NARATIF : Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika
Vol. 07 No. 02 Desember 2025
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

TRANSFORMASI MANAJEMEN KEAMANAN INFORMASI MELALUI IMPLEMENTASI *OPEN INFORMATION SECURITY MANAGEMENT MATURITY MODEL* (O-ISM3)

Muchamad Rusdan[1], Sri Kuswayati[2], Brian Damastu Ridho Hutama[3]
Departemen Teknik Informatika[1,2,3]
Universitas Teknologi Bandung[1,2,3]
rusdan@utb-univ.ac.id[1], srikuswayati@utb-univ.ac.id[2], brian.damastu@gmail.com[3]

Abstrak

Lanskap ancaman digital yang terus berubah dengan cepat dan meningkatnya kompleksitas teknologi informasi telah mendorong kebutuhan akan evolusi fundamental dalam manajemen keamanan informasi. Organisasi tidak lagi dapat mengandalkan pendekatan reaktif yang hanya berfokus pada kepatuhan semata, melainkan harus beralih ke fungsi keamanan yang proaktif, terukur, dan sepenuhnya terintegrasi dengan tujuan bisnis. Namun, banyak organisasi saat ini masih terjebak dalam kesenjangan yang signifikan antara mengimplementasikan kontrol keamanan dengan kemampuan untuk mendemonstrasikan nilai bisnis dan mencapai perbaikan berkelanjutan. Penelitian ini bertujuan untuk merumuskan strategi implementasi yang komprehensif untuk *Open Information Security Management Maturity Model* (O-ISM3) guna menjembatani kesenjangan antara teori dan praktik dalam manajemen keamanan informasi. Melalui analisis terhadap publikasi resmi, literatur akademis, dan studi kasus, penelitian ini menyimpulkan bahwa O-ISM3 merupakan kerangka kerja transformatif yang didukung oleh tiga pilar berorientasi bisnis *(business-focused)*, berbasis proses *(process-oriented*), dan digerakkan oleh pengukuran *(measurement-driven)*. Hasil analisis menunjukkan bahwa implementasi O-ISM3 yang efektif memerlukan strategi siklik yang terdiri dari lima fase Fondasi (penilaian diri dan penyelarasan bisnis), Perancangan (desain proses dan metrik), Eksekusi (implementasi bertahap), Evaluasi (pengukuran kinerja), dan Optimisasi (budaya perbaikan berkelanjutan). Temuan ini menegaskan bahwa O-ISM3 bukan sekadar kerangka kepatuhan, melainkan sebuah alat strategis yang memungkinkan organisasi untuk mengubah fungsi keamanan informasi dari pusat biaya menjadi sebuah *strategic enabler* yang memberikan nilai terukur dan terintegrasi penuh dengan tujuan organisasi. Penelitian ini berkontribusi pada penyediaan peta jalan yang dapat ditindaklanjuti bagi organisasi untuk mencapai tingkat kematangan keamanan informasi yang lebih tinggi dan membangun ketahanan dalam menghadapi lanskap ancaman digital yang terus berkembang.
Kata kunci : O-ISM3, manajemen keamanan informasi, model kematangan, strategi implementasi, tata kelola keamanan.

Abstract

The rapidly evolving digital threat landscape and the increasing complexity of information technology have necessitated a fundamental evolution in Information Security Management. Organizations can no longer rely on reactive approaches focused solely on compliance; instead, they must transition to a security function that is proactive, measurable, and fully integrated with business objectives. However, many organizations currently face a significant gap between implementing security controls and their ability to demonstrate tangible business value and achieve continuous improvement. This research aims to formulate a comprehensive implementation strategy for the Open Information Security Management Maturity Model (O-ISM3) to bridge the gap between theory and practice in Information Security Management. Through an in-depth analysis of official publications, academic literature, and industry case studies, this research concludes that O-ISM3 is a transformative framework supported by three pillars business-focused, process-oriented, and measurement-driven. The analysis reveals that an effective O-ISM3 implementation requires a cyclical strategy consisting of five phases Foundation (self-assessment and business alignment), Design (process and metric design), Execution (phased implementation), Evaluation (performance measurement), and Optimization (a culture of continuous improvement). These findings affirm that O-ISM3 is not merely a compliance framework, but a strategic tool that enables organizations to transform their information security function from a cost center into a strategic enabler that delivers measurable value and is fully integrated with organizational objectives. This research contributes by providing an actionable roadmap for organizations to achieve a higher level of information security maturity and build resilience against the continually evolving digital threat landscape.
Keywords : O-ISM3, information security management, maturity model, implementation strategy, security governance.

I. PENDAHULUAN

Pada era digital yang kian terinterkoneksi, informasi telah menjelma menjadi aset strategis penting bagi organisasi. Kondisi tersebut menjadikan keamanan informasi bukan lagi sekadar pilihan, melainkan sebuah imperatif. Namun, realitas di lapangan justru menunjukkan pertentangan, banyak organisasi masih menghadapi tantangan berat dalam mengelola keamanan informasi secara efektif. Ironisnya, implementasi berbagai kontrol keamanan dan kepatuhan *(compliance)* terhadap standar ternyata tidak serta-merta mencegah munculnya insiden keamanan baru. Fenomena tersebut mengindikasikan adanya kelemahan mendasar dalam efektivitas penerapan Sistem Manajemen Keamanan Informasi (SMKI) [1].

Akar masalah tersebut sering kali terletak pada pendekatan keamanan yang bersifat reaktif, terfragmentasi, dan terpisah *(decoupled)* dari tujuan bisnis inti. Dalam beberapa perspektif fungsi keamanan dipandang semata sebagai *cost center*, bukan sebagai *value driver* yang strategis. Dari sinilah teridentifikasi kurangnya kerangka panduan yang operasional untuk mengukur kinerja keamanan, menyelaraskan program keamanan dengan strategi bisnis, dan menjamin mekanisme perbaikan berkelanjutan *(continuous improvement)*. Standar semacam ISO/IEC 27001 memang menyediakan kerangka kontrol yang komprehensif, namun sering kali berhenti pada level *"what"* (apa yang harus dilakukan) tanpa

memberikan metodologi rinci tentang *"how"* (bagaimana mengelolanya) secara terukur dan selaras dengan dinamika misi organisasi [2]. Data dari Mend.io mengungkapkan bahwa 71% perusahaan mengakui program keamanan aplikasi *(AppSec)* dalam kondisi terus-menerus bereaksi terhadap daftar kerentanan. Akibatnya, hanya 52% perusahaan dan 44% praktisi *AppSec* mampu melakukan remediasi efektif terhadap kerentanan kritis, menunjukkan kesenjangan besar antara deteksi dan penyelesaian masalah [3]. Untuk memenuhi kepatuhan regulasi fokus pada dokumentasi/pemindaian daripada integrasi keamanan yang efektif ke dalam siklus pengembangan. Upaya pergeseran ke pengujian *"shift-left"* pun bisa menciptakan bifurkasi tanggung jawab antara tim pengembang dan tim keamanan yang jika tidak dikelola baik justru memperkuat siklus reaktif.

Bersama sifat reaktif, fragmentasi infrastruktur dan proses keamanan membentuk masalah ganda yang terus menggerogoti postur keamanan organisasi. Fragmentasi muncul dari penggunaan berbagai solusi *ad-hoc*, menciptakan ketidakselarasan alat dan proses [3]. Akibatnya, tim keamanan kesulitan melihat gambaran utuh postur keamanan, menghambat deteksi, respons, dan pemulihan yang efektif. Data dari [3] menunjukkan bahwa 65% perusahaan, infrastruktur keamanan yang terfragmentasi menghambat efektivitas respons [3]. Selain tantangan operasional terdapat hambatan strategis bahwa keamanan siber beban finansial, bukan penggerak nilai bagi bisnis. Persepsi tersebut semakin berbahaya di era digital, di mana kepercayaan dan ketahanan siber adalah aset kritis. Perkiraan *Cybersecurity Ventures* menunjukkan dampak finansial sangat besar, kerugian global akibat kejahatan siber diproyeksikan mencapai $10,5 triliun per tahun pada 2025, belum termasuk dampak reputasi dan operasional [4]. Selain itu studi University of Maryland menunjukkan bahwa serangan siber terjadi setiap 39 detik dan 59% organisasi terpapar *ransomware* dalam setahun terakhir menunjukkan bahwa pendekatan minimalis terhadap keamanan adalah bencana [1]. Investasi proaktif dalam keamanan termasuk kepatuhan terhadap standar ternyata jauh lebih murah daripada biaya pemulihan pascaserangan yang sering kali tak tertanggungkan.

Untuk menjembatani kesenjangan yang ada, *Open Information Security Management Maturity Model* (O-ISM3) hadir sebagai sebuah kerangka kerja transformatif yang secara khusus dirancang untuk mereformasi paradigma manajemen keamanan informasi. Nilai kebaruan O-ISM3 bersumber dari tiga pilar filosofis yang berorientasi bisnis *(business-focused)*, berbasis proses *(process-oriented)*, dan digerakkan oleh pengukuran *(measurement-driven)*. Berbeda dengan model kepatuhan yang bersifat *checklist-based*, O-ISM3 memfasilitasi organisasi dalam membangun SMKI yang secara inheren selaras dengan misi bisnis dan kebutuhan kepatuhannya, sekaligus adaptif terhadap variasi ukuran, konteks, dan ketersediaan sumber daya [5]. Lebih dari sekadar mendefinisikan serangkaian proses keamanan yang komprehensif, O-ISM3 melengkapinya dengan metrik operasional untuk setiap proses. Memberdayakan organisasi untuk mengukur kinerja secara kuantitatif, mengalokasikan investasi secara lebih tepat sasaran, dan mendemonstrasikan *value proposition* keamanan informasi kepada pemangku kepentingan bisnis dalam bahasa yang obyektif dan dapat dipertanggungjawabkan. Penerapan model semacam O-ISM3 semakin kritis di tengah lanskap ancaman siber yang terus berevolusi dan tuntutan bisnis akan ketahanan *(resilience)* serta kepercayaan *(trust)* digital. Tanpa kerangka kerja yang matang *(mature)* dan terukur, organisasi menghadapi risiko nyata berupa kerugian finansial, reputasi, dan operasional yang semuanya dapat dipicu oleh satu insiden keamanan yang gagal dikelola dengan baik.

Bertolak dari latar belakang yang telah dipaparkan, penelitian ini bertujuan untuk merumuskan sebuah strategi penerapan O-ISM3 yang bersifat komprehensif dan kontekstual. Menghasilkan sebuah peta jalan *(roadmap)* strategis dan terstruktur yang dapat diadaptasi oleh organisasi yang ingin memanfaatkan O-ISM3 guna meningkatkan tingkat kematangan *(maturity)* keamanan informasi. Melalui analisis mendasar terhadap arsitektur O-ISM3 yang mencakup tiga lapisan manajemen, yaitu strategis, taktis, dan operasional, serta seperangkat proses keamanan, dan model tingkat kematangan. Penelitian ini juga dirancang untuk menghasilkan sebuah panduan implementasi yang bersifat *actionable* dan bertahap. Panduan tersebut akan mencakup siklus hidup implementasi, mulai dari fase penilaian diri *(self-assessment)*, penyelarasan *(alignment)* dengan tujuan bisnis, eksekusi implementasi secara bertahap, pengukuran kinerja berbasis metrik, dan internalisasi budaya perbaikan berkelanjutan *(continuous improvement culture)*. Dengan demikian, penelitian ini diharapkan dapat berkontribusi mengisi celah literatur mengenai implementasi O-ISM3 dan memberikan instrumen yang aplikatif bagi para praktisi industri untuk mentransformasi fungsi keamanan informasi dari beban teknis yang reaktif menjadi *strategic enabler* yang terukur, tangguh, dan terintegrasi penuh dengan tujuan organisasi.

II. TINJAUAN PUSTAKA

1. Evolusi dan Tantangan Manajemen Keamanan Informasi Modern

Manajemen Keamanan Informasi (MKI) telah mengalami transformasi paradigmatik seiring meningkatnya ketergantungan organisasi pada aset digital dan infrastruktur Teknologi Informasi dan Komunikasi (TIK). Dari sebuah disiplin teknis yang semula berfokus pada perlindungan perimeter, MKI kini berkembang menjadi fungsi strategis dan tata kelola *(governance)* yang bertujuan mengelola risiko terhadap kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* informasi secara sistematis [1]. Dalam konteks bisnis, MKI menjadi tanggung jawab lintas-lini organisasi dan elemen kunci dari *enterprise risk management*.

Namun, transformasi tidak berjalan mulus menciptakan sebuah kontradiksi implementasi. Secara teori, MKI telah diakui sebagai kebutuhan strategis, tetapi dalam praktiknya terjadi kesenjangan *(implementation gap)* antara konsep dan eksekusi justru melebar. Banyak organisasi yang telah memenuhi persyaratan kepatuhan terhadap standar seperti ISO/IEC 27001, tetap mengalami insiden keamanan yang signifikan [1]. Temuan ini

mengindikasikan bahwa kepatuhan tidak identik dengan keamanan *(security)* yang efektif. Fenomena ini bersumber dari mentalitas *checkbox compliance* implementasi yang berfokus pada pemenuhan daftar persyaratan formal tanpa internalisasi filosofi manajemen risiko yang sesungguhnya dan pemahaman kontekstual terhadap kebutuhan bisnis.

Akibatnya, program keamanan sering kali menjadi kaku, tidak adaptif, dan terfragmentasi dalam silo-silo teknis tanpa visi menyeluruh. Lebih lanjut, muncul krisis legitimasi fungsi keamanan yang menyebabkan banyak organisasi gagal mengukur kinerja keamanan secara kuantitatif sehingga kesulitan mengkomunikasikan *risk posture* dan *Return on Security Investment* (ROSI) kepada pemangku kepentingan *(stakeholders)* non-teknis dalam bisnis [6]–[9]. Kondisi tersebut menciptakan siklus negatif di mana keamanan dipersepsikan sebagai *cost center* yang wajib ada bukan sebagai *strategic enabler*. Oleh karena itu, diperlukan pendekatan baru yang dapat menjembatani kesenjangan teori dan praktik, mengubah keamanan menjadi fungsi yang terukur, terkelola, dan secara intrinsik selaras dengan dinamika bisnis.

2. Peran Model Maturity dalam Peningkatan Kapabilitas Keamanan

Konsep model kematangan *(maturity model)* telah diadopsi dari disiplin ilmu rekayasa perangkat lunak seperti *Capability Maturity Model Integration* (CMMI) ke ranah keamanan informasi. Secara umum, model kematangan adalah kerangka kerja evaluatif berbasis tahap yang dirancang untuk membantu organisasi mendiagnosis kapabilitas saat ini *(as-is state)* dan memetakan perjalanan peningkatan menuju keadaan yang diinginkan *(to-be state)* [10]–[15]. Dalam konteks MKI, model CMMI menyediakan peta jalan dari praktik yang reaktif dan tidak terstruktur menuju praktik yang proaktif, terukur, dan terintegrasi.

Berbagai model telah dikembangkan dengan fokus yang berbeda-beda. COBIT berfokus pada tata kelola dan manajemen proses teknologi informasi (TI). NIST *Cybersecurity Framework* (CSF) menyediakan kerangka berbasis fungsi *(Identify, Protect, Detect, Respond, Recover)* dengan Tiers yang menggambarkan rigor proses manajemen risiko. Sementara itu, *Cybersecurity Capability Maturity Model* (C2M2) dikembangkan khusus untuk menilai kapabilitas keamanan dalam lingkungan teknologi operasional *(Operational Technology/OT)* [16]. Namun, banyak model yang ada cenderung bersifat generik atau terlalu berfokus pada aspek tata kelola dan kontrol sehingga kurang memberikan panduan operasional yang spesifik untuk mengukur kinerja proses keamanan dan menghubungkannya secara langsung dengan nilai bisnis. Kekurangan inilah yang coba diatasi oleh O-ISM3. Seperti yang diilustrasikan dalam Tabel 1, O-ISM3 menonjol dengan pendekatan berbasis proses yang terukur dan penyelarasan bisnis yang eksplisit.

TABEL I
ANALISIS KOMPARATIF MODEL-MODEL MATURITY KEAMANAN INFORMASI

FITUR	O-ISM3	COBIT 4.1	NIST CSF (TIERS)	C2M2
Fokus Utama	Manajemen Proses Keamanan Informasi yang terukur dan selaras dengan bisnis.	Tata Kelola dan Manajemen TI.	Manajemen Risiko Keamanan Siber.	Evaluasi Kapabilitas Keamanan Siber (TI & OT).
Pendekatan	Berbasis proses, berorientasi bisnis, digerakkan oleh pengukuran.	Berbasis proses dan kontrol.	Berbasis fungsi *(Identify, Protect, Detect, Respond, Recover)*.	Berbasis domain (praktik keamanan).
Jumlah Tingkat Kematangan	5 *(e.g., Initial, Managed, Defined, Quantitatively Managed, Optimizing)*.	6 (0-5)	4 Tiers *(Partial, Risk Informed, Repeatable, Adaptive)*.	3 *(Initiated, Performed, Managed)*.
Penekanan pada Metrik	Sangat kuat; metrik operasional didefinisikan untuk setiap proses.	Sedang; fokus pada pencapaian tujuan proses.	Rendah; lebih pada kematangan praktik secara umum.	Sedang; fokus pada pelaksanaan praktik.
Keselarasan dengan Bisnis	Sangat tinggi; tujuan keamanan diturunkan dari tujuan bisnis.	Tinggi; sejalan dengan tujuan *enterprise*.	Tinggi; sejajar dengan kebutuhan organisasi.	Sedang; fokus pada kapabilitas teknis.

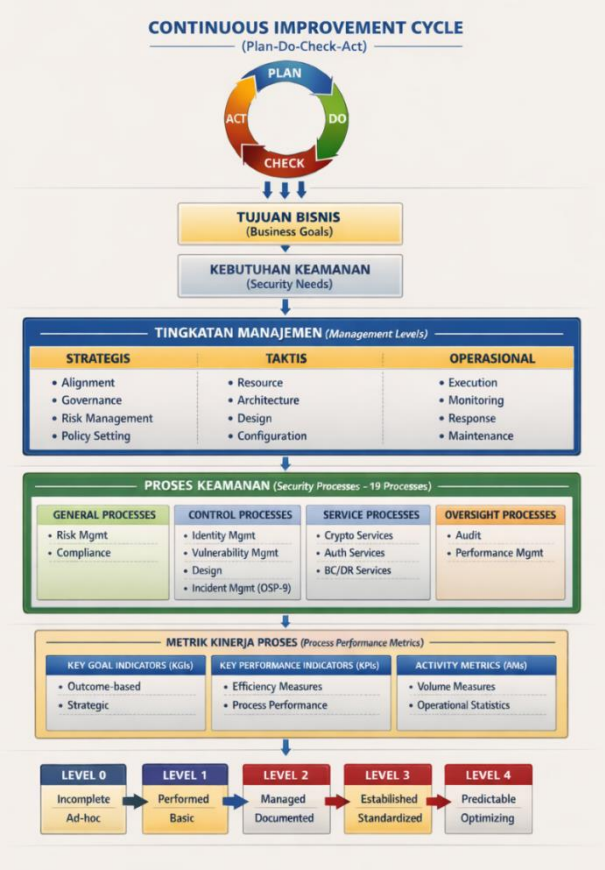
3. Arsitektur dan Filosofi *Open Information Security Management Maturity Model* (O-ISM3)

Open Information Security Management Maturity Model (O-ISM3) dikembangkan secara kolaboratif oleh The Open Group bersama ISM3 *Consortium* sebagai respons atas keterbatasan pendekatan lama. Tujuannya adalah menciptakan kerangka kerja yang praktis, terukur, dan kompatibel dengan standar seperti ISO/IEC 27001, CSC *(Critical Security Controls)*, TOGAF *(The Open Group Architecture Framework)*, SABSA *(Sherwood Applied Business Security Architecture)*, dan ITIL *(Information Technology Infrastructure Library)*, namun dengan penekanan ekstra pada dimensi kematangan dan metrik operasional [17]–[19]. Filosofi inti O-ISM3 bertumpu pada tiga aksioma operasional, yaitu Berorientasi Bisnis *(Business-Focused)*, setiap aktivitas keamanan harus diturunkan dari tujuan organisasi; Berbasis Proses *(Process-Oriented)*, manajemen keamanan dioperasionalkan melalui proses-proses yang terdefinisi; dan Digerakkan oleh Pengukuran *(Measurement-Driven)*, setiap proses harus memiliki metrik untuk menilai efektivitas dan efisiensinya [20].

Secara arsitektural, O-ISM3 dapat didekomposisi menjadi tiga lapisan komponen yang saling berinteraksi yang dapat dilihat pada Gambar 1. Pertama, Lapisan Tingkatan Manajemen *(Management Levels)* yang membentuk hierarki vertikal, yaitu Strategis (penyelarasan dengan tujuan bisnis), Taktis (perancangan dan

pengelolaan sumber daya), dan Operasional (eksekusi dan pemantauan harian) [20]. Kedua, Lapisan Proses Keamanan *(Security Processes)* yang menjadi jantung model. O-ISM3 mendefinisikan 19 proses inti yang terdistribusi pada ketiga tingkat manajemen. Proses-proses ini bersifat komprehensif namun modular, mencakup spektrum dari Manajemen Risiko Strategis (tingkat strategis), Manajemen Arsitektur Keamanan (tingkat taktis), dan Proses Operasional seperti *Vulnerability Management* (OSP-2) dan *Incident Management* (OSP-9) [1]. Setiap proses memiliki definisi operasional, yaitu tujuan *(purpose)*, aktivitas *(activities)*, masukan-keluaran *(inputs-outputs)*, dan metrik tiga lapis *Key Goal Indicators* (KGIs), *Key Performance Indicators* (KPIs), dan *Activity Metrics* (AMs). Ketiga, Model Tingkat Kematangan *(Maturity Levels)* menyediakan skala perkembangan untuk setiap proses. O-ISM3 umumnya mengadopsi skala 0 hingga 4 atau 1 hingga 5 yang merepresentasikan evolusi dari keadaan *ad-hoc* dan tidak terkelola (Level 0: *Incomplete*) menuju keadaan yang teroptimalkan dan beradaptasi secara terus-menerus (Level 4/5: *Optimizing*) [1]. Integrasi ketiga komponen menciptakan kerangka kerja yang komprehensif dan terstruktur, tidak hanya membantu organisasi memahami keadaan saat ini, tetapi juga memberikan peta jalan untuk peningkatan kapabilitas keamanan informasi yang selaras dengan tujuan bisnis.

Secara visual, hubungan integratif antara ketiga komponen arsitektur O-ISM3 dapat direpresentasikan seperti pada Gambar 1. Diagram tersebut mengilustrasikan bagaimana *Management Levels* memberikan konteks dan arahan bagi *Security Processes*, kemudian diukur menggunakan metrik tiga lapis KGIs, KPIs, AMs yang hasil pengukurannya digunakan untuk menilai *Maturity Level* setiap proses. Siklus ini berjalan dalam kerangka *continuous improvement* yang secara konstan menyesuaikan dengan tujuan bisnis organisasi. Arsitektur berlapis tersebut memastikan bahwa peningkatan kematangan keamanan informasi selalu selaras dengan nilai bisnis yang ingin dicapai.



Gambar 1. Arsitektur Integratif O-ISM3

4. Penelitian Terdahulu dan *State of the Art*

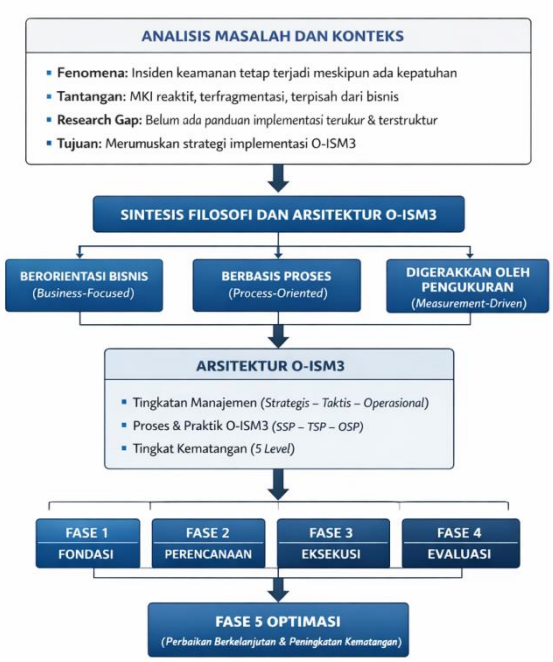
Upaya untuk membangun kerangka kerja bidang MKI telah menjadi fokus para akademisi dan praktisi selama beberapa dekade. Penelitian terdahulu telah secara luas mengeksplorasi berbagai aspek MKI, mulai dari identifikasi faktor keberhasilan hingga pengembangan model untuk menilai kematangan. Sebuah studi oleh Miloslavskaya menganalisis model kematangan O-ISM3, menyoroti evolusi standar-standar keamanan informasi dan upaya berkelanjutan untuk menyediakan alat bantu penilaian yang lebih baik bagi organisasi. Kebutuhan akan pendekatan terstruktur dan terukur menjadi prioritas. Penelitian oleh Zammani et al., mengidentifikasi kebutuhan akan model kematangan menyeluruh dengan alasan bahwa model yang ada

cenderung terlalu fokus pada proses dan teknologi, namun mengabaikan aspek manusia dan dokumen organisasional, mendasari pentingnya kerangka kerja yang menekankan keselarasan bisnis dan pengukuran.

Studi dari *Network Computing* menunjukkan bahwa banyak organisasi kesulitan menentukan baik atau buruk kinerja keamanannya, model kematangan dilihat sebagai alat untuk memberikan transparansi dan memungkinkan pengambilan keputusan yang lebih baik. Studi oleh *Secureframe* menunjukkan pentingnya dukungan eksekutif, melakukan penilaian risiko secara berkala, dan membangun budaya perbaikan berkelanjutan untuk membangun kematangan keamanan. Terdapat kesadaran luas akan pentingnya pendekatan yang matang dan terukur dalam MKI, didukung oleh berbagai model dan panduan. Namun, masih ada kekosongan dalam hal strategi implementasi yang secara khusus mengadaptasi prinsip-prinsip O-ISM3 ke dalam sebuah peta jalan yang dapat ditindaklanjuti oleh organisasi.

5. Kerangka Pemikiran Penelitian

Untuk memandu analisis dan merumuskan strategi implementasi O-ISM3, penelitian ini mengadopsi kerangka pemikiran yang terstruktur. Kerangka pemikiran divisualisasikan pada Gambar 2, menggambarkan alur logis dari identifikasi masalah hingga perumusan solusi strategis. Kerangka ini terdiri dari tiga tahap (a) Analisis Masalah dan Konteks, (b) Sintesis Filosofi dan Arsitektur O-ISM3, dan (c) Formulasi Strategi Implementasi.



Gambar 2. Kerangka Pemikiran Penelitian

III. HASIL DAN PEMBAHASAN

Berdasarkan analisis sistematis terhadap berbagai sumber termasuk publikasi resmi The Open Group, literatur akademis, artikel industri, dan materi presentasi. Penelitian ini berhasil mengidentifikasi prinsip-prinsip, komponen arsitektur, dan mekanisme implementasi yang menjadi fondasi *Open Information Security Management Maturity Model* (O-ISM3). Hasil penelitian menunjukkan bahwa O-ISM3 menawarkan pendekatan yang sistematis dan terukur untuk mentransformasi manajemen keamanan informasi dari fungsi teknis yang bersifat reaktif menjadi fungsi bisnis strategis yang proaktif dan terintegrasi. Temuan penelitian ini dapat dikategorisasi ke dalam tiga dimensi yang saling terkait, yaitu filosofi dasar, arsitektur model, dan pendekatan implementasi. Analisis mendalam terhadap data mengungkap konvergensi pandangan di berbagai sumber mengenai esensi dan mekanisme operasional O-ISM3.

1. Filosofi Tiga Pilar *Open Information Security Management Maturity Model* (O-ISM3)

Kekuatan transformatif O-ISM3 bersumber dari filosofinya yang dibangun di atas tiga pilar yang saling memperkuat *(mutually reinforcing pillars),* yaitu berorientasi bisnis *(business-focused)*, berbasis proses *(process-oriented)*, dan digerakkan oleh pengukuran *(measurement-driven)*. Pilar *business-focused* merupakan fondasi pembeda yang menempatkan O-ISM3 di atas banyak kerangka kerja keamanan. Secara eksplisit dirancang untuk menjamin bahwa setiap aktivitas keamanan secara intrinsik selaras dengan misi, tujuan, dan nilai bisnis organisasi. Implikasinya adalah bahwa alokasi investasi dan prioritas keamanan harus ditentukan berdasarkan kontribusi dalam melindungi aset dan mendukung pencapaian strategis organisasi, bukan sekadar memenuhi daftar persyaratan teknis. Selanjutnya pilar *process-oriented* menyediakan struktur operasional untuk mengelola keamanan informasi. Berbeda dengan pendekatan *checklist-based* yang berfokus pada kontrol

terisolasi, O-ISM3 mendefinisikan serangkaian proses yang komprehensif, terstruktur, dan dapat dikelola, mencakup spektrum penuh dari level strategis hingga operasional. Pendekatan pilar ini memungkinkan standardisasi, konsistensi, dan kemampuan pengulangan *(repeatability)* dalam mengelola keamanan merupakan prasyarat bagi peningkatan kematangan. Pilar ketiga *measurement-driven* merupakan elemen yang paling transformatif. O-ISM3 tidak hanya mendefinisikan proses, tetapi juga melengkapinya dengan metrik operasional untuk tiap proses, seperti diilustrasikan pada Tabel 2. Pilar ini memberdayakan organisasi dengan kemampuan untuk mengukur kinerja secara objektif, mengidentifikasi tren, memvalidasi efektivitas, dan membuat keputusan investasi berbasis data. Mengubah manajemen keamanan informasi dari praktik yang bersifat subjektif dan *ad-hoc* menjadi sebuah disiplin yang dapat dikelola dan ditingkatkan secara sistematis.

Ketiga pilar beroperasi secara sinergis dalam sebuah siklus yang berkelanjutan. Keselarasan dengan bisnis menentukan apa yang harus dilindungi dan mengapa harus dilindungi. Pendekatan berbasis proses menentukan bagaimana keamanan dikelola secara operasional. Sementara itu, pengukuran menyediakan umpan balik untuk mengevaluasi efektivitas dan mengarahkan perbaikan, sehingga menutup siklus *Plan-Do-Check-Act*. Integrasi tersebut memungkinkan O-ISM3 mentransformasi keamanan informasi menjadi fungsi secara fundamental berbeda dengan sebuah fungsi yang terukur, dapat dipertanggungjawabkan, dan secara jelas mendemonstrasikan nilai bagi bisnis.

TABEL II
SAMPEL PROSES O-ISM3 DAN METRIK TERKAIT

Tingkatan Manajemen	Kode Proses	Nama Proses	Tujuan Proses (sampel)	Metrik Kinerja (sampel)
Operasional	OSP-5	*IT Managed Domain Patching*	Mencegah insiden akibat kerentanan yang diketahui dengan menerapkan pembaruan keamanan *(patching)* pada layanan TI secara tepat waktu.	*Services Update Level:* Rata-rata jumlah hari keterlambatan penerapan tambalan di seluruh sistem. Semakin rendah semakin baik.
Operasional	OSP-24	*Handling of Incidents and Near-Incidents*	Mengelola insiden keamanan dan kejadian hampir-insiden *(near-incidents)* untuk meminimalkan dampak terhadap bisnis.	*Mean Time To Resolve (MTTR):* Rata-rata waktu yang dibutuhkan dari deteksi hingga resolusi penuh suatu insiden.
Taktis	TSP-3	*Define Security Targets and Security Objectives*	Menerjemahkan tujuan keamanan strategis organisasi menjadi target dan sasaran keamanan yang spesifik, terukur, dan dapat ditindaklanjuti.	*Coverage of Strategic Objectives:* Persentase tujuan keamanan strategis organisasi yang telah memiliki target keamanan spesifik yang didefinisikan.
Strategis	SSP-1	*Report to Stakeholders*	Mengomunikasikan status, kinerja, dan posisi risiko keamanan siber kepada pemangku kepentingan *(stakeholders)* untuk mendukung pengambilan keputusan.	*Stakeholder Satisfaction Index:* Skor kepuasan pemangku kepentingan yang diperoleh dari survei terhadap kualitas, kejelasan, dan ketepatan waktu laporan keamanan.

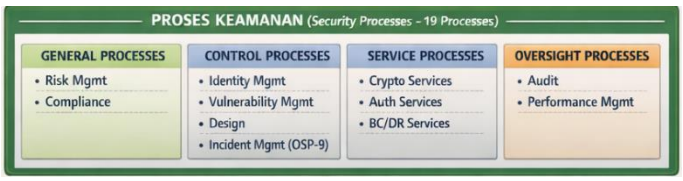
2. Arsitektur Terintegrasi *Open Information Security Management Maturity Model* (O-ISM3)

Analisis arsitektur O-ISM3 mengungkapkan sebuah struktur hirarkis terpadu yang dirancang untuk secara sistematis memandu organisasi menuju peningkatan kematangan keamanan informasi. Arsitektur ini disusun oleh tiga komponen fundamental yang saling berinteraksi, yaitu Tingkatan Manajemen, Proses Keamanan, dan Tingkat Kematangan, secara kolektif membentuk kerangka kerja yang menghubungkan strategi dengan eksekusi dan pengukuran.

Gambar 3. Tingkat Manajemen

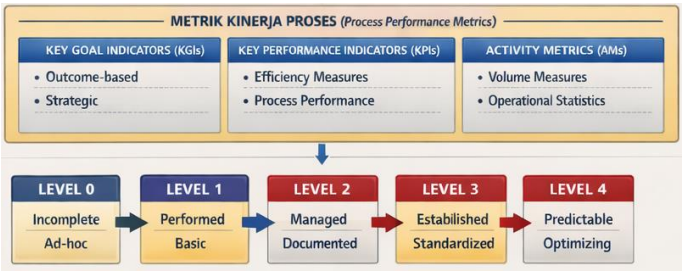
Tingkatan Manajemen membentuk hierarki pengambilan keputusan yang terdiri dari level strategis, taktis, dan operasional. Level strategis bertanggung jawab menetapkan kebijakan dan menyelaraskan keamanan dengan tujuan bisnis; level taktis menerjemahkannya menjadi rencana dan arsitektur; sementara level operasional

menjalankan proses-proses keamanan sehari-hari. Struktur hierarkis ini memastikan koherensi dan akuntabilitas dari kebijakan tingkat tinggi hingga implementasi teknis tersaji pada Gambar 3.



Gambar 4. Proses Keamanan

Proses Keamanan merupakan inti operasional dari O-ISM3 yang mendefinisikan 19 proses terstandardisasi mencakup seluruh spektrum manajemen keamanan informasi. Proses-proses ini, seperti Manajemen Sumber Daya (TSP-2), Manajemen Akses (OSP-11), dan Penanganan Insiden (OSP-24), memberikan panduan yang spesifik mengenai "apa yang harus dikelola". Setiap proses dilengkapi dengan definisi tujuan, aktivitas, masukan, keluaran, dan paling penting metrik performa yang terukur seperti disajikan pada Gambar 4.



Gambar 5. Metrik Kinerja Proses

Tingkat Kematangan menyediakan skala evaluasi untuk menilai kapabilitas setiap proses. Dengan mengadopsi skala 5 tingkat dari *Initial/Ad-hoc* hingga *Optimizing*, model ini memberikan jawaban atas "bagaimana" mengevaluasi dan meningkatkan efektivitas proses. Pada Gambar 5 setiap tingkat kematangan mendefinisikan serangkaian karakteristik dan praktik yang harus dipenuhi, memungkinkan penilaian yang obyektif dan identifikasi area perbaikan. Ketiga komponen tersebut beroperasi secara sinergis dalam sebuah sistem yang terintegrasi. Tingkatan Manajemen memberikan konteks dan arahan, Proses Keamanan menyediakan mekanisme eksekusi, dan Tingkat Kematangan menawarkan alat pengukuran dan peningkatan. Integrasi ini tidak hanya menggambarkan keadaan ideal manajemen keamanan, tetapi juga memberikan peta jalan bertahap *(gradual roadmap)*, memungkinkan organisasi untuk dapat mendiagnosis kondisi saat ini, mengidentifikasi kesenjangan, dan merencanakan langkah-langkah peningkatan terukur dan realistis.

3. Pendekatan Implementasi Siklik dan Faktor Keberhasilan O-ISM3

Temuan literatur dan studi kasus mengonfirmasi bahwa implementasi O-ISM3 yang efektif mengikuti pendekatan siklik dan inkremental, selaras dengan siklus *Plan-Do-Check-Act* (PDCA) dan prinsip perbaikan berkelanjutan diilustrasikan pada Gambar 6. Siklus siklik (iteratif) terdiri dari fase-fase berulang, yaitu Identifikasi Konteks, Penilaian Kesenjangan *(Gap Assessment)*, Perencanaan & Desain Peningkatan, Implementasi & Integrasi, dan Operasi & Tinjauan Strategis. Tujuannya adalah untuk meningkatkan kematangan manajemen keamanan informasi secara bertahap, di mana setiap siklus dimulai kembali dengan tujuan lebih tinggi sebagai respons terhadap perubahan bisnis dan ancaman baru.

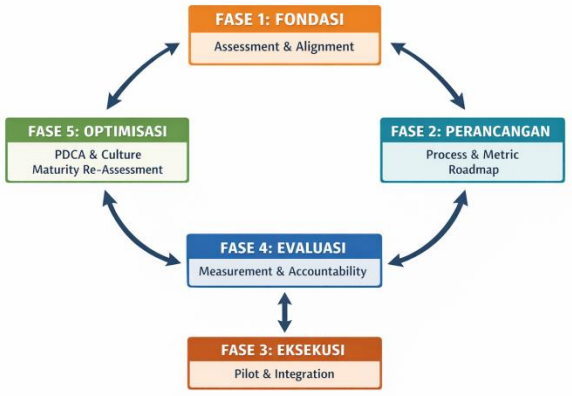
Gambar 6. Plan-Do-Check-Act (PDCA)

Siklus tersebut dimulai dengan fase penilaian *(assessment)* untuk mengukur tingkat kematangan *(maturity)* saat ini dan mengidentifikasi kesenjangan terhadap target. Fase penyelarasan strategis *(strategic alignment)* menjadi fondasi penting berikutnya, di mana tujuan keamanan secara eksplisit diturunkan dari objektif bisnis sesuai dengan faktor keberhasilan kunci keterkaitan dengan tujuan bisnis *(business alignment)*. Memastikan investasi keamanan berfokus pada area paling berdampak pada nilai bisnis. Implementasi kemudian dilakukan secara bertahap *(phased)*, diprioritaskan berdasarkan analisis risiko dan ketersediaan sumber daya. Sepanjang proses, pengukuran kinerja yang konsisten menggunakan metrik O-ISM3 (KGIs, KPIs, AMs) merupakan bagian menyeluruh dari pendekatan berbasis proses dan metrik berfungsi sebagai kompas untuk melacak kemajuan, mengidentifikasi penyimpangan, dan mendukung pengambilan keputusan berbasis data.

Bukti empiris dari studi kasus memperkuat validitas pendekatan. Implementasi di CajaMadrid (Bankia) dan *Swiss Armed Forces* menunjukkan bagaimana O-ISM3 dapat menghasilkan peningkatan terukur, mulai dari efisiensi operasional dan produktivitas tim keamanan, sampai dengan kemampuan mendemonstrasikan *Return on Security Investment* (ROSI) kepada manajemen. Temuan tersebut mengonfirmasi potensi transformasi fungsi keamanan dari *cost center* menjadi *value enabler*. Namun, penelitian juga mengidentifikasi tantangan dan prasyarat keberhasilan. Kompleksitas model dapat menjadi penghalang, terutama bagi organisasi kecil dengan sumber daya terbatas. Oleh karena itu, keberhasilan sangat bergantung pada beberapa faktor kunci. Komitmen kuat manajemen puncak untuk mengalokasikan sumber daya dan menjadikan keamanan sebagai bagian tata kelola. Pengembangan budaya organisasi yang mendukung kolaborasi, komunikasi efektif antar tingkatan, dan kesadaran keamanan berkelanjutan. Integrasi dengan kerangka kerja tata kelola dan proses bisnis yang ada. Penerapan dengan fokus pada nilai tambah, dimulai dari ruang lingkup yang terkelola untuk menghindari kompleksitas yang tidak diperlukan.

4. Strategi Implementasi *Open Information Security Management Maturity Model* (O-ISM3)

Berdasarkan sintesis temuan penelitian, dapat dirumuskan sebuah strategi Implementasi O-ISM3 yang komprehensif dan kontekstual. Strategi ini merupakan sebuah kerangka kerja adaptif *(adaptive framework)* untuk menerapkan model kematangan O-ISM3, dioperasionalkan melalui sebuah siklus implementasi berkelanjutan berbasis 5 fase berkesinambungan *(sustainable)*, dirancang untuk memandu organisasi melalui transformasi sistematis menuju kematangan keamanan informasi berkelanjutan, seperti diilustrasikan pada Gambar 7.



Gambar 7. Siklus Fase Strategi Implementasi O-ISM3

a. Fase 1: Pendirian Fondasi – Penilaian Diri dan Penyelarasan Strategis

Fase inisiasi merupakan landasan kritis yang menentukan keberhasilan implementasi. Tahap ini dimulai dengan penilaian diri secara komprehensif dan objektif. Organisasi perlu mengevaluasi kapabilitas manajemen keamanan informasi dengan memetakannya terhadap 19 proses dan tingkat kematangan O-ISM3. Melampaui sekadar penilaian *checklist-based*, memerlukan triangulasi data melalui pengumpulan informasi, wawancara mendalam dengan pemangku kepentingan pada semua level, dan analisis proses untuk menentukan *current maturity* level setiap proses, sekaligus mengidentifikasi *target maturity level* berdasarkan kebutuhan bisnis. Hasilnya adalah peta kondisi aktual *(current state map)* yang mengidentifikasi kekuatan, kelemahan, dan kesenjangan kapabilitas. Berikutnya, langkah penentu adalah penyelarasan strategis dengan tujuan bisnis. Operasionalisasi pilar *business-focused*. Tim keamanan harus berkolaborasi dengan manajemen senior untuk memahami tujuan strategis organisasi, *risk appetite*, dan prioritas bisnis. Berdasarkan pemahaman tersebut, tujuan keamanan informasi dan *Key Goal Indicators* (KGIs) yang sesuai harus diturunkan secara eksplisit *(explicitly derived)* sebagai *enabler* pencapaian tujuan bisnis. Proses ini memastikan bahwa program keamanan tidak menjadi *isolated function*, tetapi komponen menyeluruh dari pencapaian kinerja organisasi. Keluaran fase ini adalah Rencana Strategis Keamanan yang memprioritaskan area perbaikan berdasarkan dampak bisnis, sumber daya, dan urgensinya.

b. Fase 2: Perancangan – Penyusunan Rencana Implementasi Terukur

Pada fase ini menjalankan pilar *process-oriented* dan *measurement-driven*. Organisasi perlu mendefinisikan atau menyempurnakan proses target beserta kontrol-kontrolnya sesuai tingkat kematangan yang diinginkan, mencakup penyusunan atau penyempurnaan arsitektur proses, kebijakan, prosedur operasional standar (SOP), dan panduan kerja yang selaras dengan prinsip O-ISM3. Aktivitas kunci dalam fase ini adalah pendefinisian metrik kinerja. Untuk setiap proses target dan tujuannya, organisasi harus menetapkan *Key Goal Indicators* (KGIs) untuk mengukur pencapaian tujuan, *Key Performance Indicators* (KPIs) untuk mengukur efektivitas proses, dan *Activity Metrics* (AMs) untuk mengukur keluaran kegiatan spesifik, seperti contoh metrik *"Services Update Level"* untuk proses *patching*. Metrik ini harus memenuhi kriteria SMART *(Specific, Measurable, Achievable, Relevant, Time-bound)* dan terintegrasi dalam sistem pengukuran kinerja. Selain itu, diperlukan perencanaan sumber daya secara lengkap dan menyeluruh, meliputi alokasi anggaran, penugasan *champion (top management)* dan tim, serta identifikasi kebutuhan teknologi pendukung. Keluaran fase ini adalah peta jalan implementasi *(Implementation Roadmap)* jelas, rinci, *milestone* terukur, metrik keberhasilan, dan rencana kontinjensi.

c. Fase 3: Eksekusi – Implementasi Bertahap dan Integrasi

Pelaksanaan dan pengoperasian proses & kontrol. Fase ini adalah tentang menjalankan proses-proses O-ISM3 (OSP/TSP/SSP) yang telah dirancang pada tingkat kematangan yang ditargetkan, termasuk penerapan kontrol teknis dan organisasional yang telah ditetapkan, serta memulai pengumpulan data untuk metrik (AMs dan KPIs). Fase eksekusi mengubah desain menjadi realitas operasional melalui pendekatan implementasi bertahap *(phased rollout)*. Strategi ini direkomendasikan untuk mengelola kompleksitas perubahan dan meminimalkan risiko gangguan bisnis. Organisasi dapat memulai dengan proyek percontohan *(pilot project)* pada satu unit bisnis atau proses prioritas yang memungkinkan pembelajaran empiris, pengujian dan kalibrasi metrik (KGIs/KPIs), penyempurnaan, serta pembuktian nilai sebelum *scaling*. Program pelatihan dan komunikasi yang efektif menjadi penentu adopsi. Pelatihan harus diberikan kepada semua personel yang terlibat, disertai komunikasi perubahan yang konsisten untuk mengatasi resistensi dan membangun kepemilikan *(ownership)*. Mengingat O-ISM3 dirancang untuk kompatibilitas, fase ini juga mencakup integrasi dengan kerangka kerja yang ada. Organisasi yang telah mengadopsi ISO/IEC 27001, COBIT, atau ITIL dapat mengintegrasikan O-ISM3 untuk memperkaya dan mematangkan kerangka yang ada, bukan menggantikannya. Integrasi dapat memaksimalkan *return on existing investment* (ROI) dan mempercepat adopsi.

d. Fase 4: Evaluasi – Pengukuran Kinerja dan Akuntabilitas

Fase ini merupakan aktualisasi penuh pilar *measurement-driven*. Fokus utamanya adalah Pengoperasian sistem pengukuran melalui pengumpulan dan analisis data *Activity Metrics* (AMs) dan *Key Performance Indicators* (KPIs) secara sistematis menggunakan metrik yang telah didefinisikan. Data harus dikumpulkan secara konsisten, akurat, dan dianalisis untuk menghasilkan *insight* yang dapat ditindaklanjuti *(actionable insights)* mengenai efektivitas proses, pencapaian tujuan, dan area yang memerlukan intervensi. Berdasarkan analisis tersebut, organisasi harus menyusun dan menyampaikan laporan kinerja yang terdiferensiasi. Untuk audiens operasional, laporan berfokus pada metrik teknis dan kinerja proses. Untuk manajemen taktis dan strategis, laporan harus mengaitkan kinerja keamanan (KPIs) dengan pencapaian tujuan bisnis (KGIs), mendemonstrasikan kontribusi nilai *(value contribution)* dan *Return on Security Investment* (ROSI), seperti berhasil ditunjukkan dalam implementasi di *Swiss Armed Forces*. Fase ini menutup lingkar umpan balik *(feedback loop)* dan membangun akuntabilitas berbasis data. Temuan dari fase evaluasi menjadi masukan utama untuk fase 5 (optimasi), di mana rencana perbaikan dan penyesuaian strategis diformulasikan.

e. Fase 5: Optimisasi – Institusionalisasi Perbaikan Berkelanjutan

Fase akhir dan terpenting adalah institusionalisasi budaya perbaikan berkelanjutan. Implementasi O-ISM3 bukan proyek dengan *endpoint*, melainkan siklus transformasi yang terus berevolusi. Organisasi perlu mengadopsi siklus *Plan-Do-Check-Act* (PDCA) yang terstruktur, data evaluasi *("Check")* menjadi dasar perencanaan perbaikan *("Plan")*, kemudian dieksekusi *("Do")*, dan dampaknya diverifikasi *("Act")*. Penilaian kematangan berkala terhadap model O-ISM3 harus dilakukan untuk melacak kemajuan jangka panjang dan menyesuaikan strategi. Penilaian ulang kematangan *(maturity re-assessment)* terhadap 19 proses O-ISM3 harus dilakukan secara berkala atau dipicu oleh perubahan bisnis. Hasilnya dibandingkan dengan penilaian dasar *(baseline)* dari Fase 1 untuk mengukur kemajuan objektif dan menetapkan target kematangan siklus berikutnya. Organisasi memastikan bahwa sistem manajemen keamanan informasi yang ada tidak hanya responsif terhadap tantangan saat ini, tetapi juga proaktif, adaptif, dan terus meningkat, sehingga keamanan informasi benar-benar menjadi *strategic capability* yang mendukung ketangguhan dan inovasi organisasi dalam jangka panjang. Fase ini menutup siklus implementasi sekaligus memulai siklus baru yang lebih tinggi.

IV. KESIMPULAN

Penelitian ini telah merumuskan sebuah strategi implementasi *Open Information Security Management Maturity Model* (O-ISM3) yang komprehensif dan kontekstual dengan menegaskan bahwa O-ISM3 bukan sekadar kerangka kerja kepatuhan, melainkan sebuah alat transformasi strategis. Mengadopsi filosofi tiga pilar *business-focused*, *process-oriented*, dan *measurement-driven,* organisasi dapat mengubah manajemen keamanan informasi dari fungsi reaktif menjadi disiplin proaktif yang memberikan nilai bisnis yang terukur. Strategi implementasi 5 fase yang diusulkan, yaitu fondasi, perencanaan, eksekusi, evaluasi, dan optimasi, menyediakan peta jalan sistematis untuk mencapai peningkatan kematangan tersebut. Keberhasilannya bergantung pada komitmen kuat manajemen puncak, alokasi sumber daya yang memadai, dan kemauan untuk menginternalisasi budaya perbaikan berkelanjutan. Meskipun tantangan kompleksitas model, manfaat yang diperoleh, peningkatan keselarasan bisnis, pengambilan keputusan berbasis data, dan kemampuan mendemonstrasikan *Return on Security Investment* (ROSI) jauh lebih signifikan. O-ISM3 menawarkan pendekatan yang relevan dan diperlukan untuk membangun program keamanan informasi yang tangguh, adaptif, dan berorientasi nilai. Implementasinya tidak hanya memperkuat postur keamanan, tetapi pada akhirnya memungkinkan organisasi beroperasi dengan ketahanan dan kepercayaan diri di era digital.

REFERENSI

[1] M. Zammani, R. Razali, and D. Singh, “Organisational Information Security Management Maturity Model,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 9, pp. 668–678, 2021, doi: 10.14569/IJACSA.2021.0120974.
[2] N. Miloslavskaya and S. Tolstaya, “Information Security Management Maturity Models,” *Procedia Comput. Sci.*, vol. 213, no. C, pp. 49–57, 2022, doi: 10.1016/j.procs.2022.11.037.
[3] Mend.io, “From Reactive to Effective: Building Application Security that Works,” Boston, 2024. [Online]. Available: https://www.mend.io/
[4] David DeWalt, “Rethinking Cybersecurity From Cost Center To Value Driver,” Forbes Finance Council. Accessed: Nov. 18, 2025. [Online]. Available: https://www.forbes.com/councils/forbesfinancecouncil/2024/11/18/rethinking-cybersecurity-from-cost-center-to-value-driver/
[5] M. A. S. H. Almekhlafi and S. A. A. Almekhlafi, “A balanced information security maturity model based on ISO/IEC 27001:2013 and O-ISM3,” *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 6, pp. 8–6, 2023.
[6] Y. He, T. Xin, and C. Luo, “Cybersecurity Investments Metrics using FAIR-ROSI,” *UK Acad. Inf. Syst. Conf. Proc. 2024*, 2024, [Online]. Available: https://aisel.aisnet.org/ukais2024
[7] R. Y. Seetharamarao, S. Chakraborty, and S. Bardhan, “Strengthening Cyber Resilience of Small Businesses in BFSI: A CIA-Driven Strategy for Investment and Risk Management,” in *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2025, pp. 1510–1513. doi: 10.1109/COMPSAC65507.2025.00191.
[8] Y. He, T. Xin, and C. Luo, “Enhancing Cybersecurity Investment with FAIR-ROSI: A Responsible Cybersecurity Approach to Digital Society,” *Inf. Syst. Front.*, 2025, doi: 10.1007/s10796-025-10625-y.
[9] K. Barik, S. Misra, L. Fernandez-Sanz, and M. Koyuncu, “RONSI: a framework for calculating return on network security investment,” *Telecommun. Syst.*, vol. 84, no. 4, pp. 533–548, 2023, doi: 10.1007/s11235-023-01039-9.
[10] A. Singh and S. S. Gill, “Measuring the maturity of Indian small and medium enterprises for unofficial readiness for capability maturity model integration-based software process improvement,” *J. Softw. Evol. Process*, vol. 32, no. 9, p. e2261, Sep. 2020, doi: https://doi.org/10.1002/smr.2261.
[11] A. Ruzhnikov and A. Prasetyo, “Enhancing the Well Engineering Management System (WEMS) Through a Capability Maturity Model Integration (CMMI) - Based Approach,” *ADIPEC*. p. D011S002R003, Nov. 04, 2024. doi: 10.2118/221827-MS.
[12] E. J. Omol, L. W. Mburu, and P. A. Abuonji, “Digital Maturity Assessment Model (DMAM): assimilation of Design Science Research (DSR) and Capability Maturity Model Integration (CMMI),” *Digit. Transform. Soc.*, vol. 4, no. 2, pp. 128–152, Sep. 2024, doi: 10.1108/DTS-04-2024-0049.
[13] A. Rabii, S. Assoul, K. Ouazzani Touhami, and O. Roudies, “Information and cyber security maturity models: a systematic literature review,” *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 627–644, Jun. 2020, doi: 10.1108/ICS-03-2019-0039.
[14] M. Al Zeibak, M. Alshayeb, M. Baslyman, and M. Niazi, “A Cybersecurity Maturity Model for Digitally Transformed Organizations,” *J. Softw. Evol. Process*, vol. 37, no. 12, p. e70074, Dec. 2025, doi: https://doi.org/10.1002/smr.70074.
[15] M. Khraiwesh, “Measures of organizational training in the capability maturity model integration (CMMI),” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 584–592, 2020, doi: 10.14569/ijacsa.2020.0110274.
[16] F. Wafiq Zakiy and N. D. Angresti, “Comparative Analysis of Cybersecurity Maturity Frameworks: NIST-CSF and C2M2,” *JOISTECH J. Inf. Syst. Technol.*, vol. 01, no. 02, pp. 82–87, 2024.
[17] M. Graham, K. Falkner, C. Szabo, and Y. Yarom, “Security Architecture Framework for Enterprises,” *Lect. Notes Bus. Inf. Process.*, vol. 417, pp. 883–904, 2021, doi: 10.1007/978-3-030-75418-1_40.
[18] R. S. Hidayat, R. E. Indrajit, and E. Dazki, “TOGAF’s Approach in Developing an Enterprise Architecture for the Information Technology Security Industry,” *J. La Multiapp*, vol. 5, no. 5, pp. 630–645, 2024, doi: 10.37899/journallamultiapp.v5i5.1524.
[19] D. A. D. Bewasana, J. Sidabutar, S. U. Sunaringtyas, and T. Yulita, “Designing Information Security Risk Management Policies in an E-Government System Using TOGAF Enterprise Architecture,” in *2024 12th International Conference on Cyber and IT Service Management (CITSM)*, 2024, pp. 1–5. doi: 10.1109/CITSM64103.2024.10775503.
[20] The Open Group, *Open Information Security Management Maturity Model (O-ISM3)*, First edit. Berkshire: Van Haren Publishing, Zaltbommel, 2011. [Online]. Available: https://www.opengroup.org/
[21] CISA, “Zero Trust Maturity Model Version 2.0,” *Cybersecurity Infrastruct. Secur. Agency*, vol. 1, no. 1, pp. 1–32, 2023, [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf