Teknika 20 (1): 231-243

JURNAL TEKNIKA
ISSN: 0854-3143
e-ISSN: 2622-3481
Journal homepage: http://jurnal.polsri.ac.id/index.php/teknika
Journal Email: teknika@polsri.ac.id

Pengembangan Model Konseptual ISMS Perguruan Tinggi berbasis *Value Discipline Strategic* dan ISO/IEC 27001:2022 (Annex A)

Yoppy Mirza Maulana[*1]

[*1]Program Studi Sistem Informasi, Universitas Dinamika, Surabaya, Indonesia
*Email Penulis Korespondensi: yoppy@dinamika.ac.id

Abstrak

Perguruan tinggi (PT) memanfaatkan sistem informasi digital untuk mendukung proses akademik, penelitian, administrasi, dan layanan publik, sehingga aset informasi strategis seperti data mahasiswa, hasil penelitian, dan data keuangan perlu dilindungi melalui Information Security Management System (ISMS) yang handal. Meskipun ISO/IEC 27001 menyediakan kerangka kerja standar internasional, implementasinya di PT sering bersifat administratif dan kurang mengaitkan keamanan informasi dengan penciptaan nilai strategis. Penelitian ini mengembangkan model konseptual ISMS berbasis Value Discipline Strategic dalam kerangka ISO/IEC 27001 secara rasional dan teoritis, menggunakan pendekatan konseptual tanpa data empiris. Pengembangan model dilakukan melalui tiga tahap utama: (1) pemetaan domain kontrol ISO/IEC 27001 ke fokus strategis organisasi, (2) penyesuaian kontrol dengan konteks operasional PT, dan (3) perumusan Integrated Value Discipline Strategic ISMS Model. Hasil menunjukkan model ini mampu memetakan hubungan antara orientasi nilai strategis dan domain kontrol ISO/IEC 27001, menjadi pedoman konseptual bagi manajemen PT, serta mendukung pencapaian tujuan strategis melalui efisiensi, kepercayaan, dan inovasi. Penelitian ini memberikan kontribusi teoretis dan praktis, serta membuka peluang penelitian lanjutan untuk mengeksplorasi variabel tambahan seperti kesiapan teknologi dan dinamika risiko informasi.

Kata kunci—*Value Discipline Strategic, ISO/IEC 27001, Perguruan Tinggi, Model Konseptual*

Abstract

Higher education institutions utilize digital information systems to support academic processes, research, administration, and public services, so strategic information assets such as student data, research results, and financial data need to be protected through a reliable Information Security Management System (ISMS). Although ISO/IEC 27001 provides an international standard framework, its implementation in higher education institutions is often administrative and does not link information security to strategic value creation. This study develops a conceptual model of ISMS based on Value Discipline Strategic within the ISO/IEC 27001 framework rationally and theoretically, using a conceptual approach without empirical data. The model development is carried out through three main stages: (1) mapping the ISO/IEC 27001 control domain to the organization's strategic focus, (2) adjusting controls to the

Received: Oktober 28, 2025; Online Available: December 22, 2025

operational context of higher education institutions, and (3) formulating the Integrated Value Discipline ISMS Model. The results show that this model can map the relationship between strategic value orientation and ISO/IEC 27001 control domain, serving as a conceptual guideline for higher education institution management, and supporting the achievement of strategic goals through efficiency, trust, and innovation. This research provides theoretical and practical contributions and opens up opportunities for further research to explore additional variables such as technology readiness and information risk dynamics.

Keywords— *Value Discipline Strategic, ISO/IEC 27001, Higher Education, Conceptual Model*

1. PENDAHULUAN

Perguruan tinggi (PT) memanfaatkan sistem informasi digital untuk mendukung proses pendidikan, penelitian, pengabdian dan administrasi sehingga aset informasi strategis seperti data mahasiswa, hasil penelitian, dan data keuangan perlu dilindungi melalui *Information Security Management System* (ISMS) yang handal [1][2]. ISO/IEC 27001 merupakan standar internasional yang menyediakan kerangka kerja sistematis dalam membangun ISMS, termasuk kebijakan, kontrol, dan prosedur untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi [3][4]. Namun, implementasi ISO/IEC 27001 umumnya di PT cenderung bersifat administratif dan fokus pada kepatuhan formal [2][5], sehingga kurang mengaitkan keamanan informasi dengan penciptaan nilai strategis.

Analisis literatur menunjukkan bahwa penelitian sebelumnya banyak membahas penerapan ISO/IEC 27001 dari sisi kontrol operasional dan kepatuhan [2][6][7][8], sementara dimensi strategis yang mengaitkan keamanan informasi dengan orientasi nilai organisasi belum dikembangkan. Akibatnya, masih kurang model konseptual yang memetakan hubungan antara domain kontrol ISO/IEC 27001 dengan strategi nilai PT. Keamanan informasi sering dipandang semata-mata sebagai fungsi teknis, dan belum dilihat sebagai bagian integral dari strategi organisasi yang dapat menciptakan keunggulan kompetitif. Dalam konteks ini, *value discipline strategic* yang diperkenalkan oleh *Treacy* dan Wiersema memberikan kerangka untuk memahami bagaimana organisasi menciptakan nilai melalui tiga orientasi: efisiensi proses (*Operational Excellence*), kedekatan dan kepercayaan dengan pengguna (*Customer Intimacy*), serta inovasi produk dan layanan (*Product Leadership*) [9][10][11]. Integrasi *value discipline stragic* dengan ISO/IEC 27001 berpotensi menghasilkan ISMS yang tidak hanya menjaga keamanan, tetapi juga mendukung pencapaian tujuan strategis PT. Penelitian sebelumnya mengintegrasikan strategi TI berbasis COBIT 2019 atau strategi pengembangan industri dengan ISO/IEC 27001 [12][13].

Berdasarkan kesenjangan tersebut, penelitian ini mengajukan pertanyaan: bagaimana mengembangkan model konseptual ISMS pada PT berbasis *Value Discipline Strategic* dalam kerangka ISO/IEC 27001. Tujuannya adalah menghasilkan model yang memetakan hubungan antara *Value Discipline Strategic* organisasi dan domain kontrol ISO/IEC 27001. Penelitian ini menggunakan pendekatan konseptual dan rasionalistik tanpa data empiris, dengan mengandalkan studi literatur dan analisis logis terhadap keterkaitan antara fokus strategis organisasi dan kontrol keamanan informasi.

Penelitian ini memberi kontribusi teoretis, praktis, dan normatif. Secara teoretis, penelitian memperluas ISMS menjadi pendekatan *value-based* yang mengaitkan keamanan informasi dengan nilai strategis. Secara praktis, model ini menawarkan pedoman bagi PT dalam menyelaraskan kebijakan keamanan informasi dengan strategi organisasi. Secara normatif, penelitian menegaskan ISO/IEC 27001 sebagai instrumen tata kelola strategis, bukan sekadar kepatuhan. Urgensinya didorong oleh kebutuhan PT untuk menjadikan keamanan informasi sebagai pendorong efisiensi, kepercayaan, dan inovasi di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan konseptual dan rasionalistik, tanpa data empiris, dengan tujuan mengembangkan model konseptual ISMS pada PT berbasis *value discipline Strategic* dan ISO/IEC 27001:2022. Proses pengembangan model dilakukan melalui tiga tahap utama: inisiasi, pengembangan model, dan verifikasi serta penilaian koherensi teoretis.

2.1 Inisiasi

Tahap inisiasi bertujuan membangun fondasi teoritis sebagai dasar pengembangan model ISMS. Fokus utama pada tahap ini adalah kajian literatur mendalam terhadap dua aspek:

2.1.1 ISO/IEC 27001 (Annex A:2022)

Kajian literatur pertama berfokus pada ISO/IEC 27001:2022, khususnya *Annex A* yang memuat daftar kontrol keamanan sebagai bagian integral dari standar *Information Security Management System* (ISMS). Annex A:2022 merujuk langsung pada ISO/IEC 27002:2022 sebagai panduan implementasi kontrol, yang mencakup aspek organisasi, manusia, fisik, dan teknologi [14][15][16]. Dalam konteks Perguruan Tinggi, kontrol strategis seperti kebijakan keamanan informasi, manajemen risiko, tinjauan manajemen, dan keamanan pihak ketiga menjadi penting karena memastikan keselarasan ISMS dengan tujuan strategis organisasi serta menjamin keamanan layanan akademik dan administrasi. Sementara itu, kontrol operasional dan teknis seperti pembatasan hak akses, pemantauan aktivitas sistem, *backup* dan *recovery*, serta keamanan dalam pengembangan dan modifikasi sistem berperan krusial dalam menjaga kontinuitas layanan, ketersediaan data, dan integritas aplikasi akademik maupun penelitian. Kajian mendalam terhadap kontrol ISO/IEC 27001 dan ISO/IEC 27002 memungkinkan pemetaan prioritas kontrol yang relevan dengan konteks strategis PT dalam penelitian ini kontrol ISO/IEC 27001 dan ISO/IEC 27002 ditulis ISO/IEC 27001 (Annex A:2022), sehingga pemilihan kontrol tidak hanya bersifat prosedural tetapi juga berlandaskan logika strategis.

2.1.2 Value Discipline Strategic

Kajian literatur kedua dilakukan terhadap kerangka *Value Discipline Strategic* yang dikembangkan oleh Treacy dan Wiersema. Kerangka ini membagi orientasi nilai organisasi menjadi tiga fokus utama: *Operational Excellence*, *Customer Intimacy*, dan *Product Leadership* [9][10][11]. PT dengan orientasi *Operational Excellence* menekankan efisiensi proses, stabilitas layanan, dan keandalan sistem akademik serta administratif. Orientasi *Customer Intimacy* lebih menitikberatkan pada kepercayaan *stakeholder*, perlindungan data pribadi mahasiswa dan staf, serta layanan yang disesuaikan dengan kebutuhan internal maupun eksternal. Sementara itu, orientasi *Product Leadership* menekankan inovasi, penelitian, dan perlindungan kekayaan intelektual agar hasil riset dan inovasi akademik tetap aman dari kebocoran atau penyalahgunaan. Integrasi *Value Discipline Strategic* ke dalam pengelolaan ISMS memungkinkan prioritas kontrol keamanan informasi ditentukan berdasarkan orientasi strategis PT, sehingga setiap kontrol yang diterapkan memiliki relevansi konseptual dan strategis yang jelas.

Berdasarkan kedua kajian literatur tersebut, tahap inisiasi menghasilkan kerangka konseptual awal yang dinamakan *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*). Kerangka ini memetakan hubungan antara orientasi nilai organisasi, domain kontrol ISO/IEC 27001 (*Annex* A:2022), dan tujuan keamanan informasi PT. Orientasi nilai organisasi berperan sebagai pengarah prioritas kontrol, domain kontrol ISO/IEC 27001 (*Annex* A:2022) menjadi mekanisme untuk mencapai tujuan keamanan, dan konteks PT menentukan relevansi serta skala implementasi. Kerangka konseptual ini menjadi landasan teoritis yang kuat untuk tahap pengembangan model selanjutnya, memastikan bahwa model ISMS yang dihasilkan konsisten secara logis dan sesuai dengan karakteristik strategis PT.

2.2 Pengembangan Model

Tahap pengembangan model bertujuan membangun model konseptual ISMS berbasis *Value Discipline Strategic* secara rinci, menggunakan kerangka yang diperoleh pada tahap inisiasi, yaitu *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*). Pendekatan yang digunakan bersifat konseptual dan rasionalistik, sehingga seluruh tahapan dilakukan melalui analisis literatur, penalaran logis, dan integrasi teori tanpa melibatkan data empiris.

2.2.1 Tahap 1: Penentuan Fokus Strategis dan Orientasi Nilai

Tahap ini memetakan orientasi nilai organisasi dari kerangka *Value Discipline Strategic* ke domain kontrol ISO/IEC 27001 (*Annex* A:2022). Tujuannya adalah menyesuaikan prioritas kontrol dengan fokus strategis PT. PT yang mengutamakan *Operational Excellence* akan menekankan stabilitas sistem, efisiensi proses, dan kontinuitas layanan, sehingga kontrol yang mendukung *monitoring*, *backup*, dan manajemen risiko menjadi prioritas. PT dengan orientasi *Customer Intimacy* akan memprioritaskan perlindungan data pribadi, pengaturan hak akses yang ketat, serta mekanisme audit untuk membangun kepercayaan *stakeholder*. Sedangkan PT dengan fokus *Product Leadership* menekankan keamanan inovasi dan penelitian, manajemen aset strategis, serta proteksi kekayaan intelektual.

2.2.2 Tahap 2: Integrasi Kontrol dan Konteks Operasional

Pada tahap ini, setiap domain kontrol ISO/IEC 27001 (*Annex* A:2022) dianalisis untuk menentukan relevansi terhadap orientasi nilai yang telah ditetapkan. Analisis ini memastikan setiap kontrol memiliki justifikasi konseptual yang logis dan mendukung tujuan keamanan informasi. Selain itu, konteks operasional PT juga ditentukan, meliputi unit akademik, penelitian dan pengabdian, administrasi, serta layanan TI, sehingga model yang dikembangkan bersifat adaptif terhadap karakteristik institusi. Hasil tahap ini berupa pemetaan kontrol yang spesifik terhadap fokus strategis organisasi.

2.2.3 Tahap 3: Penyusunan Tabel Integratif

Tahap terakhir pengembangan model menghasilkan tabel integratif yang menghubungkan *Value Discipline*, fokus strategis organisasi, level kontrol dominan, domain kontrol ISO/IEC 27001(*Annex* A:2022), rincian dan contoh kontrol, serta tujuan keamanan utama. Tabel ini memudahkan pemahaman bagaimana orientasi nilai diterjemahkan menjadi kontrol spesifik dan bagaimana kontrol tersebut mendukung tujuan keamanan informasi. Dengan mengikuti ketiga tahap tersebut, pengembangan model berhasil membangun Model *Integrated Value Discipline ISMS* yang sistematis, logis, dan relevan secara strategis bagi PT. Model ini menyederhanakan kompleksitas ISMS sekaligus menyediakan panduan untuk prioritisasi kontrol keamanan informasi berdasarkan fokus strategis organisasi.

2.3 Verifikasi dan penilaian koherensi teoretis

Tahap verifikasi dan penilaian koherensi teoretis bertujuan memastikan bahwa model *Integrated Value Discipline ISMS* (IVD-ISMS *Framework*) yang dikembangkan konsisten secara logis, sesuai dengan prinsip ISO/IEC 27001, dan relevan terhadap fokus strategis PT. Pendekatan yang digunakan bersifat teoretis dan rasional logis, sehingga pengujian dilakukan melalui analisis konseptual dan argumentasi, tanpa melibatkan data empiris atau implementasi langsung. Tahap ini dibagi menjadi tiga sub-tahap utama sebagai berikut:

2.3.1 Tahap 1: Verifikasi Konsistensi Internal

Verifikasi konsistensi internal dilakukan untuk memastikan bahwa semua komponen model terhubung secara logis dan tidak terjadi kontradiksi antar-elemen. Pada tahap ini, orientasi nilai organisasi, domain kontrol ISO/IEC 27001, dan tujuan keamanan informasi dianalisis untuk

memastikan setiap hubungan dapat dipertanggung jawabkan secara konseptual. Misalnya, setiap kontrol yang diprioritaskan untuk *Operational Excellence* benar-benar mendukung stabilitas dan efisiensi layanan, sedangkan kontrol untuk *Product Leadership* mendukung keamanan inovasi dan perlindungan kekayaan intelektual. Analisis dilakukan secara sistematis untuk memastikan bahwa setiap elemen model memiliki dasar teoritis yang jelas dan tidak ada redundansi atau pertentangan dalam pemetaan.

2.3.2 Tahap 2: Penilaian Koherensi Teoretis terhadap Kesesuaian dengan ISO/IEC 27001

Penilaian koherensi teoretis terhadap kesesuaian dilakukan untuk memastikan bahwa semua kontrol yang termasuk dalam model tetap selaras dengan standar ISO/IEC 27001, khususnya Annex A:2022 [16]. Pada tahap ini, setiap domain kontrol diperiksa apakah implementasinya dapat secara teoritis mendukung tujuan keamanan informasi yang diidentifikasi sesuai orientasi nilai organisasi. Misalnya, kontrol *Access Control* dan *Backup & Recovery* tetap diterapkan untuk menjamin kontinuitas dan ketersediaan data pada PT yang menekankan *Operational Excellence*, sedangkan kontrol *Intellectual Property Rights* dan *Secure Development Lifecycle* sesuai dengan kebutuhan PT yang menekankan *Product Leadership*. Tahap ini memastikan bahwa model tidak hanya logis, tetapi juga sesuai dengan standar internasional yang berlaku.

2. 3.3 Tahap 3: Penilaian Koherensi Teoretis Rasional dan Keterkaitan Strategis

Tahap terakhir adalah penilaian koherensi teoretis rasional yang menekankan keterkaitan antara model dengan strategi organisasi. Penilaian ini menilai apakah prioritas kontrol, pemetaan domain ISO/IEC 27001, dan tujuan keamanan informasi mencerminkan karakteristik strategis PT secara konsisten. Misalnya, model harus menunjukkan bahwa prioritas kontrol yang dipilih benar-benar mendukung orientasi nilai organisasi dan selaras dengan strategi jangka panjang institusi, baik dalam hal efisiensi, kepercayaan *stakeholder*, maupun inovasi. Penilaian ini dilakukan melalui argumentasi logis dan analisis konseptual, memastikan model dapat dipertahankan sebagai instrumen teoritis yang kuat untuk penelitian dan praktik.

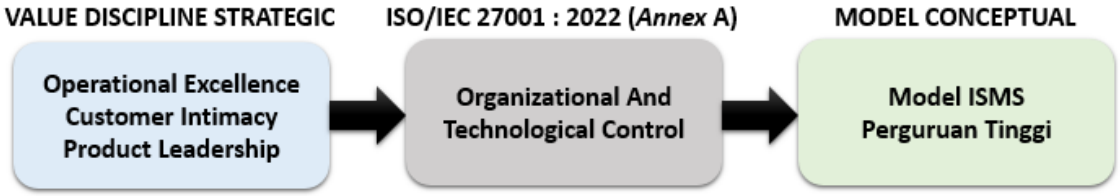
3. HASIL DAN PEMBAHASAN

3.1 Hasil dan Pembahasan Tahap Inisiasi

Hasil penelitian pada tahap inisiasi menunjukkan bahwa pengembangan model *Integrated Value Discipline ISMS* (IVD-ISMS *Framework*) membutuhkan dasar konseptual yang kuat, yang diperoleh melalui kajian literatur terkait ISO/IEC 27001 (*Annex* A:2022) dan *Value Discipline Strategic* [16]. Analisis literatur ISO/IEC 27001 menekankan pentingnya domain-domain kontrol yang komprehensif, termasuk kebijakan keamanan informasi, manajemen risiko, kontrol akses, perlindungan aset strategis, serta kontinuitas layanan. Kajian ini memberikan fondasi teoretis yang jelas mengenai prinsip, ruang lingkup, dan tujuan ISMS, sehingga dapat menjadi pedoman untuk mengembangkan model konseptual yang relevan dengan kebutuhan PT.

Studi literatur mengenai *Value Discipline Strategic* menunjukkan bahwa fokus strategis organisasi, seperti *Operational Excellence*, *Customer Intimacy*, dan *Product Leadership*, menentukan prioritas pengelolaan keamanan informasi. PT yang menekankan *Operational Excellence* akan memfokuskan kontrol pada efisiensi proses, stabilitas sistem, dan kontinuitas layanan, sementara orientasi *Customer Intimacy* menekankan perlindungan data pribadi, kontrol akses berbasis layanan, serta mekanisme audit untuk menjaga kepercayaan *stakeholder*. Di sisi lain, orientasi *Product Leadership* menekankan keamanan inovasi, perlindungan kekayaan intelektual, dan manajemen aset strategis dalam setiap tahap proyek penelitian dan pengembangan.

Berdasarkan kajian literatur tersebut, tahap inisiasi menghasilkan kerangka konseptual awal, yang selanjutnya disebut *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*), yang dapat dilihat pada Gambar 1. Kerangka ini menggambarkan hubungan logis antara orientasi nilai organisasi, domain kontrol ISO/IEC 27001, dan tujuan keamanan informasi. Diagram ini menekankan bahwa orientasi nilai organisasi berfungsi sebagai titik awal yang memandu pemilihan domain kontrol yang relevan, sehingga setiap kontrol yang diterapkan akan secara rasional mendukung tujuan keamanan informasi yang diharapkan, yaitu menjaga kerahasiaan, integritas, dan ketersediaan informasi.



Gambar 1 *Integrated Value Discipline ISMS Model* (IVD-ISMS *Framework*)

Kerangka konseptual ini menegaskan bahwa setiap orientasi nilai organisasi menentukan prioritas domain kontrol yang berbeda, namun tetap saling melengkapi untuk mencapai tujuan keamanan informasi secara menyeluruh. Diagram pada Gambar 1 juga memperlihatkan alur logis yang konsisten antara teori *Value Discipline Strategic* dan prinsip ISO/IEC 27001, sehingga model yang dikembangkan memiliki dasar konseptual yang kuat, rasional, dan dapat dipertahankan untuk pengembangan lebih lanjut pada tahap pengembangan model.

Dengan demikian, tahap inisiasi berhasil memenuhi tujuan awal penelitian, yaitu menyediakan fondasi teoritis dan kerangka konseptual yang logis, konsisten, dan relevan bagi pengembangan *Integrated Value Discipline ISMS Model* yang dapat digunakan sebagai pedoman strategis untuk PT.

3.2 Hasil dan Pembahasan Tahap Pengembangan Model

Tahap pengembangan model bertujuan untuk menerjemahkan kerangka konseptual awal menjadi *Integrated Value Discipline ISMS Model* yang lebih rinci, dengan mempertimbangkan fokus strategis PT, domain kontrol ISO/IEC 27001, dan tujuan keamanan informasi. Pengembangan dilakukan melalui tiga sub-tahap, yang dijabarkan sebagai berikut:

3.2.1 Tahap 1: Pemetaan Domain Kontrol ISO/IEC 27001 ke Fokus Strategis Organisasi

Pada tahap ini, tujuan utamanya adalah menyesuaikan domain kontrol ISO/IEC 27001 (*Annex* A:2022) dengan orientasi nilai organisasi (*Value Discipline Strategic*), yaitu *Operational Excellence*, *Customer Intimacy*, dan *Product Leadership*. Analisis literatur menunjukkan bahwa setiap orientasi nilai memiliki karakteristik strategis yang berbeda, sehingga prioritas kontrol yang diterapkan juga berbeda. *Operational Excellence* menekankan efisiensi, stabilitas, dan kontinuitas layanan, sehingga kontrol yang dominan bersifat manajerial dan operasional. *Customer Intimacy* menekankan keamanan data dan kepercayaan pelanggan, sehingga kontrol yang dominan bersifat perlindungan data dan monitoring. Sedangkan *Product Leadership* menekankan inovasi dan perlindungan aset strategis, sehingga kontrol yang dominan bersifat strategis dan mendukung pengembangan produk serta penelitian.

Tabel 1 Pemetaan Domain Kontrol ISO/IEC 27001 (*Annex* A:2022) ke Fokus Strategis Organisasi

Value Discipline	**Fokus Strategis Organisasi**	**Contoh Kontrol ISO/IEC 27001:2022 dan Penjelasan**	**Relevansi terhadap Strategi Keamanan Informasi**
Operational Excellence	Efisiensi, stabilitas, dan	A.5.1 *Policies for information security*: Menetapkan kebijakan	Menjamin efisiensi dan stabilitas operasional dengan kontrol yang

Value Discipline	Fokus Strategis Organisasi	Contoh Kontrol ISO/IEC 27001:2022 dan Penjelasan	Relevansi terhadap Strategi Keamanan Informasi
	kontinuitas layanan	keamanan yang memastikan konsistensi dan efisiensi operasional. A.5.7 *Threat intelligence*: Mengidentifikasi ancaman untuk menjaga kelancaran proses operasional. A.5.15 *Access control*: Mengatur hak akses agar efisiensi dan keamanan berjalan seimbang. A.5.30 ICT *readiness for business continuity*: Menjamin kesiapan TI dalam menjaga kesinambungan layanan. A.8.16 *Monitoring activities*: Memantau aktivitas sistem untuk deteksi dini insiden.	mendukung keberlanjutan proses bisnis dan deteksi risiko lebih awal.
Customer Intimacy	Kepercayaan, perlindungan data pribadi, dan loyalitas pengguna	A.5.12 *Classification of information*: Mengklasifikasikan informasi pelanggan berdasarkan sensitivitas. A.5.23 *Information security for use of cloud services*: Memastikan keamanan data pelanggan pada layanan *online*. A.6.3 *Information security awareness, education and training*: Meningkatkan kesadaran staf terhadap perlindungan data pelanggan. A.8.11 *Data masking*: Menjaga kerahasiaan data pelanggan melalui teknik penyamaran data. A.8.12 *Data leakage prevention*: Mencegah kebocoran informasi penting pelanggan. A.8.15 *Logging*: Merekam aktivitas sistem untuk mendeteksi pelanggaran keamanan.	Memperkuat kepercayaan pengguna dengan memastikan integritas dan kerahasiaan data pelanggan secara menyeluruh di seluruh siklus layanan.
Product Leadership	Inovasi, riset, dan perlindungan kekayaan intelektual	A.5.9 *Inventory of information and other associated assets*: Mengidentifikasi aset informasi penting bagi riset dan inovasi. A.5.13 *Information transfer*: Mengatur keamanan pertukaran data riset dan inovasi. A.5.19 *Intellectual property rights*: Melindungi hak kekayaan intelektual dan hasil riset organisasi. A.8.18 *Use of privileged utility programs*: Perlindungan perangkat penelitian dari risiko kebocoran data. A.8.25 *Secure development lifecycle*: Menjamin keamanan pada seluruh tahapan pengembangan sistem riset dan produk.	Menjaga keamanan dan integritas inovasi, melindungi hasil penelitian, dan memastikan bahwa keamanan mendukung penciptaan nilai dan daya saing akademik.

Value Discipline	Fokus Strategis Organisasi	Contoh Kontrol ISO/IEC 27001:2022 dan Penjelasan	Relevansi terhadap Strategi Keamanan Informasi
		A.8.28 *Secure coding*: Menjamin keamanan perangkat lunak inovatif yang dikembangkan internal. A.8.32 *Change management*: Menjamin stabilitas dan keamanan saat terjadi perubahan sistem riset atau inovasi.	

Hasil pemetaan pada Tabel 1 menunjukkan bahwa prioritas kontrol berbeda sesuai dengan orientasi nilai organisasi. Hal ini menegaskan bahwa ISMS yang efektif tidak bisa seragam, tetapi harus disesuaikan dengan strategi institusi. *Operational Excellence* lebih menekankan kontinuitas dan efisiensi proses, *Customer Intimacy* lebih menekankan perlindungan data dan transparansi, sementara *Product Leadership* lebih menekankan keamanan inovasi dan aset strategis. Pemetaan ini menyediakan dasar konseptual untuk penyesuaian kontrol dengan konteks operasional PT pada tahap berikutnya.

3.2.2 Tahap 2: Penyesuaian Kontrol dengan Konteks Operasional PT

Tahap ini memfokuskan pada adaptasi kontrol ISO/IEC 27001 (*Annex* A:2022) [16] yang sudah dipetakan agar sesuai dengan konteks operasional PT. PT memiliki karakteristik khusus, seperti kegiatan akademik, penelitian, layanan administrasi, dan interaksi dengan pihak ketiga. Oleh karena itu, setiap kontrol perlu dikaitkan dengan fungsi nyata, misalnya hak akses mahasiswa dan dosen pada sistem akademik (*Operational Excellence*), pengelolaan data pribadi mahasiswa dan staf (*Customer Intimacy*), serta keamanan proses penelitian dan inovasi (*Product Leadership*). Penyesuaian ini memastikan bahwa kontrol yang diterapkan relevan, operasional, dan dapat mendukung tujuan strategis masing-masing *value discipline*.

Tabel 2 Penyesuaian Kontrol ISO/IEC 27001 (*Annex* A:2022) dengan Konteks PT

Value Discipline	Fokus Strategis Organisasi	Level Kontrol Dominan	Penyesuaian Kontrol ISO/IEC 27001 (Annex A:2022) dengan Konteks PT
Operational Excellence	Efisiensi, stabilitas, dan kontinuitas layanan	Manajerial (*Organisational Controls*)	A.5.1 Kebijakan keamanan mendukung efisiensi dan stabilitas operasional kampus. A.5.7 Pemantauan ancaman terhadap sistem akademik dan layanan administrasi. A.5.30 Kesiapan TI untuk menjaga keberlanjutan layanan kampus. A.5.15 Pengaturan hak akses sesuai peran dosen, mahasiswa, dan staf.
		Operasional (*Technological Controls*)	A.8.16 Pemantauan sistem akademik untuk mendeteksi gangguan.
Customer Intimacy	Keamanan data mahasiswa, staf, dan kepercayaan pengguna	Manajerial (*Organisational Controls*)	A.5.12 Klasifikasi data mahasiswa dan staf. A.5.23 Keamanan penggunaan layanan cloud akademik. A.6.3 Edukasi keamanan informasi bagi sivitas akademika.
		Operasional (Technological Controls)	A.8.11 Perlindungan data pribadi mahasiswa melalui masking data. A.8.12 Pencegahan kebocoran data akademik dan personal. A.8.15 Pencatatan aktivitas sistem akademik untuk audit.

Value Discipline	Fokus Strategis Organisasi	Level Kontrol Dominan	Penyesuaian Kontrol ISO/IEC 27001 (Annex A:2022) dengan Konteks PT
Product Leadership	Inovasi, riset, dan perlindungan kekayaan intelektual	Strategis (*Organisational Controls*)	A.5.9 Pengelolaan aset informasi penelitian. A.5.13 Keamanan pertukaran data riset dan kolaborasi akademik. A.5.19 Perlindungan hak kekayaan intelektual hasil riset.
		Operasional (*Technological Controls*)	A.8.18 Perlindungan perangkat penelitian dari risiko kebocoran data. A.8.25 Pe§ngembangan sistem riset yang aman. A.8.28 Penerapan kode aman pada aplikasi penelitian. A.8.32 Menjamin stabilitas dan keamanan saat terjadi perubahan sistem riset atau inovasi.

Penyesuaian seperti pada Tabel 2 ini memastikan bahwa model ISMS bukan sekadar teori, tetapi relevan dengan konteks operasional PT. Dengan mengaitkan kontrol ISO/IEC 27001 (*Annex* A:2022) [16] dengan aktivitas nyata akademik dan penelitian, model menjadi lebih aplikatif, meski tetap bersifat konseptual. Tahap ini juga menunjukkan fleksibilitas model dalam menyesuaikan prioritas kontrol sesuai kebutuhan spesifik institusi, menjaga konsistensi antara tujuan strategis, domain kontrol, dan operasi sehari-hari.

3.2.3 Tahap 3: Integrasi Elemen menjadi Model Konseptual Sistematis

Tahap ini bertujuan untuk menyatukan seluruh elemen yang diperoleh dari Tahap 1 (pemetaan domain kontrol ISO/IEC 27001 (Annex A:2022) ke fokus strategis organisasi) dan Tahap 2 (penyesuaian kontrol dengan konteks operasional PT) menjadi sebuah model konseptual yang sistematis. Model ini diberi nama *Integrated Value Discipline ISMS Framework*, yang dapat menjadi acuan konseptual bagi penelitian terapan dan implementasi ISMS di PT.

Model ini menekankan integrasi antara orientasi nilai organisasi (*Operational Excellence*, *Customer Intimacy*, *Product Leadership*), domain kontrol ISO/IEC 27001 (Annex A:2022) (manajerial, teknologis, strategis), serta konteks operasional PT. Dengan demikian, setiap kontrol memiliki justifikasi strategis dan operasional, sehingga ISMS menjadi adaptif dan relevan.

Tabel 3 *Integrated Value Discipline ISMS Framework*

Value Discipline	Fokus Strategis Organisasi	Level Kontrol Dominan	Penyesuaian Kontrol ISO/IEC 27001:2022 (Annex A: 2022) dengan Konteks PT	Tujuan Keamanan Utama
Operational Excellence	Efisiensi, stabilitas, dan kontinuitas layanan	Manajerial & Operasional	Pengendalian operasional akademik, manajemen risiko, pengaturan akses, serta backup data sesuai kontrol A.5 dan A.8.	Menjamin efisiensi proses dan kontinuitas layanan.
Customer Intimacy	Keamanan data pengguna dan kepercayaan sivitas akademika	Manajerial & Operasional	Perlindungan data pribadi, pencatatan aktivitas sistem, otentikasi pengguna, dan pengelolaan retensi data sesuai kontrol A.5, A.6, dan A.8.	Menjaga kerahasiaan, integritas, dan kepercayaan data.
Product Leadership	Inovasi, riset, dan perlindungan kekayaan intelektual	Strategis & Operasional	Pengembangan sistem riset aman, pengujian keamanan aplikasi, dan perlindungan kekayaan intelektual sesuai kontrol A.5 dan A.8.	Melindungi inovasi dan mendukung keberlanjutan riset.

Hasil integrasi pada Tabel 3 ini menunjukkan bahwa model *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*) berhasil menyatukan berbagai elemen yang sebelumnya terpisah menjadi suatu kerangka konseptual yang konsisten dan logis. Model ini memungkinkan pemahaman yang jelas mengenai hubungan antara fokus strategis organisasi, domain kontrol ISO/IEC 27001, dan konteks operasional PT.

Pendekatan ini memberikan beberapa keunggulan: pertama, model memberikan panduan konseptual yang adaptif, sehingga setiap PT dapat menyesuaikan implementasi kontrol sesuai strategi dan konteksnya. Kedua, integrasi antara kontrol manajerial, teknologis, dan strategis memastikan ISMS bersifat holistik dan menyeluruh. Ketiga, model ini dapat diuji secara teoritis melalui penilain rasional-logis, tanpa memerlukan data empiris pada tahap awal. Secara keseluruhan, tahap ini menutup proses pengembangan model dengan menghasilkan kerangka konseptual yang siap untuk tahap verifikasi dan penilaian koherensi teoretis, sebagai landasan bagi implementasi dan penelitian lanjutan di bidang ISMS pada PT.

3.3 Tahap Verifikasi dan Penilaian Koherensi Teoretis

Tahap verifikasi dan penilaian koherensi teoretis bertujuan memastikan bahwa model *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*) konsisten, valid secara teoritis, dan rasional-logis. Sesuai metode, tahap ini dibagi menjadi tiga bagian, yaitu: **v**erifikasi konsistensi internal**,** Penilaian koherensi teoritis dan rasional-logis.

3.3.1 Verifikasi Konsistensi Internal

Verifikasi konsistensi internal memeriksa keterpaduan antar elemen model, yaitu antara *value discipline strategic*, domain kontrol ISO/IEC 27001 (*Annex* A: 2022), dan konteks operasional PT. Fokusnya adalah memastikan tidak ada konflik antara kontrol yang diterapkan dengan tujuan strategis masing-masing *value discipline strategic*. Analisis dilakukan dengan menelusuri tiap kontrol ISO/IEC 27001 (*Annex* A: 2022) yang dipetakan pada *value discipline strategic* dan mengevaluasi apakah setiap kontrol mendukung tujuan strategis yang sesuai.

Tabel 4 Hasil Verifikasi Konsistensi Internal

Value Discipline	Kontrol ISO/IEC 27001	Kesesuaian dengan Fokus Strategis	Kesimpulan
Operational Excellence	*Backup & Recovery, Access Control, Monitoring*	Mendukung efisiensi proses dan kontinuitas layanan	Konsisten
Customer Intimacy	*Data Classification, Logging, User Authentication*	Mendukung kerahasiaan dan integritas data pelanggan	Konsisten
Product Leadership	*Secure Development Lifecycle, IP Protection, Testing & Validation*	Mendukung keamanan inovasi dan pengembangan produk	Konsisten

Hasil pada Tabel 4 menunjukkan seluruh *value discipline strategic* memiliki kontrol yang selaras dengan tujuan strategis dan domain kontrol ISO/IEC 27001 (*Annex* A:2022)). Tidak ditemukan konflik antar kontrol, sehingga model konsisten secara internal.

3.3.2 Traceability Antar Value Discipline – Kontrol ISO 27001 – Tujuan Keamanan

Matriks traceability berikut digunakan untuk memastikan bahwa setiap kontrol ISO/IEC 27001 (*Annex* A:2022) benar-benar mendukung *value discipline strategic* serta tujuan keamanan informasi (*Confidentiality*, *Integrity*, *Availability*).

Tabel 5 *Traceability*

Value Discipline	Kontrol ISO/IEC 27001 Terkait	Tujuan Keamanan (CIA)	Kesesuaian Strategis	Skor Koherensi

Operational Excellence	*Backup & Recovery (A.8), Access Control (A.9), Monitoring (A.12)*	*Availability, Confidentiality, Integrity*	Mendukung efisiensi proses dan kontinuitas layanan	4.7
Customer Intimacy	*Data Classification (A.5), Logging & Monitoring (A.12), User Authentication (A.9)*	*Confidentiality, Integrity*	Melindungi data pelanggan dan menjaga interaksi	4.7
Product Leadership	*Secure SDLC (A.14), IP Protection (A.18), Testing & Validation (A.14)*	*Integrity, Confidentiality*	Mendukung keamanan inovasi dan kualitas produk	4.7

Hasil Tabel 5 ini menunjukkan bahwa setiap kontrol ISO/IEC 27001 memiliki keterkaitan yang jelas dengan *value discipline* dan tujuan keamanan informasi. Pada *Operational Excellence*, kontrol seperti *Backup & Recovery*, *Access Control*, dan *Monitoring* mendukung efisiensi proses serta kontinuitas layanan. Pada *Customer Intimacy*, kontrol *Data Classification*, *Logging*, dan *User Authentication* selaras dengan kebutuhan menjaga kerahasiaan dan integritas data pelanggan. Sementara itu, pada *Product Leadership*, kontrol *Secure Development Lifecycle*, *IP Protection*, dan *Testing & Validation* relevan dalam memastikan keamanan dan kualitas inovasi. Secara keseluruhan, matriks *traceability* ini memperlihatkan bahwa semua kontrol memiliki koherensi yang kuat dengan fokus strategis masing-masing *value discipline*, sehingga integrasi antara strategi dan kontrol ISO/IEC 27001 dalam model ini dinilai selaras, terukur, dan dapat ditelusuri dengan baik.

3.3.2 Penilaian Koherensi Teoritis

Penilaian koherens teoritis dilakukan dengan meninjau kesesuaian model dengan teori-teori yang relevan, seperti teori *Value Discipline Strategic*, prinsip-prinsip manajemen risiko dan keamanan informasi, serta praktik terbaik ISMS. Model dianggap valid jika koheren dengan literatur dan dapat menjelaskan hubungan antara strategi organisasi dan pengelolaan kontrol informasi.

Tabel 6 Hasil Validasi Teoritis

Aspek Teoritis	Analisis	Kesimpulan Validitas
Keselarasan dengan *Value Discipline Strategic*	Setiap *value discipline strategic* memiliki kontrol yang sesuai dengan orientasi nilai	Valid
Kepatuhan prinsip ISMS	Kontrol menutupi aspek manajerial, teknologis, dan strategis	Valid
Relevansi dengan praktik terbaik	Model mengintegrasikan kontrol yang umum diterapkan di PT	Valid

Pada Tabel 6 ini menunjukkan bahwa model ini terbukti selaras dengan teori *value discipline strategic* dan prinsip ISMS, sehingga valid secara teoritis. Ini menunjukkan model dapat digunakan sebagai referensi konseptual bagi penelitian dan implementasi ISMS.

3.3.3 Penilaian Koherensi Rasional-Logis

Tabel 7 merupakan hasil penilaian koherensi rasional-logis yaitu menilai apakah model memiliki struktur logis, koherensi argumen, dan kemampuan diterapkan secara konseptual. Analisis ini menekankan argumentasi logis dari setiap penggabungan *value discipline strategic*, kontrol ISO/IEC 27001 (*Annex* A:2022), dan konteks PT.

Tabel 7 Hasil Evaluasi Rasional-Logis

Elemen yang Dievaluasi	Analisis Rasional-Logis	Kesimpulan
Integrated Value Discipline & Control	Logis: setiap kontrol mendukung tujuan strategis organisasi	Rasional dan logis
Penyesuaian dengan Konteks PT	Logis: kontrol disesuaikan dengan aktivitas akademik, penelitian, administrasi	Rasional dan logis
Konsistensi Struktur Model	Logis: model mudah dipahami dan dapat dijadikan panduan konseptual	Rasional dan logis

Hasil pada Tabel 7 menunjukkan model *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*) memiliki struktur logis dan koheren, sehingga rasional secara konseptual. Model ini memungkinkan adaptasi dan penerapan di berbagai PT tanpa memerlukan data empiris awal. Evaluasi ini memperkuat bahwa model siap digunakan sebagai kerangka konseptual untuk pengembangan ISMS.

4. KESIMPULAN

Penelitian ini menghasilkan *Integrated Value Discipline ISMS Framework* (IVD-ISMS *Framework*) yang menghubungkan secara sistematis orientasi strategi organisasi (*Operational Excellence, Customer Intimacy, dan Product Leadership*) dengan pemilihan serta penyesuaian kontrol ISO/IEC 27001 (Annex A2022 dalam konteks Perguruan Tinggi. Melalui pemetaan fokus strategis ke domain kontrol dan penyesuaian dengan operasi PT, penelitian ini menegaskan bahwa kontrol keamanan informasi tidak hanya bersifat prosedural, tetapi perlu disejajarkan dengan prioritas strategis organisasi. Kerangka yang dihasilkan memberikan kontribusi teoretis dengan mengisi celah kajian sebelumnya yang umumnya hanya menekankan aspek teknis ISO/IEC 27001 tanpa mengaitkan strategi organisasi. Secara praktis, model ini dapat menjadi panduan konseptual bagi PT dalam merancang ISMS yang lebih adaptif, relevan, dan berorientasi nilai.

5. SARAN

Penelitian ini bersifat konseptual sehingga tidak mencakup analisis *trade-off* antar *value discipline strategic* maupun pengujian empiris. Oleh karena itu, kedua aspek tersebut direkomendasikan sebagai agenda penelitian lanjutan untuk memvalidasi dan menguji efektivitas kerangka dalam implementasi nyata.

UCAPAN TERIMA KASIH

Penulis berterima kasih kepada Tim Redaksi Jurnal Teknika Politeknik Negeri Sriwijaya atas kesempatan yang diberikan untuk mempublikasikan artikel ini.

DAFTAR PUSTAKA

[1] F. Anis Sekar Ningrum, Y. Riwanto, I. Yanuar Risca Pratiwi, and M. A. Fikri, "Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI," *Jurnal Informatika Polinema*, vol. 10, no. 3, pp. 437–444, 2024.

[2] R. Sinaga, "Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO Development of a Compliance Assessment Model for One of the Universities to ISO 27001 : 2022 Standards," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, pp. 381–394, 2023.

[3] S. juhardi Syahputra eko, Novianty lily, "Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasrkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan)," *Journal of Engineering Research*, vol. 10, no. 1, pp. 35–45, 2023.

[4] M. A. Fattah Ys, B. Parga Zen, and D. E. Wasitarini, "Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata

Kelola Teknologi Informasi," *Cyber Security dan Forensik Digital*, vol. 6, no. 2, pp. 76–82, 2024, doi: 10.14421/csecurity.2023.6.2.4190.

[5] D. Rahmat, "Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar Sni Isoiec 27001:2013," *Jurnal Informatika – COMPUTING*, vol. 6, no. 2, pp. 37–41, 2019.

[6] A. P. Damanik, A. Zaki, S. Fiddarain, and A. B. Nasution, "Implementasi ISO 27001:2013 Dalam Pengamanan Sistem Informasi Pada Yayasan Pendidikan Islam ANNUR PRIMA," *Jurnal Sains dan Teknologi (JSIT)*, vol. 3, no. 1, pp. 68–73, 2023, doi: 10.47233/jsit.v3i1.488.

[7] F. Nasher, "Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (Lpse) Di Dinas Komunikasi Dan Informatika Kabupaten Cianjur Dengan Menggunakan Sni Iso/Iec 27001:2013," *Media Jurnal Informatika*, vol. 10, no. 1, pp. 1–16, 2020, doi: 10.35194/mji.v10i1.465.

[8] S. Suroso and W. Wasilah, "Analisis Keamanan Informasi SIMRS dengan Metode Indeks KAMI dan OCTAVE Allegro," *Teknika*, vol. 19, no. x, pp. 795–808, 2025.

[9] M. Treacy and F. Wiersema, "Customer Intimacy and Other Value Disciplines Harvard Business Review," *Harvard Business Review*, p. 94, 1993.

[10] A. Stancu *et al.*, "Value creation attributes-clustering strategic options for Romanian SMEs," *Sustainability (Switzerland)*, vol. 12, no. 17, pp. 1–19, 2020, doi: 10.3390/su12177007.

[11] A. S. Y. R. M. Y. Abdul Rasyid; Steven; Malinda Sari Sembiring; Nur Syamsiyah; Acai Sudirman; Sri Sarjana; Karen Alfa Pontoan; Ikhsan;Hariandy Hasbi; Abdul Karman, *Manajemen Strategik*, vol. 2011, no. December 2022. 2022.

[12] B. Metin, S. B. Sevim, and M. Wynn, "Cybersecurity Strategy Development : Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards," *MDPI Journal*, pp. 1–26, 2025.

[13] H. Susanto, F. Bin Muhaya, M. N. Almunawar, and Y. C. Tuan, "Refinement of Strategy and Technology Domains STOPE View on ISO 27001," *Cornell University Library*, pp. 1–7, 2012.

[14] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *Jurnal SAINTEKOM*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[15] F. Pujiani and R. Bisma, "Strategi Optimalisasi Manajemen Konfigurasi untuk Keamanan Informasi Berdasarkan ISO/IEC 27001:2022," *Journal of Emerging Information Systems and Business Intelligence*, vol. 5, no. 3, pp. 223–228, 2024.

[16] ISO/IEC, *International Standard ISO/IEC 27002 Information security, cybersecurity and privacy protection-Information security controls*, vol. 2022. 2022.