BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

Melalui teknik komparasi literatur yang sistematis, peneliti mampu memetakan *state-of-the-art* dari perkembangan teknologi dan metodologi terkini, seperti evolusi standar keamanan informasi atau efektivitas berbagai framework arsitektur enterprise. Dengan mengenali limitasi pada Penelitian literatur terdahulu, penelitian ini dapat memosisikan diri secara strategis, baik dalam bentuk adaptasi standart keamanan informasi maupun penyelesaian masalah spesifik yang belum tertangani, sehingga kontribusi terhadap pengembangan ilmu pengetahuan di bidang teknologi informasi dapat terdefinisi secara distingtif.

2.1. Tinjauan Pustaka

Tinjauan Pustaka pada Tabel 2.1 dibawah ini memberikan pandangan dari berbagai penelitian terdahulu yang memiliki topik sepura dengan relevansi penelitian terhadap keamanan informasi. Penelitian ini memiliki topik "Analisa Keamanan Informasi Pada Sistem Informasi Pesantren Sesuai Standart ISO/IEC 27001:2022 Dan *Framework* Togaf" menggunakan penelitian terdahulu seperti pada Tabel 2.1 sebagai acuan dalam penelitian yang dilakukan.

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
1	*"Enterprise Architecture Data Management for Digital Transformation - A Higher Education Institute (HEI) Case"*	Aditi S. Divatia dan Jyoti Jagasia Communicatios of the Association for Information Systems (CAIS) (2025) (Divatia & Jagasia, 2025)	Permasalahan utama yang dibahas dalam studi kasus Institut Vidya Vinay (VVI) adalah kekacauan data dan aplikasi yang menghambat visi transformasi digital institusi untuk meningkatkan skala dan menawarkan program inovatif.	Kerangka Kerja (*Framework*) The Open Group Architecture Framework (TOGAF)	Hasil dari penelitian ini adalah Arah Strategis yang disepakat meliputi keputusan untuk meluncurkan program online guna meningkatkan skala institusi (*scale up*) dan rencana masa depan untuk menggunakan platform teknologi milik sendiri untuk *fleksibilita*s. Kemudian Kebutuhan Tata Kelola Data (Data *Governance*) yang kuat dengan memastikan aliran data yang lancar (*seamless data flow*) dan kepatuhan terhadap regulasi baru. Serta Fokus Arsitektur Lanjutan yaitu Penentuan serangkaian

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
					pertanyaan kunci yang harus dijawab untuk merancang arsitektur baru
2	*"Towards a digital platform for performance management and systemic improvement of education systems: evidence from Morocco"*	Hind Benlhabib. Abdelaziz Berrado Discover Education, Springer Naturer (2024) (Benlhabib & Berrado, 2025)	Permasalahan ditemukan adalah keterbatasan peran Sistem Informasi dalam pendidikan, di mana perannya secara konvensional hanya terbatas pada pengelolaan teknis indikator kinerja. Akibatnya, potensi transformatif IS di tingkat individu, institusi, dan sistemik tidak dimaksimalkan.	Metode TOGAF (The Open Group Architecture Framework) dan DSR (Design Science Research)	Berhasil merancang dan mendefinisikan *Arsitektur Platform* Digital PMSIE yang komprehensif. Platform ini dikonfirmasi dapat memaksimalkan potensi transformatif Sistem Informasi dan mendukung peningkatan sistemik dalam reformasi pendidikan, divalidasi melalui artefak EA pada studi kasus Pendidikan di Maroko.
3	*A Blockchain-Based Framework for Secure Information*	Mohd Shukri, S.B. Goyal, Deepmala Singh Journal of Logistics,	Permasalahan utama adalah belum adanya untuk menjamin keamanan (*security*), privasi (*privacy*), dan keakuratan (*accuracy*) pertukaran informasi dalam	Smart Contracts dan Enkripsi, Algoritma Proof of Resource Availability	Hasil analisis data berbasis simulasi menunjukkan bahwa kerangka kerja yang diusulkan mengungguli pendekatan yang sudah

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
	Exchange in Digital Governance Systems using Proof of Resource Availability	Informatics and Service Science (2024) (Shukri dkk., 2024)	sistem tata kelola digital (digital *governance*). Sistem sebelumnya sangat rentan karena masih menggunakan basis data terpusat (*centralized databases*), yang mudah menjadi sasaran serangan siber, pelanggaran data, dan manipulasi informasi sensitif. Selain itu, belum ada kerangka kerja komprehensif berbasis *blockchain* untuk mengatasi tantangan ini secara efektif.	(PORA), NIST Cybersecurity Framework, dan ISO/IEC 27001.	ada.dengan Kerangka kerja tersebut memberikan tingkat yang lebih tinggi dalam hal *transparency, security, privacy, accuracy, reliability, scalability, flexibility, and adaptability* dibandingkan model perbandingan. Dan Algoritma PORA memastikan pertukaran informasi hanya terjadi antara pihak yang terverifikasi dan bahwa data sensitif terlindungi secara kriptografis dan terkunci hingga verifikasi bukti sumber daya selesai.
4	*Modifications of the Formal Risk Analysis and*	Imed El Fray, Artur Wiliński	Penelitian ini dilakukan untuk mengatasi keterbatasan pada metode analisis dan penilaian risiko	Formal Model of Risk Analysis (FoMRA). dengan	Modifikasi dan abstraksi model pada FOMRA secara signifikan mempersingkat waktu perhitungan bobot

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
	Assessment for the Information System Security	Advances in Science and Technology Research Journal (2024) (Fray & Wiliński, 2024)	keamanan Sistem Informasi (SI) yang sudah digunakan (MEHARI)	mempertimbangkan pedoman standar ISO/IEC 27001 dan ISO/IEC 27005	risiko dibandingkan dengan metode MEHARI. Sistem Pemantauan *Real-Time* terintegrasi FOMRA dengan agen memungkinkan metode ini berfungsi sebagai sistem pemantauan keamanan dalam waktu *real-time*, memungkinkan reaksi cepat terhadap ancaman sistem. FOMRA dikonfirmasi sebagai metode analisis risiko aktif. Hasilnya telah diterapkan secara efisien dalam audit berbagai perusahaan dan diakui oleh badan sertifikasi untuk kepatuhan terhadap standar ISO/IEC 27001.

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
5	*Validation of the use of KPIs to measure information security management system performance in manufacturing companies*	Andrzej Pacana, Karolina Czerwińska Production Engineering Archives Polandia (2025) (Pacana & Czerwińska, 2025)	Permasalahan dalam mengukur secara efektif kinerja Sistem Manajemen Keamanan Informasi (SMKI) yang sesuai dengan standar ISO/IEC 27001, khususnya di sektor manufaktur yang menghadapi tantangan baru seiring dengan adopsi teknologi Industri 4.0. Meskipun ISO/IEC 27001 mengharuskan adanya pengukuran, perusahaan sering kali kesulitan dalam memilih dan menerapkan Indikator Kinerja Utama (KPI) yang valid dan relevan untuk mengukur efektivitas pengendalian keamanan (*security safeguards*).	Kerangka kerja standar seperti ISO/IEC 27001 dan kemudian mengidentifikasi KPI dengan memilih 32 indikator	Terdapat 32 KPI potensial, dan penelitian berhasil memvalidasi 25 KPI sebagai indikator yang *significant* (signifikan), *measurable* (terukur), dan *adequate* (memadai) untuk mengukur kinerja SMKI di perusahaan manufaktur. KPI yang tervalidasi dikelompokkan ke dalam 8 domain utama yang sejalan dengan area pengendalian keamanan. Penelitian menyimpulkan bahwa pengenalan KPI yang tervalidasi ini akan memungkinkan perusahaan manufaktur secara efektif memantau efektivitas pengendalian keamanan mereka, sehingga memungkinkan manajemen

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
					mengambil keputusan yang tepat untuk meningkatkan kinerja SMKI secara keseluruhan.
6	*A Comparative Analysis of Industrial Cybersecurity Standards*	Fatiha Djebbar, Kim Nordström. Digital Object Identifier 10.1109/ACCESS.2023.3303205 (2023) (Djebbar & Nordstrom, 2023)	tumpang tindih dan perbedaan antara tiga standar keamanan: ETSI EN 303 645 v2.1.1 untuk perangkat konsumen yang terhubung ke internet, ISA/IEC 62443-3-3:2019 untuk sistem kontrol dan otomatisasi industri, dan ISO/IEC 27001:2022 untuk sistem manajemen keamanan informasi	perbandingan mendalam terhadap tiga standar keamanan siber yaitu NIST SP 800-82, IEC 62443, dan ISO/IEC 27001/2022. analisis berfokus pada analisis struktur, isi, dan terminologi	Hasil dalam penelitian tersebut adalah terciptanya sebuah matriks pemetaan dan perbandingan komprehensif yang secara jelas menunjukkan kesamaan dan perbedaan antar standar. Hasil ini menegaskan bahwa setiap standar memiliki fokus yang berbeda: NIST SP 800-82 dan IEC 62443 berfokus pada lingkungan ICS/OT yang spesifik, sementara ISO/IEC 27001/22 bersifat lebih umum (*generic*). Matriks ini berfungsi sebagai panduan praktis

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
					bagi para praktisi untuk memilih standar yang paling optimal dan, jika perlu, mengintegrasikan berbagai standar dengan menghindari duplikasi.
7	DRSA: *A New Framework for Reliability Audit of Electronic Transaction Document Security in Electronic-Based Government Information Systems in* Indonesia	Irfani Ahmad, Purwanto, Agus Widodo. International Journal of Safety and Security Engineering (2025) (Ahmad dkk., 2025)	Kebutuhan pemerintah Indonesia terkait kebutuhan untuk menjamin keamanan dan keandalan (*reliability*) dokumen transaksi elektronik dalam Sistem Pemerintahan Berbasis Elektronik (SPBE). Meskipun pemerintah telah mengadopsi kerangka kerja keamanan seperti ISO/IEC 27001 dan Trustmark, kurangnya kerangka audit yang terintegrasi dan khusus untuk mengukur tingkat keandalan dan kepercayaan publik terhadap keamanan dokumen elektronik	DRSA (*Document Reliability and Security Audit*) yaitu kerangka kerja baru dengan penggabungan konsep ISO/IEC 27001 dan konsep Trustmark	Kerangka kerja DRSA yang diusulkan berhasil menyediakan metodologi audit yang sistematis dan spesifik untuk mengevaluasi keamanan dokumen transaksi elektronik pada sistem SPBE di Indonesia. Kerangka kerja ini dapat digunakan oleh auditor untuk mengukur tingkat keandalan sistem secara objektif, yang pada akhirnya akan membantu lembaga pemerintah dalam meningkatkan tata kelola

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
			menjadi kendala utama dalam implementasi SPBE yang sukses dan terpercaya.		keamanan informasi mereka, serta memperkuat kepercayaan publik terhadap layanan digital yang disediakan oleh pemerintah.
8	*Combining Standards to Conduct Risk Assessment at Secure End Solutions*	Muhammad Al-Abdullah, Alper Yayla, dan Mohammed Salem Al-Atoum, Journal of Information Systems Education. North Carolina, USA (2024) (Al-Abdullah dkk., 2024)	Dibutuhkannya analisis risiko keamanan informasi yang efektif dan sesuai dengan kebutuhan pelanggan oleh *SecureEnd Solutions*. Perusahaan tersebut menghadapi tantangan karena berbagai proyek keamanan mereka mewajibkan kepatuhan terhadap beragam standar keamanan (*multi-standards compliance*), seperti ISO/IEC 27001 dan NIST *Cybersecurity Framework* (CSF), sehingga diperlukan pendekatan penilaian risiko yang dapat mengakomodasi dan mengintegrasikan	Merancang metodologi penilaian risiko hibrida dari konsep Kerangka kerja ISO/IEC 27001 dan NIST *Cybersecurity Framework* (CSF), (identifikasi aset, ancaman, kerentanan, dan pengendalian yang relevan)	Berhasil menciptakan sebuah pendekatan terintegrasi yang tidak hanya memenuhi persyaratan kepatuhan ganda secara efisien tetapi juga berfungsi sebagai alat pembelajaran yang efektif bagi mahasiswa dan praktisi, menunjukkan bagaimana standar-standar keamanan yang berbeda dapat diselaraskan untuk melakukan penilaian risiko keamanan informasi yang komprehensif dan praktis.

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
			persyaratan dari standar-standar yang berbeda tersebut.		
9	*Cultivating excellence: a case study of enterprise architecture transformational journey in higher education*	Fatimah, Surya Sumarni, Nor Aziah, Nur Azaliah, Wan Azlin Zurita Indonesian Journal of Electrical Engineering and Computer Science (2024) (Amin dkk., 2024)	Institusi Pendidikan Tinggi seperti UiTM rentan terhadap kekakuan prosedur, duplikasi, dan kompleksitas operasional karena kurangnya *Arsitektur Enterprise* (EA) yang komprehensif, ditandai dengan ketidak selarasan di domain bisnis, data, aplikasi, dan teknologi.	Kerangka kerja *Enterprise Architecture* (EA) yaitu The Open Group Architecture Framework (TOGAF). dengan pendekatan studi kasus tunggal (di UiTM).	Berhasil mendeskripsikan isu-isu potensial di empat domain EA (bisnis, data, aplikasi, teknologi) dan menghasilkan diagram arsitektur sudut pandang peta lanskap (*landscape map viewpoint architecture*).
10	*Designing Information System Architecture*	Yemima Monica Geasela, Nilo Legowo	Institusi SMA di Indonesia belum mengimplementasikan teknologi informasi secara optimal dan terintegrasi di	Menggunakan *Enterprise Architecture* (EA) dengan kerangka	Dihasilkan enam *blueprint* aplikasi terintegrasi, yaitu: Sistem Akademik, Sistem Non-Akademik, Manajemen

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
	Based on Education 4.0 Case Study: Senior High School Institutions of Indonesia	Journal of Computer Science (2022) (Geasela & Legowo, 2022)	era *Edukasi* 4.0. Permasalahan ini mencakup kehilangan data, proses informasi yang lambat, dan sistem yang tidak terintegrasi.	kerja The Open Group Architecture Framework (TOGAF). Metode ini berfungsi untuk memandu perencanaan teknologi agar selaras dengan tujuan dan proses bisnis institusi	Pengadaan, Manajemen Keuangan, Manajemen SDM, dan Manajemen Data. Desain ini bertujuan menjadikan sistem sekolah lebih terintegrasi dan efisien.
11	*Governance in* Samarinda *city using* TOGAF (The open group architecture framework):	Rizki Galang Rahmadani, Oky Dwi Nurhayati, Dinar Mutiara Kusumo Nugraheni Edelweiss Applied Science	Tata kelola pemerintahan di Kota Samarinda menghadapi tantangan dalam konteks efisiensi, transparansi, dan keterlibatan warga (*citizen engagement*), yang menghambat peningkatan	Menggunakan kerangka kerja (TOGAF), yang merupakan standar Enterprise Architecture (EA), untuk memastikan keselarasan antara	Dihasilkan metode yang dapat di usulkan penerapan TOGAF sebagai kerangka kerja untuk meningkatkan proses administrasi dan operasional Kota Samarinda. TOGAF.

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Author / Tahun	Permasalahan	Metode	Hasil Penelitian
	Literature review	and Technology (2024) (Rahmadani dkk., 2024)	kualitas layanan publik dan efektivitas operasional.	tujuan bisnis (pemerintahan) dan teknologi informasi. Penelitian dilakukan dengan metode *literature review*	

.

Hasil tinjauan terhadap berbagai penelitian menunjukkan bahwa pendekatan arsitektur enterprise, tata kelola, dan manajemen risiko keamanan informasi memainkan peran strategis dalam mendukung transformasi digital di sektor pendidikan, pemerintahan, dan industri. Sejumlah penelitian menekankan pentingnya penetapan arah strategis institusi, termasuk pemanfaatan platform digital, pengembangan arsitektur teknologi yang fleksibel, serta kebutuhan tata kelola data yang kuat untuk menjamin aliran data yang terintegrasi dan kepatuhan terhadap regulasi. Selain itu, penerapan *Enterprise Architecture* (EA) terbukti efektif dalam memetakan isu-isu lintas domain, bisnis, data, aplikasi, dan teknologi serta menghasilkan blueprint dan diagram arsitektur yang mampu meningkatkan integrasi, efisiensi, dan skalabilitas sistem.

Di sisi lain, penelitian tersebut juga menegaskan bahwa manajemen keamanan informasi dan analisis risiko merupakan komponen krusial dalam transformasi digital. Berbagai kerangka kerja dan metode yang diusulkan menunjukkan keunggulan dalam aspek transparansi, keamanan, privasi, akurasi, keandalan, serta adaptabilitas sistem, termasuk melalui pemanfaatan algoritma kriptografi dan mekanisme verifikasi yang ketat. Metode analisis risiko terbukti mampu mempercepat proses evaluasi, mendukung pemantauan keamanan secara real-time, serta memenuhi standar internasional seperti ISO/IEC 27001. Namun penelitian terdahlu belum ada yang secara langsung melakukan proses pengembangan *enterprise architecture* yang terintegrasi dan patuh pada regulasi atau panduan tersetruktur terhadap keamana informasi .Secara keseluruhan, hasil-hasil penelitian tersebut memperlihatkan bahwa integrasi antara arsitektur *enterprise*, manajemen risiko, dan standar keamanan informasi merupakan pendekatan yang komprehensif dan efektif dalam mendukung keberhasilan transformasi digital dan peningkatan kepercayaan terhadap sistem informasi.

2.2. Dasar Teori

Dasar teori dalam penelitian ini berfungsi sebagai landasan konseptual yang memberikan justifikasi ilmiah terhadap parameter-parameter yang digunakan

dalam menganalisis fenomena teknologi informasi yang dikaji. Dengan meninjau teori-teori yang di mulai dari keamanan informasi, arsitektur *enterprise* hingga manajemen risiko, peneliti tidak hanya membangun peta jalan untuk memvalidasi argumen penelitian, tetapi juga menyediakan instrumen evaluasi yang kredibel untuk mengukur efektivitas implementasi teknologi di lapangan.

2.2.1. Keamanan Informasi

Dengan meningkatnya adopsi teknologi informasi dalam pendidikan, institusi diharapkan mampu menghadapi tantangan terkait dengan keamanan Informasi, terutama saat pergerakan peserta didik yang kompleks. Pada dasarnya, tata kelola arsitektur perusahaan (*Enterprise Architecture*) menjadi kunci untuk memastikan bahwa sistem informasi yang diterapkan dapat memenuhi kebutuhan keamanan yang tepat.

Enterprise Architecture berfungsi sebagai jembatan antara inisiatif bisnis dan teknologi informasi, yang sangat penting bagi institusi pendidikan untuk mengorganisir dan menyelaraskan proses dengan teknologi yang ada (Nur Hidayati dkk., 2024). Dengan pendekatan *Enterprise Architecture*, sekolah-sekolah di Indonesia dapat merancang arsitektur sistem informasi yang tidak hanya efisien tetapi juga menjaga integritas dan keamanan data peserta didik. Implementasi metode TOGAF (The Open Group Architecture Framework) dapat membawa keuntungan signifikan, seperti yang ditunjukkan dalam penelitian yang menemukan bahwa framework ini membantu dalam membangun, mengelola, dan memelihara arsitektur sistem informasi secara sistematis (Astuti dkk., 2024; Nadia Selvi Ramadhani dkk., 2025).

Dalam konteks menjalankan sistem informasi yang aman, penting bagi institusi pendidikan untuk menerapkan pengukuran yang tepat terhadap kinerja sistem manajemen keamanan informasi. Penggunaan Indikator Kinerja Utama (KPI) sebagai metode untuk mengevaluasi efektivitas sistem keamanan informasi telah dibuktikan mampu memberikan wawasan kritis terkait dengan perlindungan data, pengelolaan ancaman, dan pengendalian proses (Hardi & Legowo, 2023).

Melalui penerapan KPI, institusi pendidikan dapat melakukan analisis risiko dan meminimalkan kemungkinan kebocoran data yang dapat merugikan akademisi dan peserta didik.

Lebih jauh lagi, penelitian di beberapa institusi pendidikan tinggi di luar negeri menunjukkan pentingnya integrasi repositori data yang terpusat untuk memastikan akses yang aman dan efisien terhadap data siswa. Hal ini menjadi relevan untuk institusi pendidikan di Indonesia, di mana sering kali terdapat ketidakselarasan dalam pengelolaan data di setiap departemen (Divatia & Jagasia, 2025). Dengan mengadopsi metode yang terbukti, seperti yang diterapkan di negara lain, institusi pendidikan di Indonesia dapat memperkuat keamanan data dan meningkatkan efektivitas layanan yang diberikan kepada peserta didik.

Meningkatkan keamanan data dalam penerapan sistem informasi, institusi pendidikan di Indonesia harus memberdayakan proses tata kelola teknologi informasi yang kuat dan berkesinambungan. Hal ini mencakup pembaruan strategi keamanan berdasarkan perkembangan terbaru dalam teknologi informasi, serta penerapan praktik terbaik dalam arsitektur sistem informasi yang sudah terbukti efektif di berbagai institusi pendidikan. Dengan demikian, institusi pendidikan tidak hanya dapat melindungi data mereka tetapi juga menciptakan lingkungan belajar yang aman dan kondusif bagi semua peserta didik.

2.2.2. Manajemen Resiko

Pesantren yang menerapkan prinsip tata kelola yang baik (transparansi, akuntabilitas, pertanggungjawaban, kemandirian, kewajaran) memiliki dasar organisasi untuk merancang aturan dan mekanisme pengelolaan informasi secara tertib. Kebutuhan akuntabilitas kepada stakeholder juga menuntut adanya penyajian informasi yang relevan dan dapat dipahami (misalnya dalam laporan keuangan), sehingga pengelolaan dokumen dan data harus dilakukan secara sistematis (Istutik dkk., 2023). Praktik pendampingan penyusunan RKAPP/RAPBPP dan anjuran evaluasi pengelolaan keuangan memperlihatkan bahwa perencanaan – pelaksanaan – evaluasi merupakan siklus yang dibutuhkan dalam pengelolaan data keuangan

dan pendekatan siklus ini dapat diperluas untuk tata kelola data digital pesantren secara menyeluruh (M Zaki Mubarak dkk., 2023).

Penelitian tentang penguatan pendidikan karakter melalui peraturan pesantren menunjukkan bahwa implementasi aturan dapat memperkuat disiplin, kemandirian, dan tanggung jawab santri di era 4.0. Dalam konteks keamanan informasi, disiplin dan tanggung jawab merupakan basis perilaku organisasi untuk menjaga kerahasiaan pengelolaan dokumen ketika proses sudah terdigitalisasi (Kusuma dkk., 2021). Selain itu, studi pesantren menegaskan pentingnya pembinaan karakter sebagai fondasi perilaku warga pesantren, yang relevan sebagai landasan etika dalam pengelolaan informasi ketika akses dan diseminasi data makin mudah melalui teknologi digital (Wijaya dkk., 2024).

Dalam praktiknya, mengadopsi metodologi model proses *Plan-Do-Check-Action* (PDCA). Pendekatan siklus ini sangat penting untuk menjamin bahwa ISMS suatu organisasi tidak hanya terbentuk dan berfungsi, tetapi juga terus-menerus dievaluasi dan ditingkatkan seiring waktu. Dengan menerapkan PDCA, organisasi dapat secara sistematis merencanakan tindakan keamanan, melaksanakannya, memantau hasilnya, dan mengambil langkah korektif atau perbaikan untuk memastikan keamanan informasi tetap optimal dan relevan dengan dinamika ancaman yang ada (Alreemy dkk., 2016).

2.2.3. Data dan Informasi

Data dan informasi siswa/santri di pondok pesantren bersifat jangka panjang karena mengiringi seluruh siklus Pendidikan. Mulai dari penerimaan, pembinaan, layanan keseharian, penilaian, hingga kelulusan yang dalam praktik manajemen peserta didik juga terdokumentasi melalui observasi, wawancara, dan dokumentasi administrasi. Ketika pesantren melakukan digitalisasi, teknologi diposisikan sebagai sarana peningkatan kualitas institusi sekaligus kanal diseminasi informasi lembaga, sehingga volume, keterhubungan, dan keterpaparan data santri meningkat dan menuntut tata kelola yang lebih ketat (Petrov dkk., 2022). Dalam konteks pesantren sebagai entitas pendidikan berorientasi nirlaba, penerapan prinsip tata kelola (transparansi, akuntabilitas, pertanggungjawaban, kemandirian, kewajaran)

dipandang sebagai fondasi peningkatan efektivitas organisasi, dan fondasi ini relevan untuk memastikan perlindungan data santri berjalan seimbang dengan kebutuhan layanan dan pelaporan kelembagaan.

Perlindungan data santri menjadi krusial karena sebagian data yang dikelola pesantren menyentuh aspek keselamatan dan martabat siswa, misalnya data terkait pencegahan kekerasan/*bullying* dalam kerangka "pesantren ramah anak" yang masih memerlukan evaluasi mendalam agar efektif mencegah kekerasan, serta strategi implementasinya yang menekankan pembentukan tim, sosialisasi, pengembangan SDM, monitoring-evaluasi, dan respons terhadap masukan. Selain itu, pesantren juga berpotensi mengelola data kesejahteraan psikologis santri melalui instrumen terukur, dan data kesehatan santri melalui program edukasi kesehatan. Karena digitalisasi memperluas praktik pengumpulan dan pemanfaatan data pendidikan (termasuk aktivitas siswa dalam *platform* pembelajaran) dan dapat melibatkan pihak penyedia layanan komputasi awan/perangkat lunak, kebutuhan proteksi privasi dan etika menjadi semakin mendesak (Alif dkk., 2020), terutama ketika data pendidikan digunakan dalam konteks analitik dan otomasi pengumpulan data.

Berbasis praktik pengelolaan peserta didik dan program-program pesantren yang terdokumentasi dalam literatur, kategori data berikut perlu diprioritaskan dalam kebijakan keamanan informasi saat digitalisasi :

1. Data identitas dan administrasi santri (misalnya berkas penerimaan, status kepesertadidikan, riwayat administrasi) karena manajemen peserta didik di pesantren melibatkan dokumentasi yang bersifat berkelanjutan sepanjang masa studi, dan digitalisasi memperluas kemungkinan disimpan/ditransmisikan sebagai informasi kelembagaan.
2. Data akademik dan proses pembelajaran (misalnya penilaian, catatan pembinaan, rekam capaian) karena kualitas institusi dan proses pembelajaran merupakan komponen kinerja pesantren yang ditata melalui tata kelola organisasi, dan digitalisasi diarahkan untuk peningkatan kualitas institusi.
3. Data kesehatan santri (misalnya catatan program kesehatan/penyuluhan) karena isu kesehatan remaja putri di pesantren (contoh anemia) ditangani melalui

kegiatan edukatif yang dapat menghasilkan data kesehatan, dan data kesehatan secara umum dipandang membutuhkan kontrol privasi yang kuat.

4. Data aktivitas digital/metadata pembelajaran (jika menggunakan LMS/aplikasi) karena e-learning mengumpulkan data dan metadata aktivitas siswa, dan pemanfaatannya untuk learning analytics menuntut perspektif etika serta kontrol privasi, sementara pengumpulan data otomatis meningkatkan risiko privasi.
5. Data terkait program pembinaan nilai (misalnya moderasi beragama) karena program internalisasi moderasi beragama untuk pencegahan radikalisme melibatkan observasi, wawancara, dan dokumentasi, dan pengembangan moderasi melalui seminar/dialog dan distribusi buku juga menghasilkan dokumentasi programatik yang dapat sensitif bila terdigitalisasi dan didiseminasikan tanpa kontrol.

2.2.4. ISO/IEC 27001:2022

ISO/IEC 27001 adalah standar internasional terkemuka untuk Sistem Manajemen Keamanan Informasi (ISMS) yang dirancang untuk membantu organisasi melindungi aset informasi vital mereka. Dikembangkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC), standar ini pertama kali diperkenalkan pada tahun 2005 dan telah diperbarui, dengan revisi terbaru pada tahun 2022. Inti dari standar ini adalah menetapkan serangkaian persyaratan fundamental bagi sebuah entitas untuk membangun, menerapkan, memelihara, dan terus menyempurnakan ISMS. Organisasi yang mematuhinya dapat memperoleh sertifikasi melalui proses audit eksternal. Keamanan informasi dalam standar ini dicapai melalui serangkaian kendali terintegrasi, mulai dari kebijakan dan prosedur hingga teknologi, dan ISMS itu sendiri berfungsi sebagai kerangka kerja berbasis risiko yang sistematis untuk mengelola dan melindungi informasi secara berkelanjutan. ISO 27001 dapat membantu perusahaan mengidentifikasi berbagai potensi risiko terkait keamanan informasi dalam organisasi. Struktur organisasi ISO 27001 terbagi menjadi dua bagian besar, yaitu:

1. Klausul: Proses wajib Klausul (pasal) berisi persyaratan atau kebutuhan dan ketentuan yang harus dipenuhi oleh organisasi atau perusahaan dalam menerapkan ISMS menggunakan standar ISO 27001.
2. Lampiran A : Pengendalian Keamanan Lampiran A merupakan dokumen acuan yang disediakan dan dapat dijadikan acuan untuk menentukan pengendalian keamanan yang akan diterapkan pada sistem manajemen keamanan informasi, Lampiran A ISO 27001 yang terdiri dari 10 klausul pengendalian keamanan.

Dalam buku "Sistem Manajemen Keamanan Informasi ISO 27001" karya Sarno dan Iffano, beberapa hal penting yang dapat diperhatikan dalam penggunaan standar ISO 27001 yang dipilih sebagai standar penerapan ISMS suatu organisasi adalah sebagai berikut: ISO 27001 telah menyediakan suatu model yang lengkap mengenai bagaimana hal-hal berikut ini dilakukan. :

1. Menetapkan ISMS
2. Mengimplementasikan ISMS
3. Mengoperasikan ISMS
4. Memantau ISMS
5. Meninjau ulang ISMS Memelihara
6. Memahami ISMS Penyempurnaan

ISO 27001 dirancang agar penerapan ISMS dengan standar ini lebih fleksibel karena dapat sesuai dengan hal-hal berikut:

1. Kebutuhan organisasi
2. Sasaran organisasi yang ingin dicapai
3. Persyaratan keamanan
4. Proses bisnis yang ada
5. Jumlah karyawan dan besar kecilnya struktur organisasi

Sehingga dengan menggunakan standar ISO 27001 dalam penerapannya dapat sangat bergantung pada keadaan dan kebutuhan organisasi, karena organisasi dengan proses bisnis yang sederhana akan memerlukan ISMS yang sederhana pula. Dalam bukunya Sarno dan Iffano mengatakan bahwa pengendalian keamanan berdasarkan ISO 27001 terdiri dari 10 klausul pengendalian keamanan, 93 sasaran

pengendalian (yang disarankan untuk di adopsi dan di implementasika) terbagi menjadi,

1. 10 klausul
   a. Klausul 1 – 3 : gagasan utama (ruang lingkup, Refrensi dan istilah)
   b. Kalusul 4 – 10 : menetapkan persyaratan tertentu dan tindakan yang dapat dilakukan yang harus diikuti (dapat di tindaklanjuti / *actionales*)
2. 93 Control
   a. 37 Organisational Control
   b. 8 Peopel Control
   c. 14 physical Control
   d. 34 technologicalCcontrol

Definisi klausul wajib yang terdapat pada klausul nomor 1-3 adalah sebagai berikut:

1. *Scope* (Cakupan)

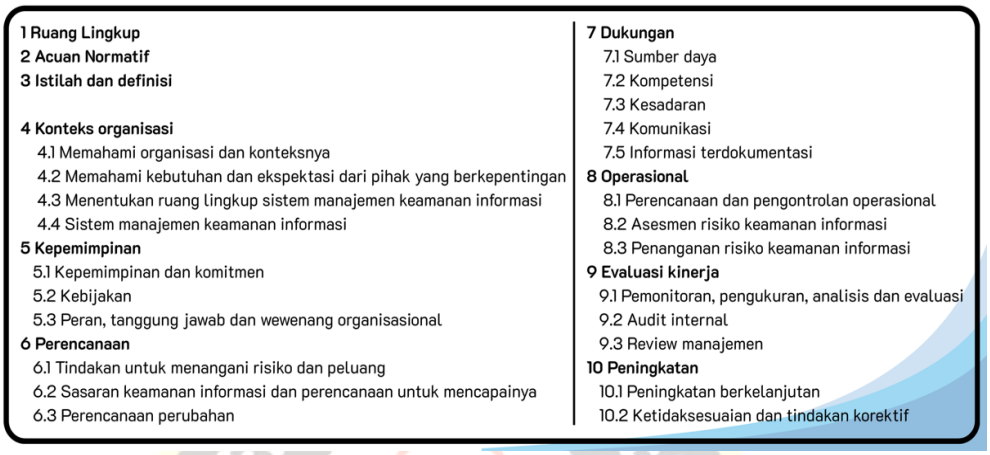
Dokumen ini menetapkan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi dalam konteks organisasi. Dokumen ini juga mencakup persyaratan untuk penilaian dan penanganan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi. Persyaratan yang ditetapkan dalam dokumen ini bersifat umum dan dimaksudkan untuk diterapkan pada semua organisasi, terlepas dari jenis, ukuran, atau sifatnya. Pengecualian terhadap persyaratan yang ditentukan dalam Klausul 4 hingga 10 tidak dapat diterima ketika suatu organisasi mengklaim kesesuaian dengan dokumen ini.

2. *Normative references* (Referensi Normatif)

Dokumen yang dirujuk dalam administrasi harian sehingga sebagian atau seluruh isinya merupakan persyaratan dari dokumen ini. Seperti contoh dokumen untuk referensi bertanggal, hanya edisi yang dikutip yang berlaku. Untuk referensi tanpa tanggal, edisi terbaru dari dokumen yang dirujuk (termasuk amandemennya) yang berlaku. Dokumen dapat berupa Surat Keputusan atau Surat Tugas.

3. *Terms and definitions* (Istilah dan Definisi)

Untuk keperluan dokumen ini, istilah dan definisi yang diberikan dalam ISO/IEC 27001 berlaku. Daftar klausul yeng di maskut dijelaskan pada gambar 2.1 berikut ini yang terdapat pada ISO/IEC 27001:2022 :



1 Ruang Lingkup
2 Acuan Normatif
3 Istilah dan definisi

4 Konteks organisasi
4.1 Memahami organisasi dan konteksnya
4.2 Memahami kebutuhan dan ekspektasi dari pihak yang berkepentingan
4.3 Menentukan ruang lingkup sistem manajemen keamanan informasi
4.4 Sistem manajemen keamanan informasi

5 Kepemimpinan
5.1 Kepemimpinan dan komitmen
5.2 Kebijakan
5.3 Peran, tanggung jawab dan wewenang organisasional

6 Perencanaan
6.1 Tindakan untuk menangani risiko dan peluang
6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya
6.3 Perencanaan perubahan

7 Dukungan
7.1 Sumber daya
7.2 Kompetensi
7.3 Kesadaran
7.4 Komunikasi
7.5 Informasi terdokumentasi

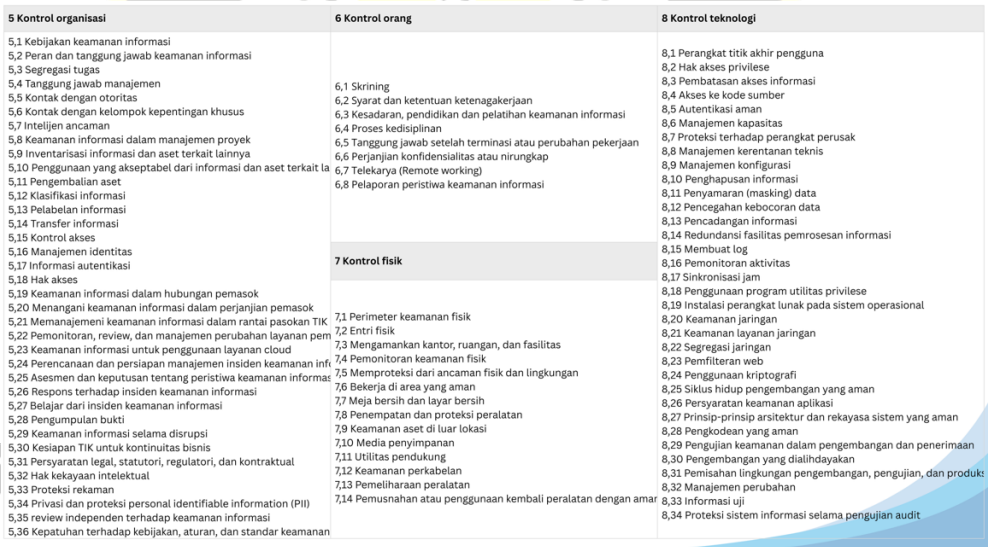
8 Operasional
8.1 Perencanaan dan pengontrolan operasional
8.2 Asesmen risiko keamanan informasi
8.3 Penanganan risiko keamanan informasi

9 Evaluasi kinerja
9.1 Pemonitoran, pengukuran, analisis dan evaluasi
9.2 Audit internal
9.3 Review manajemen

10 Peningkatan
10.1 Peningkatan berkelanjutan
10.2 Ketidaksesuaian dan tindakan korektif

Gambar 2. 1 Klausul ISO/IEC 27001:2022

Kemudian Daftar Pengendalian Keamanan yang terdapat pada Lampiran A yang terdiri dari 93 kontrol dijelaskan pada gambar 2.2 berikut ini :



5 Kontrol organisasi	6 Kontrol orang	8 Kontrol teknologi
5,1 Kebijakan keamanan informasi		8,1 Perangkat titik akhir pengguna
5,2 Peran dan tanggung jawab keamanan informasi		8,2 Hak akses privilese
5,3 Segregasi tugas		8,3 Pembatasan akses informasi
5,4 Tanggung jawab manajemen	6,1 Skrining	8,4 Akses ke kode sumber
5,5 Kontak dengan otoritas	6,2 Syarat dan ketentuan ketenagakerjaan	8,5 Autentikasi aman
5,6 Kontak dengan kelompok kepentingan khusus	6,3 Kesadaran, pendidikan dan pelatihan keamanan informasi	8,6 Manajemen kapasitas
5,7 Intelijen ancaman	6,4 Proses kedisiplinan	8,7 Proteksi terhadap perangkat perusak
5,8 Keamanan informasi dalam manajemen proyek	6,5 Tanggung jawab setelah terminasi atau perubahan pekerjaan	8,8 Manajemen kerentanan teknis
5,9 Inventarisasi informasi dan aset terkait lainnya	6,6 Perjanjian konfidensialitas atau nirungkap	8,9 Manajemen konfigurasi
5,10 Penggunaan yang akseptabel dari informasi dan aset terkait la	6,7 Telekarya (Remote working)	8,10 Penghapusan informasi
5,11 Pengembalian aset	6,8 Pelaporan peristiwa keamanan informasi	8,11 Penyamaran (masking) data
5,12 Klasifikasi informasi		8,12 Pencegahan kebocoran data
5,13 Pelabelan informasi		8,13 Pencadangan informasi
5,14 Transfer informasi		8,14 Redundansi fasilitas pemrosesan informasi
5,15 Kontrol akses		8,15 Membuat log
5,16 Manajemen identitas	**7 Kontrol fisik**	8,16 Pemonitoran aktivitas
5,17 Informasi autentikasi		8,17 Sinkronisasi jam
5,18 Hak akses		8,18 Penggunaan program utilitas privilese
5,19 Keamanan informasi dalam hubungan pemasok		8,19 Instalasi perangkat lunak pada sistem operasional
5,20 Menangani keamanan informasi dalam perjanjian pemasok	7,1 Perimeter keamanan fisik	8,20 Keamanan jaringan
5,21 Memanajemeni keamanan informasi dalam rantai pasokan TIK	7,2 Entri fisik	8,21 Keamanan layanan jaringan
5,22 Pemonitoran, review, dan manajemen perubahan layanan pem	7,3 Mengamankan kantor, ruangan, dan fasilitas	8,22 Segregasi jaringan
5,23 Keamanan informasi untuk penggunaan layanan cloud	7,4 Pemonitoran keamanan fisik	8,23 Pemfilteran web
5,24 Perencanaan dan persiapan manajemen insiden keamanan inf	7,5 Memproteksi dari ancaman fisik dan lingkungan	8,24 Penggunaan kriptografi
5,25 Asesmen dan keputusan tentang peristiwa keamanan informas	7,6 Bekerja di area yang aman	8,25 Siklus hidup pengembangan yang aman
5,26 Respons terhadap insiden keamanan informasi	7,7 Meja bersih dan layar bersih	8,26 Persyaratan keamanan aplikasi
5,27 Belajar dari insiden keamanan informasi	7,8 Penempatan dan proteksi peralatan	8,27 Prinsip-prinsip arsitektur dan rekayasa sistem yang aman
5,28 Pengumpulan bukti	7,9 Keamanan aset di luar lokasi	8,28 Pengkodean yang aman
5,29 Keamanan informasi selama disrupsi	7,10 Media penyimpanan	8,29 Pengujian keamanan dalam pengembangan dan penerimaan
5,30 Kesiapan TIK untuk kontinuitas bisnis	7,11 Utilitas pendukung	8,30 Pengembangan yang dialihdayakan
5,31 Persyaratan legal, statutori, regulatori, dan kontraktual	7,12 Keamanan perkabelan	8,31 Pemisahan lingkungan pengembangan, pengujian, dan produk
5,32 Hak kekayaan intelektual	7,13 Pemeliharaan peralatan	8,32 Manajemen perubahan
5,33 Proteksi rekaman	7,14 Pemusnahan atau penggunaan kembali peralatan dengan amar	8,33 Informasi uji
5,34 Privasi dan proteksi personal identifiable information (PII)		8,34 Proteksi sistem informasi selama pengujian audit
5,35 review independen terhadap keamanan informasi		
5,36 Kepatuhan terhadap kebijakan, aturan, dan standar keamanan		

Gambar 2. 2 Daftar Lampiran A ISO/IEC 27001:2022

ISMS (*Information Security Management System*) dapat disertifikasi sesuai dengan standar ISO/IEC 27001 oleh sejumlah Pendaftar Terakreditasi di seluruh dunia. Sertifikasi terhadap salah satu varian nasional ISO/IEC 27001 yang diakui, seperti JIS Q 27001 (versi Jepang), oleh badan sertifikasi terakreditasi secara

fungsional setara dengan sertifikasi terhadap ISO/IEC 27001 itu sendiri. Di beberapa negara, badan yang memverifikasi kesesuaian sistem manajemen dengan standar tertentu dikenal sebagai "badan sertifikasi," sementara di negara lain mereka sering disebut sebagai "badan registrasi," "badan penilaian dan registrasi," "badan sertifikasi/registrasi," dan terkadang "registrar." Sertifikasi ISO/IEC 27001, seperti sertifikasi sistem manajemen ISO lainnya, biasanya melibatkan proses audit eksternal tiga tahap yang ditentukan oleh standar ISO/IEC 17021 dan ISO/IEC 27006 (Astuti dkk., 2024).

2.2.5. TOGAF ADM

TOGAF (*The Open Group Architecture Framework*) adalah kerangka kerja yang digunakan untuk merencanakan, merancang, dan menerapkan arsitektur organisasi secara komprehensif. Salah satu komponen inti dari TOGAF adalah ADM (*Architecture Development Method*), yang menawarkan metodologi berulang untuk membangun dan mengelola arsitektur, termasuk arsitektur bisnis, informasi, dan teknologi yang relevan untuk kebutuhan organisasi. Pemahaman yang baik tentang ADM dalam TOGAF sangat penting untuk memastikan bahwa implementasi arsitektur dapat berjalan dengan efektif dan efisien.

TOGAF dilengkapi dengan berbagai alat yang membantu dalam implementasinya. Kerangka ini mulai dikembangkan pada awal tahun 1990 sebagai pengembangan arsitektur teknis dari forum *Open Group*. Pada tahun 1995, TOGAF resmi diperkenalkan dengan fokus pada pengelolaan arsitektur teknis.

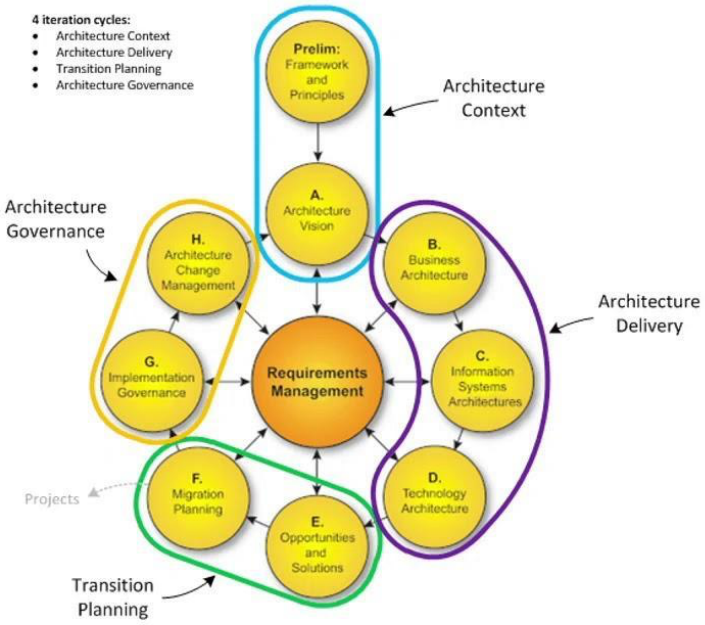
Architecture Diagram Method (ADM) merupakan suatu metode tentang bagaimana membangun, mengelola, dan mengimplementasikan *enterprise architecture* serta sistem informasi (Rachel Harrison, 2016). TOGAF ADM juga menyatakan suatu visi dan prinsip yang jelas tentang bagaimana mengembangkan *enterprise architecture*, prinsip-prinsip tersebut digunakan sebagai ukuran dalam menilai keberhasilan pengembangan *enterprise architecture* oleh suatu organisasi (The Open Group, 2009), prinsip-prinsip tersebut dapat dijelaskan sebagai berikut:

a. Prinsip-prinsip pengembangan *enterprise architecture* diharapkan dapat mendukung seluruh bagian organisasi, termasuk unit-unit organisasi yang membutuhkannya.
b. Prinsip-prinsip teknologi informasi (TI) Lebih mengarahkan konsistensi penggunaan TI di seluruh organisasi, termasuk unit-unit organisasi yang akan menggunakannya.
c. Prinsip arsitektur merancang arsitektur sistem berdasarkan kebutuhan proses bisnis dan cara mengimplementasikannya.

Salah satu keunggulan TOGAF adalah sifatnya yang fleksibel, berkat pendekatan *Open Source*-nya yang sistematis dan kaya akan teknis arsitektur. Dalam kerangka TOGAF, *Arsitektur Enterprise* dibagi menjadi empat kategori utama:

1. *Business Architecture*: Mendeskripsikan proses bisnis yang diperlukan untuk mencapai tujuan organisasi.
2. *Application Architecture*: Menjelaskan bagaimana aplikasi dirancang dan berinteraksi satu sama lain.
3. *Data Architecture:* Menguraikan proses pengelolaan dan akses data.
4. *Technical Architecture:* Menggambarkan infrastruktur yang mendukung aplikasi, termasuk perangkat keras dan perangkat lunak serta interaksinya.

TOGAF *Architecture Development Method* (ADM) adalah inti dari proses arsitektur TOGAF. ADM memungkinkan organisasi untuk mendefinisikan kebutuhan bisnis mereka dengan tujuan membangun arsitektur yang sesuai. Dapat dikatakan bahwa TOGAF ADM adalah metode kompleks yang menggunakan model yang dapat diterapkan dalam pengembangan arsitektur. Lingkup ADM mencakup penetapan kerangka, pembangunan konten arsitektur, peralihan, dan pengelolaan proses realisasi arsitektur (Lattu dkk., 2022). Proses ini diatur dalam siklus iteratif yang terdiri dari sepuluh fase sebagai pada gambar 2.3 berikut:



Gambar 2. 3 Fase dalam TOGAF ADM

1. Fase *Preliminary:* Menjelaskan persiapan dalam perancangan arsitektur dengan mendefinisikan kerangka dan prinsip untuk menyelaraskan TOGAF dengan tujuan perancangan.
2. Fase A: *Architecture Vision*: Menyediakan gambaran awal dari perancangan arsitektur, mencakup ruang lingkup, identifikasi pemangku kepentingan, penyusunan visi arsitektur, dan persetujuan untuk perancangan.
3. Fase B: *Business Architecture*: Menggambarkan arsitektur bisnis dalam konteks perancangan arsitektur, menggunakan alat dan metode seperti *Unified Model Language* (UML*), Business Process Modeling Notation* (BPMN), dan *Integration Definition* (IDEF).
4. Fase C: *Information System Architecture*: Menjelaskan pengembangan arsitektur sistem informasi yang mencakup dua domain, yaitu arsitektur aplikasi dan arsitektur data.
5. Fase D: *Technology Architecture:* Fokus pada pengembangan arsitektur teknologi yang diperlukan oleh organisasi.

6. Fase E: *Opportunity and Solution*: Menguraikan manfaat dari perancangan *arsitektur enterprise* dengan mengevaluasi kembali model yang telah dibangun.
7. Fase F: *Migration and Planning*: Melakukan analisis risiko dan biaya berdasarkan daftar prioritas proyek yang akan dilaksanakan.
8. Fase G: *Implementation Governance*: Mengawasi proses perancangan arsitektur dan merancang kontrak arsitektur untuk implementasi proyek.
9. Fase H: *Architecture Change Management*: Mengelola prosedur perubahan pada arsitektur setelah implementasi.
10. Requirement: Mengelola kebutuhan arsitektur.

Perkembangan TOGAF 9 ke TOGAF 10 menciptakan kerangka kerja yang lebih kuat dan adaptif untuk mengelola arsitektur perusahaan. Dengan fokus yang lebih besar pada kemampuan bisnis, integrasi teknologi, dan inovasi, TOGAF 10 membantu organisasi untuk tidak hanya memahami arsitektur yang berlaku saat ini, tetapi juga mempersiapkan diri mereka untuk tantangan dan peluang yang akan datang dalam era digital. Ini menciptakan nilai yang lebih tinggi bagi organisasi dalam menjalankan misinya dan mencapai tujuan strategis mereka. Penelitian oleh Widyastuti. menunjukkan bahwa TOGAF 10 memberikan panduan lebih terperinci untuk mengembangkan arsitektur yang sesuai dengan visi dan misi institusi, serta menangani masalah yang ada secara proaktif (Widyastuti dkk., 2024). Dengan pendekatan yang lebih terstruktur ini, TOGAF 10 mempermudah organisasi dalam menavigasi kompleksitas arsitektur TI, baik untuk perangkat lunak baru maupun untuk solusi yang sudah ada.

Keuntungan Metode TOGAF ADM Vertion 10

Metode TOGAF (The Open Group Architecture Vertion 10) ADM (*Architecture Development Method*) menawarkan berbagai keuntungan dalam merancang dan mengelola arsitektur sistem informasi. Pertama, pendekatan terstruktur yang dihadirkan oleh TOGAF ADM memastikan bahwa semua aspek penting dalam pengembangan arsitektur diperhatikan. Dengan mengikuti langkah-langkah yang jelas dan sistematis, organisasi dapat meminimalkan risiko kesalahan dan memastikan solusi yang dihasilkan relevan dengan kebutuhan organisasi.

Selain itu, TOGAF ADM dirancang untuk bersifat fleksibel dan dapat disesuaikan dengan berbagai konteks organisasi, baik yang besar maupun kecil, serta di berbagai sektor industri. Hal ini memungkinkan lembaga pendidikan untuk menyesuaikan kerangka kerja ini sesuai dengan kebutuhan dan sumber daya yang tersedia, memberikan kebebasan dalam merancang sistem yang paling sesuai.

Keterlibatan pemangku kepentingan merupakan keuntungan penting lainnya dari TOGAF. Metode ini menekankan pentingnya melibatkan semua pihak terkait, termasuk pengelola, guru, dan santri, dalam setiap tahap pengembangan arsitektur. Dengan melibatkan pengguna, organisasi dapat memastikan bahwa sistem informasi yang dirancang benar-benar memenuhi kebutuhan mereka, sekaligus meningkatkan akseptabilitas solusi yang dihasilkan. Di samping itu, TOGAF ADM membantu dalam meningkatkan efisiensi dan efektivitas pengelolaan sistem informasi. Dengan mengidentifikasi dan menghilangkan duplikasi fungsi serta mengoptimalkan penggunaan sumber daya, organisasi dapat mengalokasikan sumber daya secara lebih efisien untuk mencapai tujuan strategis.

Konten Metode Togaf Adm Vertion 10

Kerangka arsitektur konten TOGAF menyediakan konten arsitektur yang memungkinkan produk kerja utama didefinisikan secara konsisten, terstruktur, dan terkirim. TOGAF menggunakan 3 (tiga) kategori untuk menggambarkan jenis produk kerja arsitektur dalam konteks penggunaannya (The Open Group, 2009):

a. *Deliverables* adalah produk kerja yang didefinisikan secara spesifik dan ditinjau secara formal, disetujui, dan ditandatangani oleh para pemangku kepentingan. Hasil nyata adalah keluaran dari proyek dan dalam bentuk dokumentasi yang akan diarsipkan pada penyelesaian proyek.
b. Artifak adalah produk pengembangan arsitektur yang lebih rinci, yang menggambarkan arsitektur dari perspektif tertentu. Artifak secara umum diklasifikasikan sebagai katalog (daftar aset), matriks (menunjukkan hubungan antara berbagai hal) dan diagram (gambar).
c. *Building Blocks* adalah komponen arsitektur yang dapat digunakan kembali untuk menyusun dan mengembangkan arsitektur maupun solusi. *Building Blocks* berfungsi sebagai "blok penyusun" yang bisa digabungkan, diatur, atau

dimodifikasi sesuai kebutuhan organisasi. *Building Blocks* terbagi menjadi dua jenis, yaitu:

i. *Architecture Building Blocks* (ABB) yang bersifat konseptual dan mendefinisikan kapabilitas atau layanan yang dibutuhkan (misalnya layanan keamanan, layanan integrasi data, atau layanan autentikasi).
ii. *Solution Building Blocks* (SBB) yang merupakan implementasi nyata dari ABB, biasanya berupa teknologi, sistem, atau aplikasi tertentu (misalnya *firewall, server database*, atau perangkat lunak ERP).

Hasil nyata dari *Building Blocks* adalah tersedianya komponen standar yang bisa dipakai ulang di berbagai proyek, sehingga mempercepat proses desain, mengurangi biaya, dan memastikan konsistensi dalam arsitektur TI organisasi.

- Deliverables → apa yang diserahkan (output resmi).
- Artifacts → dokumen/diagram yang menjelaskan detail arsitektur.
- Building Blocks → komponen penyusun yang digunakan dalam solusi.

TOGAF ADM memberikan fokus pada pengelolaan risiko dalam pengembangan arsitektur sistem informasi. Dengan mengikuti metodologi ini, organisasi dapat mengidentifikasi risiko potensial di setiap tahap pengembangan dan merumuskan strategi mitigasi yang tepat. Pendekatan ini sangat penting untuk menghindari masalah yang mungkin muncul di kemudian hari, sehingga meningkatkan keberhasilan implementasi sistem informasi. Terakhir, keuntungan lain dari TOGAF adalah kemampuannya untuk diintegrasikan dengan standar dan kerangka kerja lain, seperti ISO/IEC 27001. Hal ini memungkinkan organisasi untuk mengembangkan sistem informasi yang tidak hanya efektif tetapi juga aman dan dapat dipercaya, serta memenuhi regulasi dan standar industri yang berlaku.