Model Tata Kelola BOD-SIGMA" (Board of Directors - Strategic Integration Governance pada Cyber Security)

Anwar Fattah*, Wagimin[2], Robby Rokhyadi[3]

[1,2,3] Fakultas Teknik Universitas Balikpapan
Email: [1]anwar.fattah@uniba-bpn.ac.id
*Penulis Korespondensi

Abstract-Digital transformation has shifted organizational risk from being dominated by operational risks to strategic digital and cyber risks. Although IT governance frameworks such as COBIT and the ISO/IEC 27000 information security standard are widely adopted, they are generally implemented in parallel without explicit structural integration at the board level. This creates a governance gap, where cybersecurity is often treated as a technical or compliance issue, rather than as a strategic risk within the board's fiduciary mandate. The research method uses an exploratory qualitative approach through integrated literature analysis and validation in a corporate environment to test the conceptual coherence and practical relevance of the model. The results produce the BOD-SIGMA (Board-Orchestrated Digital Security Governance and Integration Model Architecture) model, which positions the board of directors as the point of integration between the evaluate-direct-monitor principles in COBIT and the governance-risk-control mechanisms in ISO/IEC 27014/27001. This model operationalizes integration through four key mechanisms: a dual-framework mapping at the strategic level, a unified CIO-CISO reporting structure, an integrated planning cycle and risk appetite, and an integrative metrics-based cyber-IT performance dashboard. Findings indicate that active board involvement in digital risk orchestration correlates with increased consistency in strategic decision-making, transparency in accountability, and maturity in IT security governance. The study concludes that effective cyber governance requires systemic integration between IT governance frameworks, information security standards, and a stakeholder-based corporate governance perspective, with the board of directors as a central actor in bridging the strategic and operational domains in the complex and dynamic era of digital risk.

IT Security, IT Governance, COBIT, and ISO 27001

Intisari*— Transformasi digital telah menggeser risiko organisasi dari dominasi risiko operasional menuju risiko digital dan siber yang bersifat strategis. Meskipun kerangka tata kelola TI seperti COBIT dan standar keamanan informasi ISO/IEC 27000 banyak diadopsi, keduanya umumnya dijalankan secara paralel tanpa integrasi struktural yang eksplisit pada level dewan direksi. Kondisi ini menciptakan kesenjangan tata kelola (governance gap), di mana keamanan siber sering diperlakukan sebagai isu teknis atau kepatuhan, bukan sebagai risiko strategis yang berada dalam mandat fiduciary dewan. Metode penelitian menggunakan pendekatan kualitatif eksploratif melalui analisis literatur terintegrasi dan validasi pada lingkungan korporasi untuk menguji koherensi konseptual serta relevansi praktis model. Hasil penelitian menghasilkan model BOD-SIGMA (Board-Orchestrated Digital Security Governance and Integration Model Architecture), yang menempatkan dewan direksi sebagai titik integrasi antara prinsip evaluate–direct–monitor dalam COBIT dan mekanisme governance–risk–control dalam ISO/IEC 27014/27001. Model ini mengoperasionalkan integrasi melalui empat mekanisme utama: pemetaan dual-framework pada level strategis, struktur pelaporan terpadu CIO–CISO, siklus perencanaan dan risk appetite terintegrasi, serta dashboard kinerja siber–TI berbasis metrik integratif. Temuan menunjukkan bahwa keterlibatan aktif dewan dalam orkestrasi risiko digital berkorelasi dengan peningkatan konsistensi pengambilan keputusan strategis, transparansi akuntabilitas, dan kematangan tata kelola TI–keamanan. Studi ini menyimpulkan bahwa tata kelola siber yang efektif memerlukan integrasi sistemik antara kerangka tata kelola TI, standar keamanan informasi, dan perspektif tata kelola korporat berbasis stakeholder, dengan dewan direksi sebagai aktor sentral dalam menjembatani domain strategis dan operasional di era risiko digital yang kompleks dan dinamis.

***Kata Kunci*— Keamanan TI, Tata Kelola TI, COBIT, ISO 27001**

I. PENDAHULUAN

Era digital saat ini menempatkan teknologi informasi (TI) sebagai komponen vital dalam strategi organisasi. Kebutuhan untuk mengoptimalkan investasi TI sambil memitigasi risiko dan memastikan kepatuhan menyebabkan tata kelola TI menjadi esensial.

Tata Kelola TI merujuk pada proses, struktur, dan mekanisme relasional yang mengarahkan dan mengontrol pemanfaatan sumber daya TI di organisasi. Dengan menetapkan tanggung jawab yang jelas, tata kelola TI mendorong transparansi dan kolaborasi antara pemangku kepentingan TI dan bisnis. Dalam kondisi ideal, mekanisme ini memastikan keselarasan strategis antara inisiatif TI dengan tujuan bisnis, mengoptimalkan nilai investasi, dan menjamin akuntabilitas serta transparansi pengambilan keputusan TI [1].

Namun, perkembangan pesat teknologi dan meningkatnya ancaman siber memperlebar celah antara situasi ideal dan kondisi nyata.[2] Organisasi menghadapi tantangan besar berupa risiko keamanan siber, kebocoran data, dan kegagalan sistem. Misalnya, pada 2025 Jaguar Land Rover mengalami serangan siber yang menghentikan produksi di pabrik-pabriknya, sehingga pemerintah Inggris harus menyediakan dana pemulihan £1,5 miliar setelah hacker membobol sistem TI perusahaan tersebut. Insiden semacam ini menegaskan bahwa keamanan siber bukan lagi masalah teknis semata, melainkan isu bisnis strategis yang membutuhkan rencana keamanan siber terintegrasi. Tetapi, realitanya banyak organisasi belum mengintegrasikan tata kelola keamanan siber ke dalam tata kelola TI yang lebih luas.

Penelitian menunjukkan, dewan direksi cenderung mendelegasikan pengawasan TI kepada manajemen dan komite-komite teknis, alih-alih menganggapnya bagian integral dari tata kelola korporat [3]. Akibatnya, strategi keamanan seringkali terfragmentasi dan tergantung pada upaya individual, bukan melalui mekanisme tata kelola yang sistematis.

Secara ideal, dewan direksi dan manajemen puncak harus memiliki kesadaran dan kapasitas memimpin tata kelola TI, termasuk keamanan siber, guna menutup celah strategis dan operasional [4]. Namun kenyataannya, kompetensi tata kelola keamanan siber di tingkat tertinggi organisasi masih rendah. Board yang seharusnya menetapkan arah strategi seringkali belum memahami sepenuhnya mekanisme audit dan pengelolaan risiko siber. Sebaliknya, pengelolaan keamanan lebih banyak dilakukan sebagai fungsi TI operasional saja, tanpa keterlibatan penuh pemangku kepentingan non-teknis. Padahal, [5] menggarisbawahi bahwa manajemen TI saja tidak cukup untuk mengatasi ancaman siber; diperlukan tata kelola siber yang melibatkan semua pemangku kepentingan dalam proses keputusan. Dengan kata lain, tanpa kerangka governansi yang komprehensif, organisasi sulit menerjemahkan strategi keamanan ke dalam tindakan nyata [6].

Pengabaian tata kelola siber yang baik membawa konsekuensi serius. Dampak langsungnya antara lain adalah kerugian finansial besar, gangguan operasional, dan kerusakan reputasi akibat insiden siber. Kekurangan pengawasan juga menimbulkan biaya tersembunyi: biaya pemulihan pascainsiden, penalti kepatuhan, dan meningkatnya premi asuransi siber [1].

Data menunjukkan 88% kebocoran data dipicu oleh kesalahan manusia, menandakan kebutuhan pelatihan dan kultur keamanan yang kuat. Konsekuensi tidak langsungnya meliputi hilangnya kepercayaan stakeholder, penurunan nilai perusahaan, hingga peluang bisnis yang terlewat karena ketidakmampuan menjaga integritas sistem. Tanpa tata kelola yang baik, resiliensi organisasi terhadap ancaman siber akan lemah.[7]

Dalam praktik tata kelola organisasi modern, kerangka COBIT dan keluarga standar ISO/IEC 27000 sering diadopsi secara bersamaan, namun dijalankan dalam domain yang relatif terpisah [8]. COBIT berfokus pada tata kelola dan manajemen TI secara menyeluruh—menekankan keselarasan strategis, penciptaan nilai, serta mekanisme evaluate–direct–monitor di tingkat dewan dan manajemen puncak. Sebaliknya, ISO/IEC 27000[9] berorientasi pada sistem manajemen keamanan informasi, dengan penekanan pada kontrol, mitigasi risiko, dan kepatuhan operasional. Keduanya sama-sama penting, tetapi dalam banyak organisasi berjalan paralel tanpa integrasi struktural yang eksplisit.

Kondisi ini menciptakan kesenjangan tata kelola (governance gap). Di satu sisi, tata kelola TI sering kali dibahas dalam kerangka strategis korporat, namun aspek keamanan siber direduksi menjadi isu teknis atau kepatuhan. Di sisi lain, implementasi keamanan informasi sering terjebak pada pendekatan kontrol berbasis standar tanpa keterkaitan yang kuat dengan arah strategis organisasi. Akibatnya, dewan direksi—sebagai pemegang mandat fiduciary dan pengawas risiko strategis—tidak selalu diposisikan sebagai aktor integratif yang menjembatani kedua domain tersebut [10].

Model yang diusulkan dalam penelitian ini berangkat dari asumsi bahwa tata kelola TI dan keamanan siber tidak dapat dipisahkan secara konseptual maupun struktural dalam konteks transformasi digital. Risiko siber bukan semata risiko operasional, melainkan risiko strategis yang berdampak pada reputasi, keberlanjutan, dan nilai perusahaan. Oleh karena itu, diperlukan suatu model tata kelola keamanan siber terintegrasi yang secara sistemik menempatkan dewan direksi sebagai penghubung antara orientasi strategis COBIT dan mekanisme kontrol keamanan ISO/IEC 27000.[11]

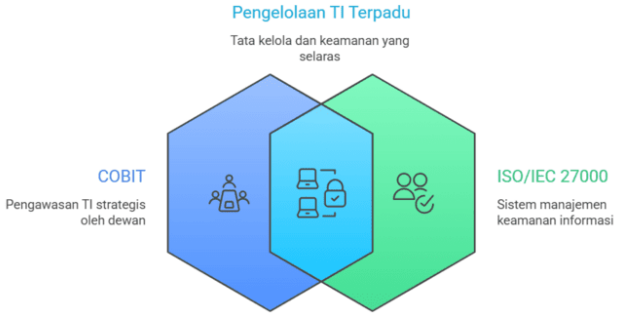
Secara konseptual, model ini mengartikulasikan peran dewan dalam tiga dimensi utama: (1) penetapan arah strategis risiko digital, (2) pembentukan struktur pengawasan dan pelaporan yang mengintegrasikan TI dan keamanan siber, serta (3) pemantauan kinerja dan akuntabilitas risiko lintas fungsi. Dengan demikian, dewan tidak lagi berperan pasif sebagai penerima laporan insiden, melainkan sebagai orkestrator tata kelola siber yang memastikan bahwa kebijakan, kontrol, dan strategi berjalan dalam satu arsitektur tata kelola yang koheren.

Pendekatan ini bertujuan untuk mengatasi fragmentasi antara tata kelola TI dan keamanan siber, sekaligus mengisi kekosongan dalam literatur yang belum secara eksplisit merumuskan mekanisme integrasi pada level dewan. Dengan membangun jembatan sistemik antara kedua kerangka tersebut, model ini diharapkan dapat memperkuat konsistensi pengambilan keputusan strategis, meningkatkan akuntabilitas, serta memperkuat ketahanan organisasi terhadap risiko siber yang semakin kompleks dan dinamis.

II. STUDI LITERATUR

Transformasi digital yang masif telah menggeser risiko organisasi dari dominasi risiko finansial dan operasional menuju risiko digital dan siber yang bersifat sistemik. Insiden pelanggaran data, gangguan layanan, dan serangan ransomware tidak lagi berdampak terbatas pada fungsi TI, tetapi memengaruhi reputasi, legitimasi, dan nilai perusahaan secara keseluruhan[12]. Dalam konteks ini, tata kelola keamanan siber berkembang dari isu teknis menjadi isu strategis tingkat dewan. Namun, literatur menunjukkan bahwa tata kelola TI dan keamanan informasi sering kali dikembangkan dalam dua jalur konseptual yang berbeda: tata kelola TI berorientasi pada keselarasan strategis dan penciptaan nilai, sedangkan keamanan informasi berfokus pada manajemen risiko dan kontrol operasional.

Kerangka seperti COBIT menekankan peran dewan dalam mengevaluasi, mengarahkan, dan memantau pengelolaan TI secara strategis [13]. Di sisi lain, keluarga standar ISO/IEC 27000 memformalkan sistem manajemen keamanan informasi berbasis siklus PDCA (plan–do–check–act) yang cenderung dijalankan pada level manajerial dan teknis [8]. Meskipun kedua kerangka ini sering diadopsi bersamaan, literatur masih minim dalam menjelaskan bagaimana keduanya dapat diintegrasikan secara sistemik melalui peran strategis dewan direksi. Kesenjangan inilah yang menjadi titik tolak penelitian ini, dengan tiga tujuan utama: (1) mengonstruksi model konseptual integrasi tata kelola TI-keamanan berbasis peran dewan, (2) melakukan eksplorasi empiris untuk memvalidasi konstruk model, dan (3) menghasilkan kerangka evaluasi diri bagi korporasi.



Gambar 1. Sinergi Pengelolaan TI Strategis dan Keamanan Informasi

A. Tata Kelola TI dan Peran Dewan Direksi

Literatur tata kelola TI secara luas menekankan pentingnya keterlibatan dewan dalam memastikan keselarasan antara strategi bisnis dan TI [14] Studi-studi awal menunjukkan bahwa organisasi dengan mekanisme tata kelola TI yang matang memiliki kinerja yang lebih baik dan kontrol risiko yang lebih efektif. Kerangka COBIT memperluas argumen ini dengan mengartikulasikan prinsip evaluate–direct–monitor sebagai tanggung jawab inti dewan [15].

Namun, sebagian besar penelitian empiris berfokus pada desain struktur (misalnya komite TI, pelaporan CIO) dan bukan pada integrasi substantif antara TI dan keamanan siber[16]. Beberapa studi kuantitatif menemukan korelasi positif antara keberadaan komite teknologi di tingkat dewan dan kualitas pengungkapan risiko siber[17]. Meski demikian, pendekatan ini cenderung strukturalis dan kurang menggali dinamika kapabilitas dewan, seperti literasi digital dan kompetensi risiko. Keterbatasan ini relevan dengan tujuan pertama penelitian, yaitu membangun model konseptual yang tidak hanya berbasis struktur formal, tetapi juga peran strategis dan kapasitas substantif dewan [10].

B. Keamanan Siber dan Sistem Manajemen

Dalam domain keamanan informasi, ISO/IEC 27000 dan pendekatan manajemen risiko telah menjadi rujukan utama[8]. Studi empiris menunjukkan bahwa sertifikasi ISO 27001 berkorelasi dengan peningkatan formalitas kontrol dan dokumentasi risiko (Baskerville et al., 2014). Namun, penelitian tersebut juga mengidentifikasi kecenderungan organisasi untuk menerapkan standar sebagai instrumen kepatuhan (compliance-driven), bukan sebagai alat integrasi strategis.

Penelitian lain dalam literatur keamanan siber menyoroti pentingnya budaya organisasi dan dukungan manajemen puncak dalam efektivitas implementasi kontrol [18], [19], [20], [21] Meski demikian, fokusnya tetap berada pada level manajemen, bukan pada peran fiduciary dewan. Hal ini menunjukkan kesenjangan konseptual antara tata kelola korporat dan praktik keamanan siber operasional—kesenjangan yang ingin dijembatani oleh model tata kelola siber terintegrasi berbasis peran dewan.

C. Perspektif Tata Kelola Korporat dan Teori Stakeholder

Teori tata kelola korporat menempatkan dewan sebagai mekanisme pengawasan utama untuk mengurangi konflik agensi dan melindungi kepentingan pemegang saham [22]. Namun, dalam konteks risiko digital, fokus shareholder-centric dianggap tidak memadai. Teori stakeholder [23] memperluas cakupan akuntabilitas perusahaan terhadap pelanggan, regulator, dan masyarakat luas—pihak-pihak yang secara langsung terdampak oleh insiden siber.

Penelitian terkini mulai mengakui bahwa risiko siber memiliki implikasi reputasional dan legitimasi yang luas [24] Meski demikian, literatur ini belum secara sistemik menghubungkan mandat normatif dewan dengan kerangka tata kelola TI dan keamanan informasi. Sebagian studi bersifat konseptual tanpa validasi empiris, sementara studi empiris sering kali tidak berakar pada kerangka teoretis yang kuat. Pola ini menunjukkan perlunya pendekatan integratif yang memadukan teori dan validasi empiris—selaras dengan tujuan kedua penelitian ini.

D. Pola, Kontradiksi, dan Kesenjangan Pengetahuan

Sintesis literatur mengungkap tiga pola utama. Pertama, terdapat konsensus bahwa keterlibatan dewan penting dalam pengawasan risiko siber. Kedua, integrasi struktural antara TI dan keamanan masih lemah, dengan banyak organisasi menjalankan keduanya secara paralel. Ketiga, sebagian besar penelitian bersifat parsial—baik berfokus pada tata kelola TI, keamanan informasi, atau tata kelola korporat—tanpa kerangka integratif yang menyatukan ketiganya.[25]

Kontradiksi muncul pada tingkat kedalaman keterlibatan dewan. Sebagian peneliti berpendapat bahwa keterlibatan yang terlalu mendalam dapat menimbulkan micromanagement, sementara penelitian lain menunjukkan bahwa minimnya literasi siber dewan justru meningkatkan risiko strategis [19]. Perbedaan ini kemungkinan dipengaruhi oleh variasi konteks organisasi dan metode penelitian yang digunakan (survei kuantitatif vs. studi kasus kualitatif).

Kesenjangan utama terletak pada kurangnya model konseptual yang secara eksplisit menjadikan dewan sebagai aktor integratif antara COBIT dan ISO/IEC 27000, serta minimnya instrumen evaluasi diri yang dapat digunakan korporasi untuk menilai kematangan sinergi tata kelola siber. Literatur saat ini belum menyediakan kerangka evaluasi berbasis peran dewan yang komprehensif dan teruji secara empiris.

Gambar 1. Kesenjangan Dalam Model Sistem Terintegrasi

Secara umum, literatur tata kelola TI dan keamanan siber cukup matang secara konseptual dan metodologis. Namun, fragmentasi teoretis dan operasional masih menjadi kelemahan utama. Banyak studi menggunakan desain survei cross-sectional yang membatasi inferensi kausal.

Selain itu, sebagian besar penelitian berfokus pada konteks negara maju, sehingga transferabilitas temuan ke konteks lain masih terbatas.

Penelitian ini berupaya mengatasi kesenjangan tersebut melalui tiga kontribusi. Pertama, mengembangkan model konseptual integratif berbasis teori tata kelola korporat dan stakeholder yang memosisikan dewan sebagai pusat orkestrasi tata kelola siber. Kedua, melakukan eksplorasi empiris melalui studi kasus dan validasi pakar untuk memastikan relevansi konstruk model. Ketiga, merancang kerangka self-assessment yang memungkinkan organisasi mengukur tingkat kematangan sinergi tata kelola TI-keamanan secara reflektif dan terstruktur.

III. MODELTATA KELOLA BOD-SIGMA

Literatur mutakhir menunjukkan bahwa perhatian terhadap peran dewan dalam tata kelola keamanan siber semakin menguat, dengan munculnya beberapa model sejenis yang relevan sebagai pembanding BOD-SIGMA.

1. Board Cybersecurity Governance Framework (BCGF)** (University of Technology Sydney, 2024) menawarkan kerangka komprehensif bagi direktur non-teknis melalui tujuh komponen utama: Assets, Risk Appetite Statement, Standards, Risk Clusters, Metrics, Questions, dan Culture. Model ini telah melalui evaluasi pakar dan survei empiris, sehingga memiliki fondasi validasi yang relatif kuat. Kesamaannya dengan BOD-SIGMA terletak pada fokus terhadap peran aktif dewan, peningkatan literasi siber, dan pentingnya pengukuran kinerja keamanan. Namun, BCGF lebih menekankan perangkat kognitif dan tata kelola berbasis pertanyaan untuk membantu proses deliberatif dewan, sedangkan BOD-SIGMA menekankan integrasi struktural antara tata kelola TI dan keamanan siber secara sistemik.[26]
2. GUBERNA/INSEAD (2025) mengidentifikasi enam tipologi model tata kelola siber tingkat dewan—mulai dari fully integrated hingga minimalist/reactive—yang dilengkapi dengan “plug-in” penguatan. Kontribusinya bersifat deskriptif-tipologis, memetakan praktik yang ada. Sebaliknya, BOD-SIGMA bersifat preskriptif dan integratif, karena tidak hanya mengklasifikasikan model, tetapi juga membangun jembatan konseptual antara dua domain tata kelola.[27]
3. Model Five Lines of Accountability dari ISACA (2024) memperluas Three Lines Model dengan menempatkan dewan sebagai “fifth line”. Model ini kuat dalam perspektif risk assurance dan hierarki akuntabilitas, namun tidak secara eksplisit mengintegrasikan tata kelola TI dan keamanan sebagai satu arsitektur strategis.[28]
4. CISA/NACD (2025) menekankan kepemilikan risiko siber oleh dewan dan pemberdayaan CISO, tetapi bersifat principles-based guidance, bukan model konseptual terintegrasi.[29]

Secara keseluruhan, meskipun model-model tersebut memperkuat urgensi peran dewan, belum ada yang secara eksplisit membangun integrasi sistemik antara tata kelola TI dan keamanan siber.

a. Integrasi Prinsip COBIT dan ISO/IEC 27000

• Kesesuaian Prinsip dan Kontrol: COBIT 2019 lebih menitikberatkan pada tata kelola TI secara keseluruhan, sedangkan ISO/IEC 27000 fokus pada pengelolaan risiko dan kontrol keamanan spesifik. Kajian literatur menunjukkan bahwa domain tata kelola dalam COBIT sangat selaras dengan struktur kontrol dalam ISO/IEC 27001, memungkinkan pembentukan model terpadu yang memperkuat alignment strategis, manajemen risiko, dan kepatuhan. Sebagai contoh, prinsip “Tailored to Enterprise Needs” dan “Dynamic Governance” dalam COBIT mendukung adaptasi model sesuai kebutuhan organisasi, sementara pendekatan PDCA (Plan-Do-Check-Act) dalam ISO/IEC 27001 menjamin perbaikan berkelanjutan dalam pengendalian keamanan.

• Kerangka Konseptual Terpadu: Penelitian terbaru mengembangkan kerangka konseptual integrasi dengan enam tema utama, yakni: (1) Strategi TI dan Digitalisasi; (2) Tata Kelola Keamanan & Budaya; (3) Manajemen Risiko & Kepatuhan Terpadu; (4) Pemantauan Kinerja & Penjaminan; (5) Penyelarasan Strategis Bisnis-TI-Keamanan; dan (6) Keterlibatan Pemangku Kepentingan & Risiko Pihak Ketiga

Gambar 2 . Sinergi Keunggulan TI, keamanan dan Bisnis

Tema-tema ini mencerminkan kekuatan COBIT dalam strategi dan tata kelola TI, serta kekhususan ISO/IEC 27000 dalam pengelolaan keamanan. Misalnya, ISO/IEC 27014 memberikan arah tata kelola bagi manajemen puncak untuk menyelaraskan strategi keamanan dengan tujuan organisasi, sedangkan COBIT menyediakan mekanisme pelaksanaan dan pengukuran risiko. Dengan demikian, kerangka ini memanfaatkan prinsip COBIT (evaluasi, arah, pemantauan) dan kontrol ISO (kebijakan, proses, kontrol) secara sinergis.

• Proses Pengembangan Strategi Siber: Proses integrasi diuraikan dalam tiga langkah utama: (1) Tinjau dan Susun Tujuan Bisnis-TI: memastikan tujuan keamanan informasi terukur sesuai sasaran bisnis (Strategic Alignment, Risk Appetite, dll.), (2) Kembangkan atau Revisi Strategi TI: menerjemahkan tema-tema di atas ke dalam kebijakan dan portofolio TI menggunakan objektif COBIT (EDM, APO, dll.), (3) Definisikan Strategi Siber: menetapkan sasaran keamanan spesifik dan kontrol berdasarkan ISO/IEC 27014 untuk arahan, ISO/IEC 27001 untuk operasionalisasi ISMS, ditambah ISO/IEC 27036/27701 untuk isu pihak ketiga dan privasi. Model ini memastikan konsistensi antara kebijakan tingkat tertinggi dan pelaksanaan taktis keamanansiber

b. MODEL INTEGRASI BOD-SIGMA: BLUEPRINT OPERASIONAL

Model integrasi BOD-SIGMA tidak sekadar menempatkan COBIT dan ISO 27000 dalam satu ruang, tetapi merancang mekanisme konversi dan penerjemahan antara kedua domain tersebut dengan Dewan Direksi sebagai "integration point". Berikut adalah rincian arsitektur integrasinya.

1. FONDASI INTEGRASI: DUAL-FRAMEWORK MAPPING (COBIT 2019 ↔ ISO/IEC 27014)

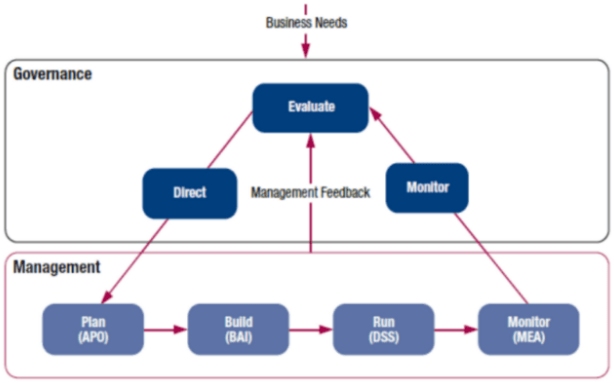
Integrasi dimulai dari level konseptual dengan memetakan domain governance COBIT 2019 (EDM – Evaluate, Direct, Monitor) ke dalam proses governance ISO/IEC 27014.[9], [30], [31]

Tabel 1. Model Integrasi BOD-SIGMA

Lapisan Integrasi	COBIT 2019 (Tata Kelola TI)	ISO/IEC 27014 (Tata Kelola Keamanan)	Fungsi Integrasi oleh Dewan
Strategis (Why)	EDM01: Memastikan penetapan dan pemeliharaan kerangka tata kelola	Evaluate: Menilai kebutuhan keamanan dan ekspektasi pemangku kepentingan	Dewan menyatakan **Risk Appetite Terintegrasi** (bukan dua dokumen terpisah untuk TI dan Keamanan)
Direktif (What)	EDM02: Memastikan optimalisasi risiko dan sumber daya	Direct: Menetapkan arah dan kebijakan keamanan	Dewan menerbitkan **Cyber Strategy Mandate** yang menjadi turunan dari IT Strategic Plan
Supervisi (How)	EDM03: Memastikan transparansi dan akuntabilitas	Monitor: Mengawasi kinerja dan kepatuhan	**Dewan menerima Unified Dashboard** yang menggabungkan metrik TI (SLA, kapasitas) dan metrik Keamanan (kerentanan, insiden)
Komunikasi	EDM04: Memastikan komunikasi kepada pemangku kepentingan	Communicate: Melaporkan status governance	Dewan memastikan **CISO dan CIO melapor secara simultan** dalam forum yang sama

Poin Kunci Integrasi:

Dalam praktik konvensional, COBIT digunakan oleh CIO untuk perencanaan TI, sementara ISO 27001 digunakan oleh CISO untuk sertifikasi. BOD-SIGMA memaksa konvergensi di level EDM (Evaluate, Direct, Monitor) sehingga dewan tidak lagi menerima dua laporan terpisah, melainkan satu laporan yang menunjukkan bagaimana investasi TI menghasilkan postur keamanan, dan bagaimana risiko keamanan mempengaruhi roadmap TI .



Gambar 3. Governance and Management Key Areas.

2. MEKANISME INTEGRASI STRUKTURAL (TATA KELOLA)

Integrasi struktural adalah desain organisasi dan akuntabilitas yang menjadikan sinergi TI-Keamanan sebagai keharusan sistemik, bukan sukarela.

A. Unified Reporting Structure (CIO-CISO Joint Accountability)

Integrasi paling mendasar adalah menghilangkan silo pelaporan. Literatur menunjukkan bahwa salah satu akar masalah adalah CISO sering melapor melalui CIO, menciptakan konflik kepentingan dan penyaringan informasi.

Mekanisme BOD-SIGMA:

- Dewan mewajibkan laporan kuartalan bersama antara CIO dan CISO.Agenda laporan tidak boleh hanya berisi status proyek TI atau daftar insiden, tetapi harus menjawab tiga pertanyaan integratif:

1. Apakah arsitektur TI yang sedang dikembangkan saat ini sudah mempertimbangkan prinsip secure-by-design?
2. Apakah pengendalian keamanan yang diimplementasi masih relevan dengan arah transformasi digital perusahaan?
3. Apakah ada duplikasi investasi atau konflik prioritas antara penguatan infrastruktur TI dan penguatan deteksi ancaman?

- KPI bersama: Persentase proyek TI yang memiliki security gate review sebelum go-live; time-to-close kerentanan pada aset kritis bisnis .

Gambar 4 . Integrasi Pelaporan CIO dan CISO

B. Cyber-Steering Committee

Banyak organisasi memiliki IT Steering Committee, tetapi keamanan hanya diundang jika diperlukan. BOD-SIGMA melembagakan kolaborasi .

Mekanisme:

- Dewan mengamanatkan pembentukan Cyber and IT Strategy Integration Committee di tingkat eksekutif (bukan hanya teknis).
- Komite bertemu bulanan, dengan risalah disampaikan ke dewan setiap kuartal.
- Komite ini diwajibkan memiliki anggota tetap dari:
  - CIO (memimpin portofolio TI)
  - CISO (memimpin portofolio keamanan)
  - CFO (memastikan alokasi anggaran terintegrasi)
  - Perwakilan Dewan (memastikan akuntabilitas strategis)

Fungsi Komite:

✓ Menengahi konflik sumber daya: misalnya, ketika proyeks TI membutuhkan akselerasi namun CISO meminta pengujian keamanan yang memakan waktu.

✓ Menyetujui exception to policy secara terdokumentasi, bukan diam-diam .

Gambar 5 . Struktur Komite Keamanan Siber

3. MEKANISME INTEGRASI PROSES (SIKLUS PERENCANAAN)

Integrasi proses berarti siklus hidup perencanaan strategis TI dan siklus perencanaan keamanan siber tidak lagi berjalan sendiri-sendiri.

A. Aligned Planning Cycle

Studi terkini menunjukkan kelemahan utama integrasi adalah perbedaan siklus . Rencana strategis TI biasanya 3-5 tahunan dengan review tahunan, sementara strategi keamanan sering reaktif terhadap insiden.

Mekanisme BOD-SIGMA:

- Sinkronisasi waktu penyusunan: Strategi keamanan siber wajib disusun dalam periode yang sama dengan penyusunan rencana strategis TI.
- Dependency mapping: Setiap inisiatif dalam master plan TI harus memiliki security enablement plan yang jelas.
- Resource pooling: Alokasi anggaran untuk keamanan tidak boleh berupa pos terpisah yang rentan dipotong, tetapi dipersentasekan dari total belanja modal TI (misal: minimum 10% dari Capex TI dialokasikan untuk pengendalian keamanan) .

Gambar 6. Integrasi Strategi TI dan Keamanan

B. Integrated Risk Appetite Statement

Praktik umum saat ini adalah perusahaan memiliki Risk Appetite Statement untuk risiko operasional, dan IT Risk Appetite terpisah untuk keamanan siber. Akibatnya, dewan kesulitan memaknai apakah eksposur risiko saat ini masih dalam batas wajar.

Mekanisme BOD-SIGMA:

o Dewan menetapkan satu pernyataan selera risiko terintegrasi yang secara eksplisit menghubungkan gangguan TI dengan dampak bisnis. Contoh: "Perusahaan menerima potensi downtime sistem core banking maksimal 4 jam per tahun. Setiap inisiatif pengembangan TI baru harus dilengkapi dengan analisis dampaknya terhadap eksposur downtime dan kontrol mitigasi yang membuat risikonya tetap dalam batas tersebut.

Gambar 7. Risk Appetite Statement

4. MEKANISME INTEGRASI PENGUKURAN (METRIK TERPADU)

Pada metrik integrative di lakukan pengukuran :

A. Unified Cybersecurity & IT Performance Dashboard

Dewan tidak membutuhkan daftar panjang kerentanan teknis. Dewan membutuhkan jawaban atas pertanyaan: "Apakah uang yang kita keluarkan untuk TI membuat perusahaan lebih aman atau justru menciptakan risiko baru?"

Mekanisme BOD-SIGMA

Tabel 2. Metrik Konvensional vs Metrik BOD-SIGMA

Dimensi	Metrik Konvensional (Terpisah)	Metrik Integratif BOD-SIGMA
Efektivitas Investasi	ROI proyek TI (CIO); % kerentanan tertutup (CISO)	**Cyber-ROI**: Berapa banyak risiko bisnis yang direduksi per rupiah belanja modal TI?
Kapasitas	Uptime server, response time aplikasi	**Secure Capacity**: Persentase aset kritis yang telah dimitigasi risikonya sebelum ekspansi kapasitas dilakukan
Agilitas vs Keamanan	Time-to-market fitur baru	**Secure Velocity**: Rata-rata waktu pengembangan fitur baru yang tetap lolos security gate tanpa penundaan >48 jam
Kepatuhan	% pemenuhan kontrol ISO 27001	**Business Alignment Compliance**: % kontrol keamanan yang secara eksplisit melindungi proses bisnis prioritas tertinggi

B. Mekanisme Validasi: "Red Flag" Terintegrasi
Dewan menetapkan ambang batas peringatan bersama.Contoh: Jika utilisasi server core mencapai 85% dan jumlah kerentanan kritis di server tersebut >5, ini otomatis menjadi red flag yang wajib dilaporkan ke dewan. Logika: Kapasitas menipis + kerentanan tinggi = risiko kegagalan sistem yang sangat nyata. Ini bukan lagi masalah TI saja atau keamanan saja

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa integrasi perspektif tata kelola korporat dan teori stakeholder ke dalam kerangka tata kelola TI–keamanan menghasilkan model tata kelola siber yang lebih strategis, terstruktur, dan berorientasi pada akuntabilitas dewan. Secara khusus, hasil analisis kualitatif dan validasi korporasi mengindikasikan bahwa peran aktif dewan direksi—yang diwujudkan melalui mekanisme evaluasi, pengarahan, dan pemantauan risiko siber—berkorelasi dengan tingkat kematangan tata kelola TI-keamanan yang lebih tinggi, konsistensi pengambilan keputusan strategis, serta peningkatan kesadaran risiko lintas organisasi. Temuan ini memperkuat asumsi normatif bahwa tata kelola siber yang efektif tidak dapat semata-mata diserahkan pada manajemen atau fungsi TI, melainkan memerlukan keterlibatan eksplisit pada level puncak organisasi.

Penelitian inijuga konsisten dengan arus literatur yang menekankan pentingnya board-level cybersecurity oversight. Sejumlah penelitian sebelumnya menunjukkan bahwa keterlibatan dewan dalam isu siber berkontribusi pada peningkatan kualitas pelaporan risiko dan kesiapan respons insiden. Dalam konteks tersebut, hasil studi ini memperkuat argumen bahwa keberadaan komite risiko atau komite TI di tingkat dewan, serta agenda tetap terkait keamanan siber dalam rapat dewan, menjadi indikator struktural dari tata kelola yang lebih matang. Area kesepakatan dengan literatur sebelumnya terletak pada pengakuan bahwa risiko siber merupakan risiko strategis, bukan sekadar risiko operasional.

Dibandingkan dengan pendekatan berbasis standar keamanan informasi seperti ISO/IEC 27000, model yang diusulkan dalam penelitian ini menunjukkan bahwa standar teknis dan kontrol operasional cenderung efektif ketika diintegrasikan dalam kerangka akuntabilitas dewan. Literatur sebelumnya sering memperlakukan ISO/IEC 27000 sebagai instrumen manajemen keamanan informasi pada level manajerial. Temuan penelitian ini mengindikasikan bahwa legitimasi dan efektivitas implementasi standar tersebut meningkat ketika terdapat tekanan dan dukungan eksplisit dari dewan direksi. Di sini, kebaruan penelitian terletak pada artikulasi hubungan vertikal antara governance layer (dewan) dan control layer (manajemen dan fungsi TI), yang sebelumnya cenderung dibahas secara terpisah.

Secara keseluruhan, penelitian ini menegaskan bahwa tata kelola siber yang efektif menuntut integrasi antara kerangka tata kelola TI, prinsip keamanan informasi, dan perspektif tata kelola korporat yang berorientasi pada pemangku kepentingan. Dengan mengangkat peran dewan sebagai aktor strategis dalam orkestrasi risiko digital, studi ini berkontribusi pada pengembangan teori dan praktik tata kelola di era transformasi digital yang semakin kompleks

REFERENSI

[1] C. Ebert, A. Vizcaino, and A. Manjavacas, “IT governance,” *IEEE Softw.*, 2020, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9238656/

[2] J. Lenong, “State Cybersecurity Governance in the Fourth Industrial Revolution: An International Law Perspective,” *… Fourth Ind. Revolut. Technol. Soc. …*, 2020, doi: 10.1007/978-3-030-48230-5_4.

[3] S. Héroux and A. Fortin, “Board of directors’ attributes and aspects of cybersecurity disclosure,” *J. Manag. Gov.*, 2022, doi: 10.1007/s10997-022-09660-7.

[4] ITGI, *Board Briefing on IT Governance*. 2003.

[5] R. Nolan and F. W. McFarlan, “Information technology and the board of directors,” 2005.

[6] Y. Maleh and Y. Maleh, “Understanding Cybersecurity Standards,” *Cybersecurity in Morocco*, 2022, doi: 10.1007/978-3-031-18475-8_2.

[7] F. R. Bechara and S. B. Schuch, “Cybersecurity and global regulatory challenges,” *J. Financ. Crime*, 2021, doi: 10.1108/JFC-07-2020-0149.

[8] M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann, and K. Sakurai, “An analysis of IT assessment security maturity in higher education institution,” in *Lecture Notes in Electrical Engineering*, 2016. doi: 10.1007/978-981-10-0557-2_69.

[9] M. Spremić, “IT governance mechanisms in managing IT business value,” *WSEAS Trans. Inf. Sci. Appl.*, 2009.

[10] ISO; IEC, “Corporate governance of information technology (ISO/IEC 38500:2008(E)),” 2008.

[11] D. Sulistyowati, F. Handayani, and Y. Suryanto, “Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss,” *JOIV Int. J. …*, 2020, [Online]. Available: http://joiv.org/index.php/joiv/article/view/482

[12] G. J. Selig, “Implementing IT Governance A Practical Guide to Global Best Practices in IT Management,” *Van Haren Publ.*, 2008.

[13] S. Ali and P. Green, “Effective information technology governance mechanisms in public sectors: An Australian case,” in *PACIS 2006 - 10th Pacific Asia Conference on Information Systems: ICT and Innovation Economy*, 2006.

[14] P. Weil and J. W. Ross, "IT Governance : How Top Performers Manage IT," *Int. J. Eletronic Gov. Res.*, 2005, doi: 10.2139/ssrn.664612.
[15] R. Kerkdijk, S. Tesink, F. Fransen, and F. Falconieri, "Evidence-Based Prioritization of Cybersecurity Threats," 2021, *isaca.org*. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats
[16] N. Shariffuddin and A. Mohamed, "IT Security and IT Governance Alignment: A Review," *... 3rd Int. Conf. ...*, 2020, doi: 10.1145/3386723.3387843.
[17] M. B. Rahman, T. Karim, and I. U. Chowdhury, "Role of Boards in Cybersecurity Risk Profiling: The Case of Bangladeshi Commercial Banks," 2021. [Online]. Available: https://www.academia.edu/download/78532978/5-Role-of-Boards-in-Cyber-Security.pdf
[18] T. P. Liang, Y. C. Chiu, S. P. J. Wu, and D. Straub, "The impact of IT governance on organizational performance," in *17th Americas Conference on Information Systems 2011, AMCIS 2011*, 2011.
[19] N. Lankton, J. B. Price, and M. Karim, "Cybersecurity breaches and the role of information technology governance in audit committee charters," *J. Inf. ...*, 2021, [Online]. Available: https://publications.aaahq.org/jis/article-abstract/35/1/101/945
[20] IT Governance Institute, *Board Briefing on IT Governance*. 2003.
[21] S. De Haes and W. Van Grembergen, "IT Governance and its Mechanisms," *Inf. Syst. Control J.*, 2004, doi: citeulike-article-id:9755150.
[22] M. C. Jensen and W. H. Meckling, "Theory of the firm: Managerial behavior, agency costs and ownership structure," *J. financ. econ.*, 1976, doi: 10.1016/0304-405X(76)90026-X.
[23] S. Kotcharin, S. Eldridge, and J. Freeman, "Investigating the relationships between internal integration and external integration and their impact on combinative competitive capabilities," no. January 2016, pp. 1–12, 2010.
[24] Z. Zulkifli, N. A. Molok, N. Z. binti A. Rahim, and S. Talib, *Cyber Security Awareness Among Secondary School Students in Malaysia*. 2020.
[25] H. F. Al-Turkistani, S. Aldobaian, and ..., "Enterprise architecture frameworks assessment: Capabilities, cyber security and resiliency review," *2021 1st Int. ...*, 2021, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9425343/
[26] University of Technology Sydney, "Board Cybersecurity Governance Framewor," University of Technology Sydney.
[27] Board-Level Cybersecurity Governance Models, "No Title," 2025.
[28] ISACA, "Five Lines of Accountability: Extending the Three Lines Model," vol. 1, 2024.
[29] CISA, "Cybersecurity Governance Principles for Boards," 2925.
[30] C. Marnewick and L. Labuschagne, "An investigation into the governance of information technology projects in South Africa," *Int. J. Proj. Manag.*, 2011, doi: 10.1016/j.ijproman.2010.07.004.
[31] W. van Grembergen and S. de Haes, "COBIT as a Framework for Enterprise Governance of IT," *Enterp. Gov. Inf. Technol.*, pp. 137–164, 2009, doi: 10.1007/978-0-387-84882-2_5.