Peradaban Journal of Interdisciplinary EDUCATIONAL RESEARCH
e-ISSN: 3025-2121
Volume 4, Issue 1, February 2026, pp. 37–49
DOI: https://doi.org/10.59001/pjier.v4i1.803

Article

Model Tata Kelola Keamanan Data pada Ekosistem Pendidikan Muhammadiyah : Sintesis ISO 27001:2022 dan Nilai PHIWM

Ady Suprayitno
Universitas Ahmad Dahlan, Yogyakarta, Indonesia; Universitas Muhammadiyah Magelang, Magelang, Indonesia;
email: *rahmat.aiman@unm.ac.id*

Abstract

Digital transformation requires educational institutions to manage data as a strategic asset to support learning and academic services, yet it simultaneously increases the complexity of security risks. Muhammadiyah, as an organization overseeing thousands of educational units, faces challenges with fragmented data security governance due to its federative organizational structure. This research aims to develop a federated data security governance model through the synthesis of the ISO/IEC 27001:2022 standard and the values of the Islamic Pedagogy of Life for Muhammadiyah Members (Pedoman Hidup Islami Warga Muhammadiyah or PHIWM). Utilizing a conceptual literature review approach with content and thematic analysis, this study examines international standards, normative organizational documents, and relevant scientific literature. The results formulate a "centralized policy and distributed execution" model that integrates strategic leadership, policy formulation, shared security services, and technical implementation at the educational unit level. This model offers a balance between organizational standardization and operational flexibility for educational institutions, grounded in the ethics of science and technology. This research contributes to the

development of a value-based data security governance framework for the digital education ecosystem within Muhammadiyah and similar educational organizations.

Keyword
Data Security, Digital Education, Federated Governance, ISO 27001:2022, Muhammadiyah, PHIWM

Abstrak

Transformasi digital menuntut institusi pendidikan mengelola data sebagai aset strategis untuk mendukung pembelajaran dan layanan akademik, namun hal ini juga meningkatkan kompleksitas risiko keamanan. Muhammadiyah, sebagai organisasi dengan ribuan Amal Usaha Muhammadiyah (AUM) di bidang pendidikan, menghadapi tantangan tata kelola keamanan data yang terfragmentasi akibat struktur organisasi yang federatif. Penelitian ini bertujuan menyusun model tata kelola keamanan data terfederasi melalui sintesis standar ISO/IEC 27001:2022 dan nilai Pedoman Hidup Islami Warga Muhammadiyah (PHIWM). Menggunakan metode conceptual literature review dengan analisis isi dan tematik, penelitian ini mengkaji dokumen standar internasional, dokumen normatif organisasi, dan literatur terkait. Hasil penelitian merumuskan model centralized policy and distributed execution yang mengintegrasikan lapisan kepemimpinan strategis hingga pelaksanaan teknis di tingkat unit pendidikan. Model ini menawarkan keseimbangan antara standardisasi kebijakan organisasi dan fleksibilitas operasional institusi pendidikan dengan landasan nilai etika IPTEK. Penelitian ini berkontribusi dalam pengembangan kerangka tata kelola keamanan data berbasis nilai bagi ekosistem pendidikan digital Muhammadiyah dan organisasi pendidikan serupa.

Kata Kunci
ISO 27001:2022, Keamanan Data, Muhammadiyah, PHIWM, Tata Kelola Terfederasi.

PENDAHULUAN

Transformasi digital dalam sektor pendidikan telah mendorong institusi pendidikan untuk mengelola data sebagai aset strategis yang mendukung proses pembelajaran, pengelolaan akademik, penelitian, serta pelayanan kepada mahasiswa dan masyarakat. Perguruan tinggi dan lembaga pendidikan modern kini bergantung pada berbagai sistem informasi, seperti sistem informasi akademik, sistem manajemen pembelajaran, serta layanan administrasi digital yang menghasilkan dan mengelola data dalam jumlah besar (Bisyri, Santoso, & Maryati, 2023). Dalam situasi tersebut, keamanan data menjadi isu yang semakin krusial karena kebocoran atau penyalahgunaan data tidak hanya berdampak pada operasional institusi, tetapi juga berpotensi menurunkan kepercayaan sivitas akademika serta memengaruhi kualitas tata kelola pendidikan (Aidah, Arifudin, & Ibrahim, 2024).

Dalam perspektif pendidikan interdisipliner, data yang dikelola oleh institusi pendidikan tidak terbatas pada aktivitas akademik, tetapi juga mencakup data administrasi, kepegawaian, keuangan, penelitian, serta berbagai layanan publik yang terhubung dengan ekosistem pendidikan. Ketergantungan yang semakin tinggi terhadap sistem digital menyebabkan kompleksitas pengelolaan dan perlindungan data juga meningkat. Tantangan ini menjadi semakin signifikan terutama pada organisasi pendidikan berskala besar yang memiliki struktur terdesentralisasi dan unit kerja yang beragam, sehingga memerlukan kerangka tata kelola keamanan data yang terkoordinasi secara sistematis (Felix C

Aguboshim, Ifeyinwa N Obiokafor, & Anastasia O Emenike, 2023).

Muhammadiyah merupakan salah satu organisasi keagamaan yang memiliki jaringan lembaga pendidikan terbesar di Indonesia, yang mencakup ribuan sekolah dasar dan menengah, ratusan perguruan tinggi, serta berbagai lembaga pendidikan nonformal (Fikar, 2024). Dalam ekosistem pendidikan Muhammadiyah, berbagai aktivitas akademik dan kelembagaan menghasilkan beragam jenis data, seperti data mahasiswa dan siswa, data akademik, data penelitian, data kepegawaian, serta data administrasi institusi. Digitalisasi layanan pendidikan yang terus berkembang menyebabkan pengelolaan data tersebut menjadi semakin kompleks dan membutuhkan tata kelola keamanan informasi yang memadai agar data akademik dan kelembagaan dapat terlindungi secara optimal (Muhammadiyah, 2007). Kondisi ini berdampak pada fragmentasi tata kelola data, perbedaan standar pengamanan informasi, serta lemahnya koordinasi keamanan data lintas unit. Berdasarkan berbagai kajian terdahulu, hingga saat ini belum terdapat kebijakan maupun model tata kelola keamanan data yang terintegrasi secara terpusat ataupun terfederasi di tingkat organisasi Muhammadiyah (Fathurohman, Setiawan, & Darmawan, 2025; Syafruddin Akbar & Haryanti, 2024).

Karakteristik Muhammadiyah sebagai organisasi yang bersifat federatif, dengan tingkat otonomi yang tinggi pada setiap Amal Usaha Muhammadiyah (AUM), menyebabkan pengelolaan sistem informasi pendidikan dan data kelembagaan sering kali dilakukan secara mandiri oleh masing-masing unit (Fikar, 2024). Kondisi ini memberikan fleksibilitas dalam pengelolaan layanan pendidikan di tingkat lokal, namun pada saat yang sama dapat menimbulkan fragmentasi dalam standar keamanan data dan tata kelola sistem informasi. Perbedaan kapasitas sumber daya teknologi, kebijakan pengamanan data, serta praktik pengelolaan informasi antar institusi pendidikan Muhammadiyah berpotensi meningkatkan risiko keamanan data jika tidak diimbangi dengan kerangka tata kelola yang terkoordinasi secara organisasi. Sejumlah penelitian telah dilakukan untuk mengkaji aspek keamanan data dan sistem informasi di lingkungan Muhammadiyah. Beberapa studi berfokus pada evaluasi keamanan sistem informasi di rumah sakit dan perguruan tinggi Muhammadiyah dengan menggunakan kerangka kerja tata kelola teknologi informasi, seperti ISO 27001 dan COBIT (Iqbal, 2024; Nugroho & Rochmadi, 2024). Hasil penelitian tersebut umumnya menunjukkan bahwa sistem yang dikaji berada pada kondisi cukup baik atau sesuai dengan standar yang digunakan, namun masih memerlukan perbaikan pada aspek prosedural dan pengendalian internal. Meskipun demikian, kajian-kajian tersebut masih terbatas pada lingkup unit tertentu dan belum diarahkan pada perancangan kebijakan keamanan data yang bersifat lintas amal usaha dan terkoordinasi secara organisasi (Nursyarif, Sumadi, & Arbansyah, 2024; Rahmatullah, 2025; Wiliam Aryanda, 2022).

Penelitian lain menyoroti upaya peningkatan keamanan data melalui pendekatan literasi dan sosialisasi keamanan digital, khususnya pada lingkungan pendidikan dan sistem internal Muhammadiyah. Pendekatan ini berkontribusi pada peningkatan kesadaran pengguna terhadap risiko keamanan data, namun masih berada pada tataran edukatif dan operasional. Selain itu, inisiatif pembentukan layanan keamanan siber di lingkungan Muhammadiyah menunjukkan adanya kesadaran organisasi terhadap pentingnya keamanan informasi, tetapi belum dikembangkan sebagai kerangka tata kelola keamanan data yang bersifat strategis dan berlaku lintas unit (Ilmiana et al., 2025; MPI, 2025).

Di luar konteks Muhammadiyah, penelitian pada sektor lain, seperti organisasi keuangan dan fintech, telah mengusulkan model tata kelola keamanan data berbasis standar internasional dan manajemen risiko untuk mengatasi kompleksitas pengelolaan data terdistribusi. Model-model tersebut menunjukkan bahwa pendekatan tata kelola terfederasi dapat menjadi solusi bagi organisasi dengan struktur yang kompleks. Namun, model yang dikembangkan umumnya berorientasi pada organisasi komersial dan belum mempertimbangkan konteks organisasi nirlaba berbasis nilai keagamaan, sehingga kurang relevan jika diadopsi secara langsung pada lingkungan Muhammadiyah (Lestari, Puspita, Wijaya, & Vicky, 2025).

Selain aspek teknis dan struktural, Muhammadiyah memiliki Pedoman Hidup Islami Warga Muhammadiyah (PHIWM) sebagai landasan nilai dan etika dalam menjalankan kehidupan organisasi. Nilai-nilai seperti amanah, keadilan, tanggung jawab, dan kemaslahatan memiliki keterkaitan yang kuat dengan prinsip-prinsip keamanan data, khususnya dalam hal perlindungan hak pemilik data dan akuntabilitas pengelola data. Namun demikian, penelitian yang mengintegrasikan nilai-nilai PHIWM secara eksplisit ke dalam kerangka tata kelola keamanan data masih sangat terbatas. Nilai-nilai tersebut umumnya dipahami secara normatif, tetapi belum disintesis secara sistematis dengan standar keamanan informasi modern sebagai bagian dari desain tata kelola organisasi (Faradhilla & Sipahutar, 2024; Utomo & Rokhmah, 2022).

Berdasarkan telaah terhadap penelitian-penelitian terdahulu tersebut, dapat disimpulkan bahwa kajian keamanan data di lingkungan Muhammadiyah masih bersifat parsial, terfragmentasi, dan didominasi oleh pendekatan teknis atau operasional pada level unit. Belum ditemukan penelitian yang mengusulkan suatu model tata kelola keamanan data yang bersifat terfederasi, terstandar secara organisasi, serta mengintegrasikan standar keamanan informasi internasional dengan nilai-nilai PHIWM secara eksplisit sebagai landasan normatif. Kesenjangan penelitian pada level tata kelola strategis inilah yang menjadi dasar perlunya penelitian ini dilakukan.

Penelitian ini bertujuan untuk menyusun model tata kelola keamanan data terfederasi Muhammadiyah melalui sintesis antara standar ISO/IEC 27001:2022 dan nilai-nilai PHIWM. Melalui pendekatan literature review konseptual, penelitian ini diharapkan dapat memberikan kontribusi teoretis berupa pengembangan kerangka tata kelola keamanan data berbasis nilai, serta kontribusi praktis sebagai rujukan kebijakan keamanan data bagi organisasi pendidikan dan amal usaha Muhammadiyah dalam konteks pendidikan interdisipliner.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan *literature review* konseptual untuk merumuskan model tata kelola keamanan data terfederasi Muhammadiyah melalui sintesis antara standar keamanan informasi dan nilai organisasi. Pendekatan ini dipilih karena penelitian tidak bertujuan melakukan pengujian empiris atau implementasi sistem, melainkan mengembangkan kerangka konseptual tata kelola yang relevan dengan karakter organisasi pendidikan dan sosial berbasis nilai.

Sumber data penelitian terdiri atas dokumen standar internasional ISO/IEC

27001:2022, dokumen normatif organisasi berupa Pedoman Hidup Islami Warga Muhammadiyah (PHIWM), serta artikel ilmiah dan laporan penelitian terdahulu yang membahas keamanan data, tata kelola teknologi informasi, dan pengelolaan data pada organisasi terdistribusi. Literatur dipilih berdasarkan relevansi topik, kredibilitas sumber, dan keterkaitan dengan konteks organisasi Muhammadiyah maupun organisasi sejenis.

Analisis data dilakukan melalui analisis isi (*content analysis*) dan analisis tematik (*thematic analysis*) untuk mengidentifikasi prinsip, kontrol, dan nilai yang relevan dengan tata kelola keamanan data. Hasil analisis kemudian disintesis secara konseptual melalui proses pemetaan antara kontrol ISO/IEC 27001:2022 dan nilai-nilai PHIWM, yang selanjutnya digunakan sebagai dasar perancangan model tata kelola keamanan data terfederasi Muhammadiyah.

HASIL DAN PEMBAHASAN

Kondisi Eksisting Tata Kelola Data di Muhammadiyah

Berdasarkan hasil telaah literatur, tata kelola data di lingkungan Muhammadiyah, khususnya pada sektor pendidikan, masih bersifat terfragmentasi dan dikelola secara mandiri oleh masing-masing Amal Usaha Muhammadiyah (AUM). Jaringan pendidikan Muhammadiyah yang terdiri dari sekolah, perguruan tinggi, dan berbagai lembaga pendidikan lainnya menghasilkan beragam jenis data pendidikan, seperti data siswa dan mahasiswa, data akademik, data penelitian, data kepegawaian, serta data administrasi kelembagaan. Dalam praktiknya, setiap institusi pendidikan Muhammadiyah umumnya mengembangkan dan mengelola sistem informasi pendidikan secara independen sesuai dengan kebutuhan lokal. Pola pengelolaan yang bersifat otonom ini memberikan fleksibilitas operasional bagi masing-masing institusi, namun pada saat yang sama menimbulkan tantangan dalam konsistensi standar keamanan data, integrasi sistem informasi pendidikan, serta pengendalian risiko keamanan informasi secara organisasi (Fathurohman, Setiawan, & Darmawan, 2025; Syafruddin Akbar & Haryanti, 2024).

Sejumlah penelitian menunjukkan bahwa upaya pengamanan data di lingkungan Muhammadiyah umumnya dilakukan melalui pendekatan evaluatif dan teknis pada level institusi pendidikan tertentu, seperti audit sistem informasi akademik, penilaian kepatuhan terhadap kerangka kerja tata kelola teknologi informasi, serta peningkatan literasi keamanan digital bagi sivitas akademika. Pendekatan tersebut berkontribusi pada peningkatan kesadaran keamanan data di tingkat institusi, namun sebagian besar masih terbatas pada lingkup unit tertentu dan belum membentuk kerangka kebijakan keamanan data yang terkoordinasi lintas lembaga pendidikan Muhammadiyah. Akibatnya, pengelolaan risiko keamanan data pendidikan masih sangat bergantung pada kapasitas masing-masing institusi, baik dari sisi sumber daya manusia, infrastruktur teknologi, maupun kebijakan internal yang dimiliki (Ilmiana et al., 2025; MPI, 2025; Syauqil et al., 2024). Meskipun pendekatan tersebut penting, fokus yang terlalu lokal dan operasional menyebabkan belum terbentuknya kebijakan keamanan data yang terkoordinasi dan berlaku lintas AUM. Akibatnya, pengelolaan risiko keamanan data masih bergantung pada kapasitas masing-masing unit dan belum berada dalam satu kerangka tata kelola strategis .

Temuan tersebut menunjukkan bahwa ekosistem pendidikan Muhammadiyah yang

luas dan terdistribusi membutuhkan pendekatan tata kelola keamanan data yang mampu menjaga keseimbangan antara otonomi institusi pendidikan dan kebutuhan standardisasi kebijakan keamanan informasi secara organisasi. Dalam organisasi pendidikan berskala besar dengan struktur terdesentralisasi, pendekatan tata kelola terfederasi sering dipandang sebagai solusi yang memungkinkan koordinasi kebijakan keamanan data secara terpusat, sekaligus tetap memberikan ruang fleksibilitas bagi masing-masing institusi dalam mengelola sistem informasi pendidikan mereka (Zhang, 2024). Dalam konteks ini, pendekatan tata kelola terfederasi menjadi relevan untuk menjawab kompleksitas pengelolaan data di lingkungan lembaga pendidikan Muhammadiyah dan perserikatan secara umum.

Analisis Kerangka ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Data

ISO/IEC 27001:2022 merupakan standar internasional yang menyediakan kerangka kerja sistematis dalam membangun Sistem Manajemen Keamanan Informasi (*Information Security Management System* / ISMS). Standar ini dirancang untuk membantu organisasi mengelola risiko keamanan informasi secara terstruktur melalui pendekatan berbasis manajemen risiko, pengendalian keamanan informasi, serta mekanisme evaluasi dan perbaikan berkelanjutan. Dalam kerangka tersebut, ISO/IEC 27001:2022 menekankan pentingnya komitmen kepemimpinan organisasi, perumusan kebijakan keamanan informasi, identifikasi dan perlindungan aset informasi, pengendalian akses terhadap data, serta proses monitoring dan audit yang berkesinambungan (ISO/IEC 27001, 2022).

Dalam konteks organisasi pendidikan yang semakin bergantung pada sistem informasi digital, kerangka kerja ISO/IEC 27001:2022 menjadi semakin relevan. Institusi pendidikan saat ini mengelola berbagai jenis data strategis, seperti data akademik mahasiswa dan siswa, data penelitian, data kepegawaian, serta data administrasi kelembagaan yang terintegrasi dalam berbagai sistem informasi pendidikan. Kerentanan terhadap ancaman keamanan siber, kebocoran data, maupun penyalahgunaan informasi menuntut adanya sistem tata kelola keamanan data yang mampu menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi sebagai tiga prinsip utama dalam manajemen keamanan informasi.

Namun demikian, penerapan ISO/IEC 27001:2022 secara seragam pada organisasi yang memiliki struktur federatif seperti Muhammadiyah menghadapi sejumlah tantangan struktural. Ekosistem Muhammadiyah yang terdiri dari berbagai Amal Usaha Muhammadiyah (AUM), termasuk sekolah dan perguruan tinggi yang tersebar di berbagai wilayah, memiliki tingkat otonomi kelembagaan yang relatif tinggi. Setiap institusi pendidikan Muhammadiyah umumnya mengembangkan sistem informasi dan praktik pengelolaan data yang disesuaikan dengan kebutuhan operasional masing-masing. Perbedaan kapasitas sumber daya manusia, infrastruktur teknologi, serta kebijakan internal menyebabkan penerapan standar keamanan informasi secara terpusat dan seragam berpotensi kurang efektif jika tidak mempertimbangkan keragaman kondisi tersebut.

Dalam situasi tersebut, ISO/IEC 27001:2022 perlu diposisikan tidak semata sebagai standar teknis yang diterapkan secara identik pada seluruh unit organisasi, melainkan sebagai kerangka kebijakan dan kontrol strategis yang memberikan arah tata kelola keamanan data pada tingkat organisasi. Pendekatan ini memungkinkan organisasi

menetapkan prinsip, kebijakan, serta standar minimum keamanan informasi secara terpusat, sementara implementasi teknisnya dapat disesuaikan dengan konteks operasional masing-masing institusi pendidikan. Dengan demikian, standar ISO/IEC 27001:2022 dapat berfungsi sebagai kerangka koordinasi tata kelola keamanan data yang menjaga konsistensi kebijakan organisasi sekaligus tetap memberikan ruang adaptasi bagi unit-unit pendidikan yang memiliki karakteristik berbeda.

Melalui pendekatan tersebut, ISO/IEC 27001:2022 tidak hanya dipahami sebagai standar teknis pengamanan sistem informasi, tetapi juga sebagai instrumen tata kelola yang mendukung pengambilan keputusan strategis dalam pengelolaan keamanan data pada organisasi pendidikan yang bersifat terdistribusi. Dalam konteks Muhammadiyah, pemanfaatan kerangka ini berpotensi memperkuat tata kelola keamanan data pendidikan secara lebih terkoordinasi, sekaligus mendukung pengembangan ekosistem pendidikan digital yang aman, terpercaya, dan berkelanjutan.

Nilai PHIWM dalam Konteks Keamanan dan Tata Kelola Data

Pedoman Hidup Islami Warga Muhammadiyah (PHIWM) tidak hanya memuat nilai-nilai etika umum, tetapi juga memberikan panduan prinsipil dalam pengembangan dan pemanfaatan ilmu pengetahuan dan teknologi (IPTEK). Dalam pokok kehidupan Muhammadiyah di bidang IPTEK, ditegaskan bahwa penguasaan dan penggunaan teknologi harus diarahkan untuk kemaslahatan umat, dilaksanakan secara bertanggung jawab, serta tidak menimbulkan kerusakan atau ketidakadilan. Prinsip tersebut memiliki relevansi langsung dengan tata kelola keamanan data, mengingat data dan sistem informasi merupakan produk utama dari perkembangan IPTEK di era digital (PP Muhammadiyah, 2018).

Dalam konteks keamanan data, nilai amanah dalam PHIWM bidang IPTEK dapat dimaknai sebagai tanggung jawab moral dan institusional dalam menjaga kepercayaan pemilik data, baik sivitas akademika maupun masyarakat. Nilai keadilan berkaitan dengan pengaturan hak akses dan pemanfaatan data secara proporsional, sehingga tidak terjadi penyalahgunaan informasi atau diskriminasi berbasis akses teknologi. Sementara itu, nilai tanggung jawab dan kemaslahatan menekankan bahwa pengelolaan teknologi informasi, termasuk sistem pengolahan data, harus berorientasi pada perlindungan kepentingan publik dan martabat manusia.

Dengan demikian, keamanan data dalam perspektif PHIWM bidang IPTEK tidak dipahami semata-mata sebagai mekanisme teknis pengamanan sistem, melainkan sebagai bagian dari etika pemanfaatan teknologi yang bertanggung jawab. Pendekatan ini memperluas makna keamanan data dari sekadar kepatuhan teknis menjadi instrumen tata kelola yang selaras dengan visi tajdid Muhammadiyah dalam mengembangkan IPTEK yang berkemajuan dan berkeadaban.

Sintesis ISO/IEC 27001:2022 dan Nilai PHIWM

Sintesis antara kontrol ISO/IEC 27001:2022 dan nilai-nilai PHIWM dalam penelitian ini dilakukan dengan pendekatan tata kelola berlapis yang menyesuaikan struktur organisasi Muhammadiyah. Setiap lapisan tata kelola dipetakan berdasarkan fungsi teknis keamanan data serta dikaitkan dengan nilai PHIWM yang relevan, sehingga membentuk kerangka tata

kelola keamanan data yang bersifat teknis sekaligus bernilai.

Untuk memperjelas pemetaan antara fungsi teknis ISO/IEC 27001:2022 dan integrasi nilai-nilai PHIWM pada setiap lapisan tata kelola, sintesis kontrol keamanan data dirangkum dalam Tabel 1.

Tabel 1. Sintesis Kontrol ISO/IEC 27001:2022 dan Nilai PHIWM dalam Tata Kelola Keamanan Data
(diadaptasi dari ISO/IEC, 2022; PP Muhammadiyah, 2018)

Komponen Diagram	Fungsi Teknis (ISO 27001:2022)	Integrasi Nilai PHIWM
PP Muhammadiyah *(Supreme Governance)*	***Governance Body* (Klausul 5.1):** Memberikan mandat strategis dan komitmen kepatuhan keamanan informasi (*Leadership & Commitment*).	**Bab: Kehidupan Berorganisasi** Melaksanakan prinsip *Imamah* (kepemimpinan) dan menjadikan organisasi sebagai alat dakwah *Amar Ma'ruf* dengan mewajibkan sistem yang melindungi umat.
Majelis Pustaka & Informasi *(Strategic Layer)*	***Policy Maker* (Klausul 5.2):** Menetapkan kebijakan keamanan nasional. **Identity Provider (A.9.1):** Mengelola identitas tunggal (NBM) sebagai *Root of Trust*.	**Bab: Kehidupan dalam Mengelola Amal Usaha** Menjalankan prinsip *Amanah* (akuntabilitas) dalam mengelola aset digital persyarikatan sebagai titipan yang harus dipertanggungjawabkan.
Muhammadiyah *Security Center* *(Shared Service)*	***Threat Intelligence* (A.5.7):** Analisis dan penyebaran info ancaman siber. **Incident Response (A.16.1):** Pusat koordinasi penanganan insiden.	**Bab: Kehidupan Bermasyarakat** Mengamalkan prinsip *Ta'awun* (tolong-menolong) antar elemen persyarikatan untuk mencegah *Fasad* (kerusakan/serangan) pada sistem orang lain.
AUM / ORTOM *(Operational Layer)*	***Executor* (A.8 - A.10):** Penerapan kontrol teknis (Enkripsi, Logging, Firewall) secara presisi.	**Bab: Kehidupan dalam IPTEK & Profesi** 1. **IPTEK:** Menguasai teknologi keamanan terkini sebagai sarana ibadah/dakwah. 2. **Itqan:** Profesionalitas kerja dalam menjaga integritas data.

Tabel diatas menunjukkan bahwa integrasi nilai PHIWM tidak bersifat simbolik, tetapi terdistribusi secara fungsional pada setiap lapisan tata kelola keamanan data, mulai dari tingkat kepemimpinan strategis hingga pelaksanaan teknis di tingkat AUM dan Ortom. Nilai PHIWM berperan sebagai landasan normatif yang memperkuat penerapan kontrol ISO/IEC 27001:2022, khususnya pada aspek kepemimpinan, akuntabilitas, kolaborasi keamanan, dan profesionalisme dalam pengelolaan IPTEK. Dengan demikian, tabel ini menegaskan bahwa tata kelola keamanan data Muhammadiyah dirancang sebagai sistem yang koheren antara standar internasional dan nilai organisasi.

Model Tata Kelola Keamanan Data Terfederasi Muhammadiyah

Berdasarkan sintesis antara kontrol ISO/IEC 27001:2022 dan nilai-nilai PHIWM yang dirangkum, penelitian ini mengusulkan model tata kelola keamanan data terfederasi Muhammadiyah. Model ini dirancang untuk menjawab tantangan pengelolaan keamanan data pada organisasi yang bersifat terdistribusi, dengan tetap menjaga keseimbangan antara

otonomi unit dan konsistensi kebijakan keamanan data secara organisasi.

Model yang diusulkan mengadopsi prinsip *centralized policy and distributed execution*, di mana arah kebijakan, standar, dan komitmen keamanan data ditetapkan secara terpusat pada tingkat organisasi, sementara pelaksanaan teknis dan operasional dilakukan oleh masing-masing unit sesuai dengan konteks dan kapasitas lokal (Chen, 2020). Pendekatan ini dipandang lebih adaptif bagi organisasi besar dengan struktur federatif seperti Muhammadiyah, dibandingkan dengan pendekatan sentralisasi penuh yang berpotensi mengurangi fleksibilitas unit. Untuk memperjelas struktur dan relasi antar komponen dalam model tata kelola keamanan data terfederasi yang diusulkan, arsitektur model disajikan dalam Gambar 1.

Gambar 1. Model Tata Kelola Keamanan Data Terfederasi Muhammadiyah

Gambar diatas menunjukkan model tata kelola keamanan data yang terdiri atas beberapa lapisan utama. Pada lapisan *supreme governance*, PP Muhammadiyah berperan sebagai pengambil keputusan strategis yang menetapkan arah kebijakan dan komitmen keamanan data organisasi. Lapisan ini berfungsi memastikan bahwa keamanan data menjadi bagian dari agenda strategis organisasi dan selaras dengan nilai-nilai PHIWM.

Pada lapisan *strategic layer*, Majelis Pustaka dan Informasi berperan sebagai perumus kebijakan dan pengelola standar keamanan data, termasuk pengaturan identitas dan pengendalian akses sebagai fondasi kepercayaan (*root of trust*). Lapisan ini menjembatani kebijakan strategis dengan kebutuhan operasional, sehingga standar keamanan data dapat diterapkan secara konsisten lintas unit.

Lapisan *shared service* direpresentasikan oleh Muhammadiyah Security Center, yang berfungsi sebagai pusat koordinasi keamanan data, khususnya dalam hal analisis ancaman dan penanganan insiden. Keberadaan layanan bersama ini memungkinkan terjadinya kolaborasi keamanan data antar AUM, sehingga risiko keamanan dapat dideteksi dan ditangani secara kolektif tanpa harus menghilangkan kemandirian masing-masing unit.

Pada lapisan *operational layer*, AUM dan Ortom bertindak sebagai pelaksana kebijakan dengan menerapkan kontrol teknis keamanan data sesuai standar yang ditetapkan. Penerapan kontrol teknis ini diposisikan sebagai wujud profesionalisme (*itqan*) dalam pengelolaan IPTEK, di mana penguasaan teknologi keamanan informasi digunakan secara bertanggung jawab untuk menjaga integritas dan keandalan data.

Secara keseluruhan, model tata kelola keamanan data terfederasi yang diusulkan mengintegrasikan aspek kepemimpinan strategis, perumusan kebijakan, layanan keamanan bersama, serta pelaksanaan kontrol teknis pada tingkat unit dalam satu kerangka yang koheren. Pendekatan ini relevan dengan berbagai temuan penelitian mengenai tata kelola teknologi informasi di institusi pendidikan yang menunjukkan bahwa pengelolaan layanan TI sering kali dilakukan secara otonom oleh masing-masing unit tanpa koordinasi kebijakan yang memadai (Suhartini & Herwidyaningtyas, 2024). Kondisi tersebut berpotensi menimbulkan ketidakkonsistenan standar keamanan informasi dan meningkatkan risiko dalam pengelolaan data organisasi. Dalam perspektif tata kelola keamanan informasi, keberadaan kerangka kebijakan yang jelas juga penting untuk memastikan pengelolaan risiko data serta kepatuhan terhadap regulasi perlindungan data (Atmojo, 2023).

Dalam konteks organisasi pendidikan yang memiliki banyak unit otonom, pendekatan tata kelola terfederasi menjadi lebih adaptif dibandingkan model sentralisasi penuh karena memungkinkan standardisasi kebijakan keamanan informasi tanpa menghilangkan kemandirian institusi pendidikan dalam mengelola sistem informasinya. Model tata kelola yang mengombinasikan koordinasi kebijakan secara terpusat dengan implementasi yang fleksibel pada tingkat unit memungkinkan organisasi pendidikan besar mengelola kompleksitas sistem informasi yang berkembang seiring dengan transformasi digital dalam proses pembelajaran, administrasi akademik, dan layanan institusional.

Berbeda dengan sebagian besar model tata kelola keamanan data yang berorientasi pada organisasi komersial atau sektor teknologi, model yang diusulkan dalam penelitian ini mengintegrasikan dimensi nilai organisasi melalui sintesis antara kerangka teknis ISO/IEC 27001:2022 dan nilai-nilai Pedoman Hidup Islami Warga Muhammadiyah (PHIWM). Integrasi ini menunjukkan bahwa tata kelola keamanan data tidak hanya dipahami sebagai mekanisme teknis pengamanan sistem informasi, tetapi juga sebagai bagian dari etika pemanfaatan teknologi yang menekankan prinsip amanah, tanggung jawab, dan kemaslahatan dalam pengelolaan data. Dengan demikian, model yang diusulkan memperluas pendekatan tata kelola keamanan data dari perspektif teknis menuju kerangka tata kelola berbasis nilai (*value-based governance*), yang berpotensi menjadi rujukan konseptual bagi pengembangan kebijakan keamanan data pada organisasi pendidikan Muhammadiyah maupun institusi pendidikan berbasis nilai lainnya.

KESIMPULAN

Berdasarkan hasil kajian literatur dan analisis konseptual, dapat disimpulkan bahwa pengelolaan keamanan data di lingkungan Muhammadiyah, khususnya dalam ekosistem pendidikan yang mencakup sekolah, perguruan tinggi, serta berbagai layanan pendidikan digital, masih bersifat terfragmentasi dan berfokus pada lingkup unit masing-masing Amal Usaha Muhammadiyah (AUM). Kondisi tersebut menyebabkan belum terbentuknya kerangka

tata kelola keamanan data yang terkoordinasi secara strategis lintas institusi pendidikan Muhammadiyah. Fragmentasi pengelolaan data ini berpotensi menimbulkan tantangan dalam konsistensi kebijakan, pengendalian risiko keamanan informasi, serta perlindungan data akademik dan data sivitas akademika secara organisasi. Hasil penelitian menunjukkan bahwa ISO/IEC 27001:2022 memiliki relevansi yang kuat sebagai kerangka teknis dalam pengembangan tata kelola keamanan data pada institusi pendidikan yang semakin bergantung pada sistem informasi digital. Namun demikian, penerapan standar tersebut perlu diadaptasi agar sesuai dengan karakter organisasi Muhammadiyah yang bersifat federatif dan memiliki tingkat otonomi tinggi pada masing-masing lembaga pendidikan. Integrasi dengan nilai-nilai Pedoman Hidup Islami Warga Muhammadiyah (PHIWM), khususnya pada dimensi kehidupan berorganisasi, pengelolaan amal usaha, kehidupan bermasyarakat, serta kehidupan dalam IPTEK dan profesi, memungkinkan penerapan standar keamanan data yang tidak hanya sah secara teknis, tetapi juga memiliki legitimasi normatif dan kultural dalam pengelolaan institusi pendidikan berbasis nilai. Sintesis ini menunjukkan bahwa keamanan data dapat diposisikan sebagai bagian dari etika pemanfaatan teknologi informasi dalam pendidikan yang bertanggung jawab dan berorientasi pada kemaslahatan. Sebagai kontribusi utama, penelitian ini mengusulkan model tata kelola keamanan data terfederasi yang mengadopsi prinsip *centralized policy and distributed execution*. Model tersebut mengintegrasikan peran kepemimpinan strategis, perumusan kebijakan, layanan keamanan bersama, serta pelaksanaan kontrol teknis pada tingkat institusi pendidikan dalam satu kerangka tata kelola yang koheren. Model ini tidak dimaksudkan sebagai desain implementasi teknis, melainkan sebagai rujukan konseptual bagi pengembangan kebijakan keamanan data dan tata kelola sistem informasi pendidikan di lingkungan Muhammadiyah, khususnya dalam pengelolaan data akademik, administrasi pendidikan, serta layanan pendidikan digital yang terus berkembang. Penelitian ini memiliki keterbatasan karena bersifat konseptual dan belum diuji melalui implementasi empiris pada institusi pendidikan Muhammadiyah tertentu. Oleh karena itu, penelitian selanjutnya dapat diarahkan pada validasi model melalui pendekatan studi kasus pada sekolah atau perguruan tinggi Muhammadiyah, *expert judgment*, maupun penerapan terbatas untuk menguji kelayakan dan efektivitas model yang diusulkan dalam konteks pengelolaan sistem informasi pendidikan. Selain itu, pengembangan instrumen kebijakan turunan serta panduan implementasi teknis bagi institusi pendidikan Muhammadiyah juga menjadi peluang penelitian lanjutan yang relevan.

DAFTAR PUSTAKA

Aguboshim, F. C., Obiokafor, I. N., & Emenike, A. O. (2023). Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review. *World Journal of Advanced Research and Reviews, 17*(2), 378–385. doi:10.30574/wjarr.2023.17.2.0154

Aidah, A., Arifudin, O., & Ibrahim, T. (2024). Pengembangan sistem informasi manajemen dalam dunia pendidikan. *Jurnal Tahsinia, 5*(6), 966–977. doi:10.57171/jt.v5i6.604

Akbar, I. S., & Haryanti, T. (2024). Penerapan framework COBIT 5 pada domain DSS untuk mengidentifikasi keamanan tata kelola website universitas swasta di Surakarta. *Journal of Computer Science, 5*(2), 12–17.

Aryanda, W. (2022). *Evaluation information security on Universitas Muhammadiyah Kalimantan Timur using Indeks KAMI* (Unpublished thesis/report). Universitas Muhammadiyah Kalimantan Timur. Retrieved from https://lib.unnes.ac.id/20002/

Atmojo, Y. P. (2023, Agustus 30). *Manajemen keamanan informasi dan tata kelola TI*. Retrieved March 10, 2026, from LPPM STIKOM Bali website: https://lppm.stikom-bali.ac.id/2023/08/30/manajemen-keamanan-informasi-dan-tata-kelola-ti/

Bisyri, M., Santoso, A., & Maryati, H. (2023). Pemanfaatan teknologi informasi dan komunikasi dalam bidang pendidikan. *Jurnal Sistem Informasi, 12*(2), 70–76. doi:10.51998/jsi.v13i2.536

Chen, G. (2020). A new framework for multi-agent reinforcement learning - centralized training and exploration with decentralized execution via policy distillation. *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS*, 1801–1803.

Faradhilla, A. R., & Sipahutar, L. (2024). Perancangan aplikasi keamanan data nilai siswa pada sekolah SMK Muhammadiyah 04 Medan menggunakan metode RC4 berbasis android. *Seminar Nasional Teknologi Komputer & Informatika (SENADIMU), 1*(1), 1–14. Retrieved from https://senadimu.potensi-utama.ac.id

Fathurohman, A., Setiawan, R., & Darmawan, F. E. (2025). Analisis risiko jaringan komputer untuk meningkatkan kualitas keamanan pada jaringan komputer Rumah Sakit Universitas Muhammadiyah Semarang. *Proceeding of Informatics Collaborations and Dessimenation Meeting Infocoding 2025*, 45–52.

Fikar, R. Z. (2024, November 18). *Refleksi 112 tahun Muhammadiyah*. Retrieved from https://www.suaramuhammadiyah.id/read/refleksi-112-tahun-muhammadiyah

Ilmiana, I. R., Ikram, R., Raihan, H. A., Krisna, B., Rivai, Z. Y., Yudhana, A., & Umar, R. (2025). Peningkatan literasi keamanan dan etika berinternet di SMP Muhammadiyah Al Mujahidin Gunungkidul. *GERVASI: Jurnal Pengabdian Kepada Masyarakat, 9*(2), 1241–1255.

Iqbal, M. (2024). Audit sistem informasi website Universitas Muhammadiyah Purworejo menggunakan COBIT 5 MEA. *Computing Insight: Journal of Computer Science, 5*(2), 34–38. doi:10.30651/comp_insight.v5i2.19332

ISO/IEC 27001. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection*. Retrieved from https://www.v-comply.com/library/iso-27001-annex-a-controls/

Lestari, M., Puspita, M. E., Wijaya, A. F., & Vicky. (2025). Model tata kelola TI terintegrasi untuk keamanan informasi di sektor fintech. *Jurnal Teknologi Dan Manajemen Industri Terapan, 4*(3), 766–776. doi:10.55826/jtmit.v4i3.943

Majelis Pustaka dan Informasi (MPI). (2025, Desember 29). *Menuju digitalisasi data yang aman dan keberlanjutan*. Retrieved from https://www.suaramuhammadiyah.id/read/menuju-digitalisasi-data-yang-aman-dan-keberlanjutan

Muhammadiyah. (2007). *Organisasi otonom Muhammadiyah*. Retrieved December 29, 2025, from https://muhammadiyah.or.id/organisasi-otonom/

Nugroho, S., & Rochmadi, T. (2024). Analysis of information security readiness using the Index KAMI. *Decode: Jurnal Pendidikan Teknologi Informasi, 4*(3), 881–886. doi:10.51454/decode.v4i3.602

Nursyarif, M. K., Sumadi, M. T., & Arbansyah. (2024). Sistem keamanan berbasis sidik jari pada prodi TI Universitas Muhammadiyah Kalimantan Timur. *Jurnal Informatika Polinema,*

11(1), 19–27.

Rahmatullah, W. N. (2025, Desember 29). *Umsida luncurkan UCS, siap jaga aset digital persyarikatan*. Retrieved from https://pwmu.co/umsida-luncurkan-ucs-siap-jaga-aset-digital-persyarikatan/

Suhartini, A. M., & Herwidyaningtyas, F. B. (2024). Tata kelola teknologi informasi pada perguruan tinggi menggunakan ITIL 4. *JUSTIN (Jurnal Sistem dan Teknologi Informasi), 12*(4), 767–775. doi:10.26418/justin.v12i4.86464

Syauqil, M., Eviyanti, A., Rosid, M. A., & Azinar, A. W. (2024). Information systems audit at the Language Center of Muhammadiyah University of Sidoarjo [Audit sistem informasi pada Pusat Bahasa Universitas Muhammadiyah Sidoarjo]. *Journal of Information Systems and Management*, 1–10.

Utomo, I. C., & Rokhmah, S. (2022). Konfigurasi SSL untuk meningkatkan keamanan web server pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta. *Jurnal Rekayasa Teknologi Informasi (JURTI), 6*(2), 143. doi:10.30872/jurti.v6i2.8333

Zhang, X. (2024). A more secure framework for open government data sharing based on federated learning. *Government Information Quarterly, 41*(4), 101981. doi:10.1016/j.giq.2024.101981