor internal. Melalui pendekatan ini, penelitian ini memberikan pemahaman yang lebih mendalam tentang bagaimana *framework* COSO memengaruhi dan meningkatkan tata kelola internal di institusi pendidikan tinggi [35].

Dalam konteks penelitian *Development of Website Service Governance at the Muhammadiyah University Palembang Using the ITIL V3 Method*, penggunaan *framework* ITIL (*Information Technology Infrastructure Library*) menunjukkan efektivitasnya dalam memperbaiki dan mengelola layanan situs web universitas. ITIL V3 memberikan pendekatan sistematis terhadap manajemen layanan IT, dengan memfokuskan pada lima aspek utama yaitu strategi layanan, desain layanan, transisi layanan, operasi layanan, dan peningkatan layanan. Dengan mengadopsi prinsip-prinsip ITIL V3, universitas dapat meningkatkan efisiensi operasional, meningkatkan pengelolaan kapasitas, dan meningkatkan tingkat kepuasan pengguna layanan situs web. Penerapan ITIL V3 tidak hanya meningkatkan kualitas layanan, tetapi juga membantu universitas dalam menangani masalah-masalah umum yang dihadapi, seperti standar data, ketersediaan sistem, dan beban pengguna. Selain itu, *framework* ini memberikan arahan untuk memprioritaskan proses layanan yang perlu diperbaiki, seperti manajemen katalog layanan, manajemen tingkat layanan, dan manajemen pemasok. Dengan demikian, judul penelitian mencerminkan pendekatan holistik terhadap peningkatan tata kelola layanan situs web di Universitas Muhammadiyah Palembang, yang melibatkan implementasi ITIL V3 sebagai metodologi utama. Keseluruhan, penerapan ITIL V3 dapat memperkuat tata kelola layanan teknologi informasi di universitas, membawa manfaat bagi pengguna layanan dan mendukung pencapaian tujuan institusi dalam era digital [36].

Penelitian lainnya berjudul *Planning of Higher Education Information Technology Strategy Using TOGAF (A Case Study at AMN Cilacap)*, memberikan kontribusi penting terhadap perencanaan strategis teknologi informasi di lembaga pendidikan tinggi. Dengan mengadopsi pendekatan TOGAF, penelitian ini membantu merumuskan strategi yang tepat untuk pengembangan dan pemanfaatan teknologi informasi di AMN Cilacap. Hasil penelitian memberikan pemahaman mendalam tentang keadaan internal lembaga, menyoroti kekuatan dan kelemahan, serta peluang dan tantangan yang dihadapi dalam menghadapi persaingan yang semakin ketat. Dengan menganalisis *value chain* dan menerapkan konsep SWOT, penelitian ini menciptakan pandangan yang komprehensif tentang cara integrasi teknologi informasi dapat mendukung visi dan misi AMN Cilacap. Selain itu, TOGAF memberikan pandangan arsitektur perusahaan yang terinci, mencakup berbagai aspek seperti penerimaan mahasiswa baru, arsitektur bisnis akademis, arsitektur bisnis lulusan, hingga arsitektur keuangan dan infrastruktur. Dengan menggunakan metode *Structural Equation Modeling* (SEM), data yang terkumpul

divalidasi secara ilmiah untuk memastikan keakuratan hasil. Oleh karena itu, penelitian ini memberikan landasan kuat untuk pengambilan keputusan di tingkat manajerial, dengan menyusun panduan implementasi teknologi informasi yang berkelanjutan untuk meningkatkan daya saing dan memenuhi tuntutan masa depan di AMN Cilacap [37].

Penelitian *Developing Enterprise Architecture Using TOGAF 9.1 for IT Master Plan in the Graduate Program of Institute of Informatics and Business Darmajaya*, menekankan penggunaan TOGAF 9.1 sebagai kerangka kerja yang efektif untuk merancang *Master Plan* Teknologi Informasi (TI). Fokusnya adalah mengidentifikasi risiko tinggi terkait pengelolaan dan keamanan data di Program Pascasarjana IIB Darmajaya, yang memicu kebutuhan mendesak akan dukungan TI yang optimal. Studi ini menguraikan fase-fase TOGAF, mulai dari tahap awal hingga perancangan arsitektur teknologi, membentuk panduan pengembangan TI yang sesuai dengan kebutuhan pengguna dan meningkatkan efektivitas implementasi TI. Penerapan TOGAF dalam penelitian ini menghasilkan arsitektur perusahaan yang terinci, mencakup proses bisnis utama seperti Manajemen Keuangan, Proses Akademis, Pengelolaan Data, dan Manajemen Teknologi Informasi. Dengan menggunakan pemodelan bisnis, analisis kesenjangan, dan penilaian kebutuhan bisnis, TOGAF memberikan landasan strategis untuk mengembangkan rencana TI yang terarah dan berkelanjutan. Kesimpulan penelitian menegaskan bahwa TOGAF 9.1 berperan signifikan dalam mengarahkan strategi TI di Program Pascasarjana IIB Darmajaya, membantu meningkatkan kualitas layanan, serta memastikan keamanan data sesuai dengan tujuan institusi [38].

Penelitian selanjutnya berjudul *Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)*, secara efektif memanfaatkan pendekatan CMMI untuk mengevaluasi dan meningkatkan tingkat kematangan keamanan Sistem Informasi Akademik (SIA) di Universitas Ahmad Dahlan. Dalam penelitian ini, CMMI digunakan sebagai alat analisis yang merinci tingkat kematangan menggunakan *framework* COBIT 5, terutama pada *domain* DSS05. Hasil penelitian menunjukkan bahwa penerapan CMMI berhasil menghasilkan *Maturity Level* sebesar 4,458, mencerminkan tingkat keamanan SIA yang terkelola dan dapat diukur. Oleh karena itu, penelitian ini menunjukkan efektivitas CMMI sebagai metode evaluasi yang berhasil digunakan untuk meningkatkan keamanan SIA di lingkungan pendidikan tinggi, sesuai dengan fokus penelitian yang tercantum dalam judulnya [39].

Penelitian terakhir yang berjudul *Framework Information Technology Infrastructure Library (ITIL V3): Audit Teknologi Informasi Sistem Informasi Akademik (Siakad) Perguruan Tinggi*, menyajikan analisis efektivitas penerapan *Framework Information Technology Infrastructure Library (ITIL V3)* pada Sistem Informasi Akademik (Siakad) di XYZ University. Metode penelitian melibatkan beberapa tahap, termasuk identifikasi masalah, studi literatur, pengumpulan data melalui

observasi, wawancara, dan kuesioner menggunakan instrumen ITIL V3, serta verifikasi, validasi, dan penyusunan laporan audit. Hasil perhitungan tingkat kematangan (*Maturity Level*) menunjukkan bahwa XYZ University telah mencapai tingkat kematangan yang tinggi, terutama pada *domain Continuous Service Improvement (CSI)* dengan nilai 4,09 pada level 4 (*Managed and Measureable*). Temuan ini mengindikasikan bahwa perguruan tinggi mampu mengukur dan memonitor prosedur yang ada dengan baik, memungkinkan penanggulangan yang efektif jika terjadi penyimpangan, dan proses yang ada berjalan dengan baik dan konsisten. Analisis kesenjangan (*Gap Analysis*) menyoroti bahwa nilai rata-rata *gap* sebesar 0,73, menunjukkan bahwa penerapan layanan TI di XYZ University sangat baik. Rekomendasi yang dihasilkan fokus pada pemeliharaan dan perbaikan layanan TI yang sudah ada, serta perlunya evaluasi berkala untuk perbaikan berkelanjutan. Perguruan tinggi dianjurkan untuk memberikan kemudahan akses layanan TI di mana saja, bahkan melalui perangkat *mobile*, sekaligus melakukan review terhadap pengembangan layanan IT berdasarkan hasil uji coba. Secara keseluruhan, penelitian menyimpulkan bahwa XYZ University telah berhasil menerapkan layanan teknologi informasi dengan baik, dengan ITIL V3 memberikan kerangka kerja yang efektif untuk pengukuran dan peningkatan kualitas layanan TI. Evaluasi yang berkala dan pemeliharaan tingkat kematangan yang tinggi merupakan kunci keberhasilan dalam mendukung kegiatan akademik di perguruan tinggi tersebut [40].

V. KESIMPULAN

Berdasarkan hasil penelitian yang disajikan mengindikasikan bahwa berbagai *framework* audit IT memiliki efektivitas dalam meningkatkan tata kelola dan keamanan sistem informasi di berbagai lembaga pendidikan tinggi. Berikut adalah kesimpulan mengenai keefektifan masing-masing *framework*:

1. COBIT 2019
COBIT 2019 terbukti efektif dalam mengidentifikasi kekurangan dan memberikan panduan perbaikan dalam tata kelola TI. Meskipun memberikan nilai positif, tantangan implementasi dan tingkat kematangan rendah menunjukkan perlunya perubahan signifikan dan komitmen organisasi untuk mencapai tingkat kematangan yang diinginkan.
2. COBIT 4.1
COBIT 4.1 efektif dalam mengidentifikasi dan mengukur tingkat kematangan implementasi e-learning. Memberikan panduan konkret untuk perbaikan dan dasar yang kuat untuk pengelolaan teknologi informasi yang lebih baik di lingkungan akademis.
3. HCYMAF (*Holistic Cybersecurity Maturity Assessment Framework*)
HCYMAF efektif dalam menciptakan solusi komprehensif dan terukur untuk mengevaluasi kematangan keamanan siber di lembaga pendidikan tinggi. Terintegrasi dengan berbagai model dan standar keamanan siber serta regulasi,



memberikan pandangan holistik yang mencakup kontrol teknis dan kepatuhan regulasi.

4. ISO/IEC 27002:2013

Framework ini efektif dalam mengaudit dan meningkatkan keamanan sistem informasi di universitas. Memberikan gambaran menyeluruh, rekomendasi tindakan konkret, dan pemahaman yang lebih dalam terkait kematangan keamanan sistem informasi.

5. COSO Framework

COSO Framework membantu meningkatkan efektivitas dan efisiensi operasional di Al-Muthanna State University. Dalam konteks auditor internal, COSO membantu mengevaluasi kinerja dan efektivitas auditor internal, serta berkontribusi pada peningkatan tata kelola internal.

6. ITIL V3

ITIL V3 membuktikan efektivitasnya dalam memperbaiki dan mengelola layanan situs web universitas, serta dalam meningkatkan tata kelola layanan teknologi informasi. Memberikan pendekatan sistematis terhadap manajemen layanan IT. Penerapan ITIL V3 dapat memperkuat tata kelola layanan teknologi informasi di universitas, serta mendukung pencapaian tujuan institusi dalam era digital.

7. TOGAF

Framework TOGAF efektif dalam menyediakan panduan komprehensif untuk mengembangkan dan mengelola arsitektur informasi perusahaan. Dengan pendekatan yang terstruktur dan metodologi yang dapat diadaptasi, TOGAF membantu organisasi menyelaraskan strategi bisnis dengan infrastruktur TI, meningkatkan fleksibilitas sistem, dan meminimalkan risiko dalam pengembangan solusi TI.

8. CMMI

Dalam penelitian yang ditinjau menunjukkan efektivitas CMMI sebagai metode evaluasi yang berhasil digunakan untuk meningkatkan keamanan SIA di lingkungan pendidikan tinggi, sesuai dengan fokus penelitian yang tercantum dalam judulnya.

Setelah melihat hasil dari berbagai *framework* audit IT, tidak dapat secara mutlak menyatakan bahwa satu *framework* lebih baik daripada yang lain. Pilihan *framework* tergantung pada kebutuhan, sumber daya, dan tujuan spesifik lembaga pendidikan tinggi. Masing-masing *framework* memberikan kontribusi yang berharga untuk meningkatkan tata kelola TI, keamanan sistem informasi, dan kepuasan pengguna.

REFERENSI

- [1] Ian Lloyd, *Information Technology Law*. Oxford University Press, 2020. [Online]. Available: https://books.google.co.id/books?hl=id&lr=&id=rKXaDwAAQBAJ&oi=fnd&pg=PP1&dq=Information+Technology+impact+on+daily+life%22&ots=iVyOm_mW8D&sig=BtRLXM3rS3Gd7XZz_I4L7RPDoSw&redir_esc=y#v=onepage&q=Information+Technology+impact+on+daily+life%22&f=false
- [2] L. Harahap, "Prosiding Seminar Nasional Teknologi Pendidikan Pascasarjana UNIMED PERAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DALAM PENDIDIKAN," pp. 375–381, 2019.
- [3] R. P. Kusuma, "Audit Teknologi Informasi Menggunakan Framework Cobit 5 Pada Domain Dss (Deliver, Service, and Support) (Studi Kasus : Konsultan Manajemen Pusat)," *J. Digit*, vol. 9, no. 1, p. 97, 2020, doi: 10.51920/jd.v9i1.137.
- [4] N. D. Ramadhani, W. H. N. Putra, and A. D. Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 5, pp. 1490–1498, 2020, [Online]. Available: <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7259>
- [5] M. Muthmainnah, D. Yulisda, and V. Ilhadi, "Academic Information System Audit Using Cobit 5 Domain APO Framework," *Int. J. Eng. Sci. Inf. Technol.*, vol. 2, no. 1, pp. 123–130, 2021, doi: 10.52088/ijesty.v2i1.223.
- [6] I. P. Windasari, A. F. Rochim, S. N. Alfiani, and A. Kamalia, "Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019," *J. Sist. Info. Bisnis*, vol. 11, no. 2, pp. 131–138, 2022, doi: 10.21456/vol11iss2pp131-138.
- [7] F. Muttaqin, M. Idhom, F. A. Akbar, M. H. P. Swari, and E. D. Putri, "Measurement of the IT Helpdesk Capability Level Using the COBIT 5 Framework," *J. Phys. Conf. Ser.*, vol. 1569, no. 2, pp. 39–46, 2020, doi: 10.1088/1742-6596/1569/2/022039.
- [8] C. K. Sastradipraja, "Rancang Bangun Simulasi Tool Sistem Audit Teknologi Informasi Berbasis Web," *J. Ris. Sist. Inf. dan Teknol. Inf.*, vol. 2, no. 1, pp. 46–58, 2020, doi: 10.52005/jursistekni.v2i1.38.
- [9] D. M. Elisabeth, "Kajian Terhadap Peranan Teknologi Informasi Dalam Perkembangan Audit Komputerisasi (Studi Kajian Teoritis)," *METHOMIKA J. Manaj. Inform. Komputerisasi Akunt.*, vol. 3, no. 1, pp. 40–53, 2019.
- [10] M. S. Dr. Ir. Sumijan and M. K. Pradani Ayu Widya Purnama, S.Kom., *Audit Teknologi Informasi Penerapan Pada E-Government (Best Practice e-government Pemerintah Kota)*. PENERBIT INSAN CENDEKIA MANDIRI, 2020.
- [11] A. Y. El-Bably, "Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management," *J. Inf. Secur. Cybercrimes Res.*, vol. 4, no. 1, pp. 95–102, 2021, doi: 10.26735/wlpw6121.
- [12] S. Rif and R. Bisma, "Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO / IEC 27001 : 2013 dan ISO / IEC 27002 : 2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun," *JEISBI Vol. 01 Nomor 01, 2020 (Journal Emerg. Inf. Syst. Bus. Intell. Pembuatan)*, vol. 01, pp. 43–50, 2020.
- [13] R. R. Rahmawati and Y. Prihadi, "Tata Kelola Keamanan Informasi Layanan Ti Menggunakan Framework Itil V3 Domain Service Design Di Lingkungan Smkn 4 ...," *Sci. Regendi*, vol. 2, pp. 116–131, 2021, [Online]. Available: <http://journal.unla.ac.id/index.php/scientiaregendi/article/view/1664>
- [14] I. P. Ramayasa, "Penerapan Framework Itil V3 Dalam Analisis Tata Kelola Sistem Informasi Layanan Akademik Domain Service Transition," *J. Teknol. Inf. dan Komput.*, vol. 06, no. 02, pp. 134–141, 2020.
- [15] S. S. Hilabi *et al.*, "TechnoXplore Jurnal Ilmu Komputer & Teknologi Informasi ISSN : 2503-054X Vol 4 No: 1, April 2019," *J. Ilmu Komput. Teknol. Inf.*, vol. 4, no. 1, pp. 28–37, 2019.
- [16] Kurniawati and J. B. Armiranto, "Peran Audit Internal atas Persediaan Barang dagangan berbasis COSO Framawork Pada CV. Zidan Jaya Surabaya," *J. Ris. Ilmu Akunt.*, vol. 2, no. 1, pp. 218–231, 2023.
- [17] R. K. Jaya and M. I. Fianty, "IT Project Management Control and The Control Objectives for IT and Related Technology COBIT 2019 Framework," *Indones. J. Comput. Sci.*, vol. 12, no. 2, pp. 284–301, 2023, doi: <https://doi.org/10.33022/ijcs.v12i1.3135>.
- [18] A. A. P. Ardyanti, D. B. Rarasati, P. Jen, P. R. Hon, and B. Hakim, "Analisis Penerapan Framework COBIT 5 Pada Tingkat Kesiapan Sistem Pemantauan PT. ATW Solar," *JBASE - J. Bus. Audit Inf. Syst.*, vol. 6, no. 2, pp. 16–25, 2023, doi: 10.30813/jbase.v6i2.4671.
- [19] A. N. Priyohutomo and M. N. N. Sitokdana, "Dampak Implementasi Iso/Iec 20000 Pada Perusahaan Pt. Visionet Data Internasional," *Sebatik*, vol. 24, no. 1, pp. 29–36, 2020, doi: 10.46984/sebatik.v24i1.923.
- [20] R. Anderson and J. F. Andry, "Perancangan Enterprise Arsitektur Menggunakan Framework Togaf (Studi Kasus PT. Ikido Jorr Sepatu Indo)," *Ultim. InfoSys J. Ilmu Sist. Inf.*, vol. 12, no. 1, pp. 58–66,

- [21] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, pp. 1–26, 2021, doi: 10.7717/peerj-cs.703.
- [22] T. Muhammad, M. T. Munir, M. Z. Munir, and M. W. Zafar, "Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future," *Int. J. Comput. Sci. Technol.*, vol. 6, no. 4, pp. 99–135, 2022, [Online]. Available: <https://ijcst.com.pk/IJCST/article/view/274>
- [23] A. O. Gopstein Cuong Nguyen Cheyney and F. Nelson Hastings David Wollman, "DRAFT NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0," pp. 2–228, 2020.
- [24] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 3, pp. 417–432, 2020, doi: 10.17762/ijcnis.v12i3.4817.
- [25] A. Febriani, D. C. Lubis, K. M. Parapat, and ..., "Meningkatkan Keterampilan Menyimak Anak Usia SD di Kelas Tinggi melalui Pembelajaran STEAM dengan Media Cerita Animasi," ... *Dunia J. Ris.* ..., vol. 2, no. 3, 2023, [Online]. Available: <https://journal.unimar-amni.ac.id/index.php/insdun/article/view/990%0Ahttps://journal.unimar-amni.ac.id/index.php/insdun/article/download/990/806>
- [26] S. Khairunnisa and T. A. Aziz, "Studi Literatur: Digitalisasi Dunia Pendidikan dengan Menggunakan Teknologi Augmented Reality pada Pembelajaran Matematika," *J. Ris. Pendidik. Mat. Jakarta*, vol. 3, no. 2, pp. 53–62, 2021, doi: 10.21009/jrpmj.v3i2.22267.
- [27] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, "Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu)," *2020 3rd Int. Conf. Comput. Informatics Eng. IC2IE 2020*, no. December, pp. 236–241, 2020, doi: 10.1109/IC2IE50715.2020.9274599.
- [28] E. Sutadji, W. N. Hidayat, S. Patmanthara, S. Sulton, N. A. M. Jabari, and M. Irsyad, "Analysis of information technology governance in the planning and organization of e-learning at Universitas Negeri Malang," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 732, no. 1, pp. 0–7, 2020, doi: 10.1088/1757-899X/732/1/012114.
- [29] W. Verronica S, R. B. Prakoso, and Ilham, "Audit information systems in digilib university of UIN sunan ampel surabaya using cobit framework 4.1," *Libr. Philos. Pract.*, vol. 2019, 2019.
- [30] A. Aliyu *et al.*, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Appl. Sci.*, vol. 10, no. 10, 2020, doi: 10.3390/app10103660.
- [31] L. Maglaras, I. Kantzavelou, and M. A. Ferrag, "Digital transformation and cybersecurity of critical infrastructures," *Appl. Sci.*, vol. 11, no. 18, pp. 4–8, 2021, doi: 10.3390/app11188357.
- [32] K. Kim, F. A. Alfouzan, and H. Kim, "Cyber-attack scoring model based on the offensive cybersecurity framework," *Appl. Sci.*, vol. 11, no. 16, 2021, doi: 10.3390/app11167738.
- [33] S. C. and B. Lamar, "MANAGING CYBER HYGIENE AT A HIGHER EDUCATION INSTITUTION IN THE UNITED STATES," *Assoc. Inf. Syst. AIS Electron. Libr.*, 2022.
- [34] R. Santi, A. I. Alfresi, and B. Octariana, "Information System Security Audit Using Iso/Iec 27002:2013 At University of Xxx," *J. Tek. Inform.*, vol. 4, no. 4, pp. 733–750, 2023, doi: 10.52436/1.jutif.2023.4.4.689.
- [35] W. H. Abd, A. D. Kareem, and E. E. Jassim, "The role of the modern COSO framework in evaluating the internal control system through the mediating role of the internal auditor: (Al-Muthanna State University as a model)," *Res Mil.*, vol. 12, no. 2, pp. 4376–4391, 2022.
- [36] K. Muhammad, W. Hidayat, W. Cholil, and T. B. Kurniawan, "Development of Website Service Governance at the Muhammadiyah University Palembang Using the ITIL V3 Method," *J. DATA Sci.*, vol. 2022:15, no. November, 2022.
- [37] O. T. Prayitno, "Planning of Higher Education Information Technology Strategy Using TOGAF (A Case Study at AMN Cilacap)," *Indones. J. Inf. Syst.*, vol. 2, no. 1, pp. 67–79, 2019, doi: 10.24002/ijis.v2i1.2349.
- [38] S. Sutedi and N. Handayani, "Developing Enterprise Architecture Using Togaf 9.1 for It Master Plan in the Graduate Program of Institute of Informatics and Business Darmajaya," *Int. Conf.*, no. December, pp. 110–120, 2020.
- [39] E. Handoyo, R. Umar, and I. Riadi, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)," *Sci. J. Informatics*, vol. 6, no. 2, pp. 193–202, 2019, doi: 10.15294/sji.v6i2.17387.
- [40] R. D. Handayani and R. A. Aziz, "Framework Information Technology Infrastructure Library (Itil V3): Audit Teknologi Informasi Sistem Informasi Akademik (Siakad) Perguruan Tinggi," *Explor. J. Sist. Inf. dan Telemat.*, vol. 11, no. 1, p. 29, 2020, doi: 10.36448/jsit.v11i1.1456.



{Halaman ini sengaja dikosongkan}