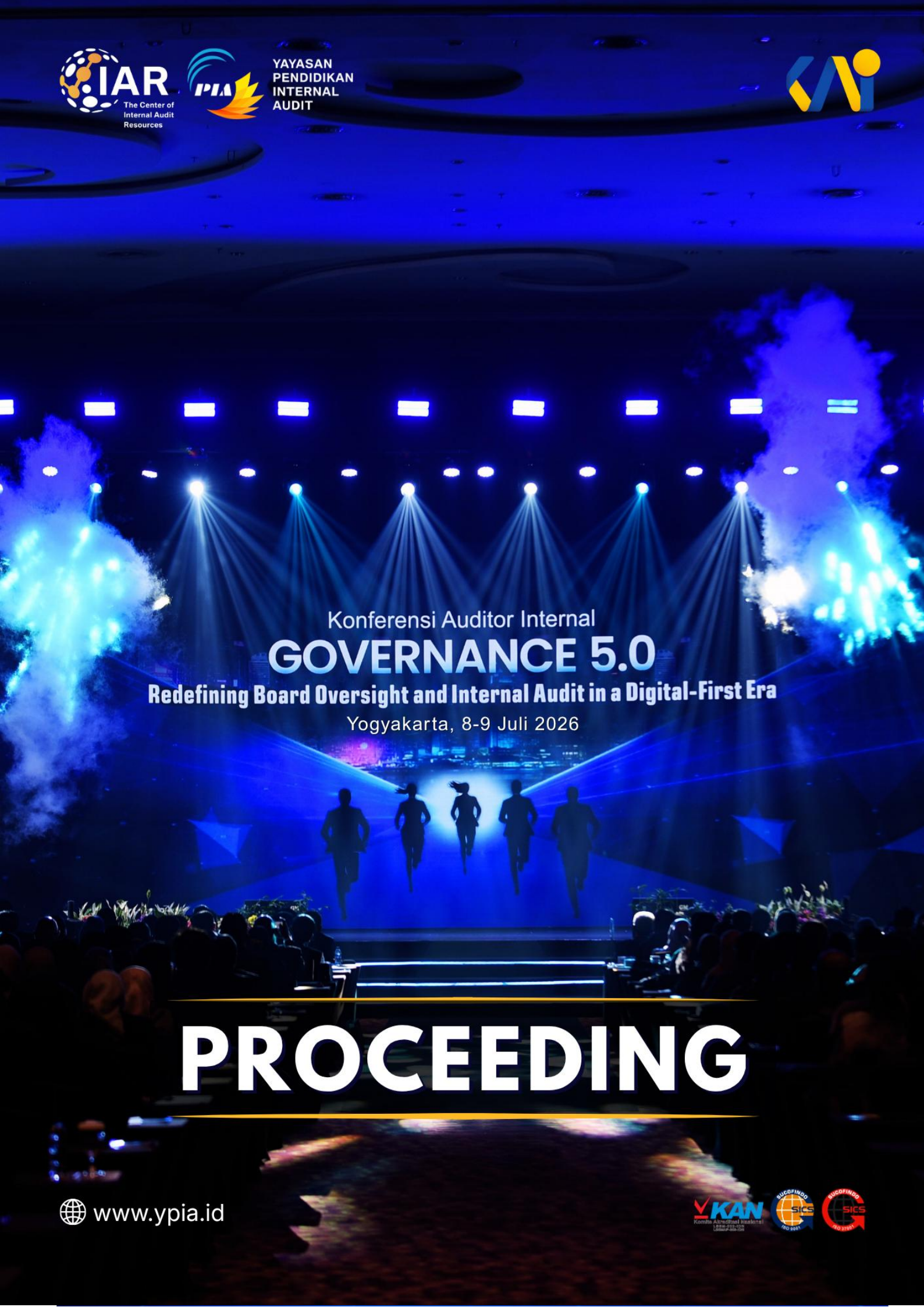

IAR
The Center of Internal Audit Resources
YAYASAN PENDIDIKAN INTERNAL AUDIT
Konferensi Auditor Internal
GOVERNANCE 5.0
Redefining Board Oversight and Internal Audit in a Digital-First Era
Yogyakarta, 8-9 Juli 2026
PROCEEDING
www.ypia.id

Kata Pengantar Ketua Umum Pengurus YPIA

Puji syukur ke hadirat Tuhan Yang Maha Esa atas terselenggaranya Konferensi Auditor Internal (KAI) 2026 pada tanggal 8–9 Juli 2026 di Yogyakarta. Mengusung tema "*Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era*," konferensi ini menjadi wadah strategis bagi regulator, anggota dewan, pimpinan organisasi, akademisi, dan praktisi untuk mendiskusikan transformasi *governance* di tengah percepatan *artificial intelligence*, meningkatnya kompleksitas risiko global, serta pergeseran menuju *digital-first governance*. Dalam lanskap ini, organisasi tidak lagi hanya dituntut memenuhi *compliance*, tetapi juga membangun *digital trust*, memperkuat *organizational resilience*, dan menciptakan *long-term value* melalui *governance* yang adaptif dan berbasis data.

Perubahan tersebut turut mentransformasi peran *Board Oversight* dan *Internal Audit*. Sejalan dengan standar, auditor internal dituntut melampaui fungsi *assurance* tradisional untuk menghasilkan *insight*, *foresight*, dan *strategic advice* melalui *continuous auditing*, *continuous assurance*, *advanced analytics*, serta pendekatan *risk-based* dalam mengantisipasi *emerging risks*. Melalui berbagai sesi yang menghadirkan para pemimpin, regulator, dan pakar dari berbagai sektor, KAI 2026 membahas isu-isu strategis mulai dari *global governance*, *Agentic AI*, transformasi digital, *Three Lines Model*, *digital trust*, hingga kepemimpinan sektor publik di era digital.

KAI 2026 juga memiliki makna yang istimewa karena menjadi momentum peluncuran buku *Beyond Compliance: Transformasi Audit Internal dalam Menjaga Integritas, Mengelola Risiko, dan Membangun Nilai*, yang merupakan hasil refleksi, pemikiran, praktik baik, dan pembelajaran kolektif para peserta *Professional Recognition Program for Qualified Internal Auditor (PRP for QIA) 2025–2026*. Kedua inisiatif tersebut menjadi wujud komitmen YPIA dalam memperkuat kompetensi, standar profesi, dan pengembangan keilmuan audit internal di Indonesia.

Proceeding ini disusun sebagai *knowledge repository* yang mendokumentasikan berbagai gagasan, pengalaman, dan pembelajaran selama konferensi. Kami berharap publikasi ini dapat menjadi referensi bagi auditor internal, anggota dewan, regulator, akademisi, serta para pemimpin organisasi dalam memperkuat praktik *governance*, manajemen risiko, dan pengendalian internal yang relevan dengan tantangan masa depan. Kami menyampaikan apresiasi kepada seluruh *keynote speaker*, narasumber, moderator, sponsor, mitra kerja, panitia, dan peserta atas kontribusi yang telah diberikan. Semoga *proceeding* ini menjadi kontribusi nyata YPIA dalam mendorong terwujudnya *governance* organisasi Indonesia yang berintegritas, adaptif, inovatif, dan berdaya saing global.

Ketua Umum Pengurus YPIA
Dr. Setyanto P. Santosa, SE, MA, QIA

Daftar Isi

PROCEEDING

Kata Pengantar Ketua Umum Pengurus YPIA i
Daftar Isi ii
Mengapa *Governance 5.0* Dilahirkan? 1
Ringkasan Eksekutif 2
Conference Substance Infographic 12
Conference Substance Matrix 13
Sekilas Mengenai KAI 2026 14
Conference Output: Executive Communiqué 21
Conference Output: Rumusan dan Rekomendasi 23
PRESS RELEASE KAI 2026 27

SUPPLEMENTARY DOCUMENT

KEYNOTE SPEECH 29
GENERAL SESSION 1 34
PANEL DISCUSSION - 1 38
TRACK 1-A 43
TRACK 1-B 47
GENERAL SESSION 2 53
PANEL DISCUSSION 2 57
TRACK 2-A 62
TRACK 2-B 66
PANEL DISCUSSION – 3 71
GENERAL SESSION 3 77
ONE ON ONE DISCUSSION 81

Mengapa *Governance 5.0* Dilahirkan?

Tata kelola tidak lahir dalam satu bentuk yang final. Ia berkembang mengikuti perubahan lingkungan organisasi, teknologi, risiko, dan ekspektasi para pemangku kepentingan. *Governance* 1.0 berangkat dari kepatuhan, memastikan aturan dan prosedur dijalankan dengan benar. Ketika organisasi dituntut tidak hanya patuh tetapi juga menghasilkan kinerja, berkembang *Governance* 2.0 yang menekankan efektivitas, efisiensi, dan penciptaan nilai. Berbagai krisis kemudian menggeser perhatian pada ketidakpastian dan ketahanan, melahirkan *Governance* 3.0 berbasis risiko. Memasuki era digital, data, *AI*, *cloud*, dan *cybersecurity* membawa *governance* pada *Governance* 4.0, ketika teknologi menjadi bagian penting dari pengambilan keputusan dan pengawasan. Perjalanan tersebut kemudian mengarah pada *Governance* 5.0: *Human-Centric & Intelligent Governance*. Pada tahap ini, pertanyaannya tidak lagi berhenti pada apakah organisasi telah patuh, berkinerja, mampu mengendalikan risiko, atau berhasil mengadopsi teknologi, tetapi bagaimana seluruh kapabilitas tersebut diintegrasikan, tetapi manusia tetap menjadi pusat pertimbangan dan pemegang keputusan; teknologi harus berjalan bersama etika, akuntabilitas, keberlanjutan, dan kepentingan para pemangku kepentingan. *Governance* 5.0 merupakan integrasi dari *compliance, performance, risk, digital capability,* dan *human intelligence* untuk membangun *trust, resilience,* serta *sustainable value* dalam jangka panjang.

Alur Evolusi *Governance* 1.0 s.d. 5.0

Konsepsi *Governance* 5.0 menjadi penting karena organisasi kini tidak cukup hanya memastikan kepatuhan, kinerja, dan pengendalian risiko, tetapi juga dituntut mampu memanfaatkan teknologi dengan tetap berpusat pada manusia, adaptif, dan berorientasi pada nilai jangka panjang. Melalui KAI 2026, YPIA membawa perspektif ini sebagai ajakan untuk melihat peran *governance* dan internal audit secara lebih progresif, bukan sekadar sebagai penjaga kepatuhan, tetapi sebagai bagian penting dalam membangun organisasi yang *intelligent, ethical, resilient,* dan berkelanjutan.

Ringkasan Eksekutif

Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era

ABSTRAK

Perkembangan *artificial intelligence*, transformasi digital, meningkatnya ancaman siber, fragmentasi geopolitik, serta perubahan ekspektasi para pemangku kepentingan telah mengubah secara fundamental cara organisasi menciptakan nilai, mengelola risiko, dan menjalankan *governance*. Dalam lingkungan yang semakin digital-first, model governance konvensional yang berfokus pada kepatuhan dan pengawasan periodik tidak lagi memadai untuk menjawab kompleksitas risiko yang berkembang secara cepat dan dinamis. Kondisi tersebut menuntut redefinisi peran *Board* dan Internal Audit agar mampu memberikan pengawasan strategis, pengambilan keputusan berbasis data, serta *assurance* yang berkelanjutan. Ringkasan Eksekutif ini menyajikan sintesis pemikiran yang berkembang dalam Konferensi Auditor Internal (KAI) 2026 dengan tema *Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era*. Berbeda dengan pendekatan *governance* sebelumnya, *Governance 5.0* menempatkan trust sebagai fondasi utama organisasi melalui integrasi kepemimpinan strategis, *governance Artificial Intelligence*, transformasi digital, *cyber resilience, ethical governance*, dan *continuous assurance*. Konsep tersebut dirumuskan melalui kerangka *Governance 5.0* DNA, yang terdiri atas enam dimensi yang saling terintegrasi, yaitu *Governance Context, Governance Evolution, Digital Capability, Governance Execution, Internal Audit Evolution,* dan *Governance Impact*. Berdasarkan sintesis *keynote speech, general session, panel discussion, track session, Executive Communiqué*, serta rumusan rekomendasi KAI 2026, keberhasilan organisasi di era digital tidak hanya ditentukan oleh kemampuan mengadopsi teknologi, melainkan oleh kemampuannya membangun *governance* yang adaptif, akuntabel, dan dipercaya. *Governance 5.0* menjadi paradigma yang menghubungkan inovasi teknologi dengan integritas, resiliensi, dan penciptaan nilai jangka panjang, sehingga memberikan arah baru bagi pengembangan praktik board oversight dan profesi internal audit di era *Artificial Intelligence.*

Kata Kunci: Governance 5.0; Board Oversight; Digital Trust; Continuous Assurance

Pendahuluan

Perkembangan *artificial intelligence*, transformasi digital, meningkatnya ancaman siber, fragmentasi geopolitik, serta perubahan ekspektasi para pemangku kepentingan telah mengubah lanskap *governance* organisasi secara fundamental. Organisasi tidak lagi hanya dihadapkan pada risiko-risiko tradisional yang bersumber dari aspek operasional maupun keuangan, tetapi juga menghadapi risiko yang semakin kompleks, saling terhubung, dan berkembang secara eksponensial, seperti

algorithmic bias, *deepfake*, *cyberattack*, *misinformation*, gangguan rantai pasok global, hingga ketidakpastian ekonomi akibat dinamika geopolitik. Kondisi tersebut menyebabkan lingkungan bisnis bergerak semakin cepat sehingga pendekatan *governance* konvensional yang bersifat periodik dan reaktif tidak lagi memadai untuk mengantisipasi perubahan yang berlangsung secara *real-time*.

Transformasi digital juga telah mengubah cara organisasi menciptakan nilai (*value creation*), mengambil keputusan, serta berinteraksi dengan para pemangku kepentingan. Pemanfaatan *big data*, *cloud computing*, *Internet of Things* (*IoT*), *robotic process automation* (*RPA*), dan terutama *artificial intelligence* telah membuka peluang besar bagi organisasi untuk meningkatkan efisiensi, inovasi, dan kualitas layanan. Namun demikian, teknologi tersebut juga memperluas eksposur terhadap risiko baru, antara lain penyalahgunaan data, rendahnya transparansi model AI, risiko pihak ketiga (*third-party risk*), serta meningkatnya kompleksitas pengendalian digital. Oleh karena itu, transformasi digital harus diimbangi dengan *governance* yang mampu memastikan bahwa teknologi digunakan secara bertanggung jawab, etis, transparan, dan akuntabel.

Perubahan tersebut turut memengaruhi ekspektasi terhadap fungsi *board oversight* dan *internal audit*. Dewan Komisaris tidak lagi hanya menjalankan fungsi pengawasan terhadap kepatuhan (*compliance oversight*), tetapi dituntut mampu memberikan pengawasan strategis terhadap implementasi teknologi, pengelolaan risiko digital, ketahanan siber (*cyber resilience*), serta kualitas pengambilan keputusan berbasis data. Di sisi lain, *internal audit* juga mengalami transformasi dari fungsi pemberi *assurance* secara periodik menjadi mitra strategis organisasi yang mampu memberikan *insight*, *foresight*, serta *continuous assurance* melalui pemanfaatan analitik data dan teknologi digital. Pergeseran ini menunjukkan bahwa *governance* modern membutuhkan mekanisme pengawasan yang lebih adaptif, kolaboratif, dan berorientasi masa depan.

Sejalan dengan perkembangan tersebut, berbagai organisasi internasional juga menempatkan risiko digital sebagai prioritas utama *governance*. *Global Risks Report* dari *World Economic Forum* menempatkan *misinformation and disinformation*, *cyber insecurity*, serta dampak negatif perkembangan AI sebagai risiko utama yang akan memengaruhi organisasi dalam beberapa tahun mendatang.

Dalam konteks tersebut, Konferensi Auditor Internal (KAI) 2026 mengangkat tema "***Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era***". Tema tersebut merefleksikan kebutuhan untuk mendefinisikan ulang paradigma *governance* organisasi agar mampu menjawab tantangan era digital. Istilah *redefining* tidak dimaknai sebagai perubahan terminologi semata, melainkan sebagai transformasi menyeluruh terhadap cara organisasi memahami, merancang, dan menjalankan fungsi *governance*. Fokus utama tidak lagi terbatas pada kepatuhan terhadap regulasi, tetapi bergeser menuju pembangunan organisasi yang adaptif, tangguh, berorientasi data, serta mampu membangun kepercayaan (*trust*) sebagai aset strategis.

Artikel ini bertujuan untuk menyajikan sintesis konseptual mengenai paradigma *Governance 5.0* berdasarkan pemikiran yang berkembang dalam Konferensi Auditor Internal 2026. Melalui integrasi berbagai *keynote speech*, *general session*, *panel discussion*, *track session*, *Executive Communiqué*, serta rumusan rekomendasi konferensi, artikel ini mengembangkan kerangka *Governance 5.0 DNA* sebagai model konseptual yang menjelaskan bagaimana organisasi perlu mentransformasikan *board oversight*, *internal audit*, kapabilitas digital, mekanisme *governance*, dan kepemimpinan agar mampu menciptakan nilai berkelanjutan di era *digital-first*. Dengan demikian, artikel ini diharapkan dapat memberikan kontribusi konseptual bagi pengembangan praktik *governance* modern sekaligus menjadi referensi bagi Dewan Komisaris, Direksi, Komite Audit, *internal auditor*, regulator, maupun akademisi dalam merancang sistem *governance* yang adaptif terhadap perkembangan teknologi dan dinamika risiko global.

Governance 5.0: Paradigma Baru *Governance* di Era *Digital-First*

Governance 5.0 merupakan paradigma *governance* yang merepresentasikan evolusi dari pendekatan *corporate governance* tradisional menuju *governance* yang adaptif, berbasis teknologi, dan berorientasi pada pembangunan kepercayaan (*trust*) di era *digital-first*. Berbeda dengan paradigma sebelumnya yang menitikberatkan pada kepatuhan (*compliance*), pengendalian (*control*), dan pelaporan (*reporting*), *Governance 5.0* memandang *governance* sebagai suatu sistem yang mampu

mengintegrasikan kepemimpinan strategis, pemanfaatan teknologi digital, pengelolaan risiko, serta penciptaan nilai (*value creation*) secara berkelanjutan.

Paradigma ini muncul sebagai respons terhadap meningkatnya kompleksitas lingkungan strategis. Perkembangan *artificial intelligence*, *machine learning*, *cloud computing*, *blockchain*, serta *digital ecosystem* telah mengubah cara organisasi beroperasi dan mengambil keputusan. Pada saat yang sama, meningkatnya risiko siber, penyalahgunaan data, *algorithmic bias*, *hallucination* pada AI generatif, serta *misinformation* menuntut adanya mekanisme pengawasan yang mampu memastikan bahwa inovasi digital tetap berjalan dalam koridor etika, transparansi, dan akuntabilitas. Dengan demikian, tantangan utama organisasi bukan lagi sekadar bagaimana mengadopsi teknologi, melainkan bagaimana memastikan teknologi tersebut digunakan secara bertanggung jawab melalui *governance* yang efektif.

Dalam perspektif *Governance 5.0*, keberhasilan organisasi tidak hanya diukur berdasarkan kinerja keuangan atau tingkat kepatuhan terhadap regulasi, tetapi juga berdasarkan kemampuannya membangun dan mempertahankan *trust*. Kepercayaan menjadi modal strategis yang memungkinkan organisasi memperoleh legitimasi publik, meningkatkan keyakinan investor, memperkuat loyalitas pelanggan, serta menjaga keberlanjutan hubungan dengan seluruh pemangku kepentingan. Oleh karena itu, *governance* harus mampu menjamin bahwa setiap keputusan organisasi diambil secara transparan, berbasis data, mempertimbangkan aspek etika, dan tetap berada di bawah *human oversight*, meskipun didukung oleh teknologi AI.

Transformasi tersebut juga mengubah secara mendasar peran *board oversight*. Dewan Komisaris tidak lagi hanya menjalankan fungsi pengawasan terhadap laporan keuangan dan kepatuhan, tetapi juga bertanggung jawab memastikan organisasi memiliki strategi digital yang jelas, *governance* AI yang memadai, *cyber resilience*, mekanisme pengelolaan risiko yang adaptif, serta budaya integritas yang mampu mendukung inovasi. Dengan kata lain, *board oversight* berevolusi dari fungsi pengawasan administratif menjadi pengawasan strategis yang berorientasi pada keberlanjutan organisasi.

Perubahan yang sama terjadi pada fungsi *internal audit*. Dalam paradigma *Governance 5.0*, *internal audit* tidak lagi diposisikan sebagai fungsi pemeriksa

(*watchdog*), tetapi sebagai *strategic assurance partner* yang memberikan *assurance*, *insight*, dan *foresight* bagi Dewan Komisaris dan manajemen. Pemanfaatan *continuous auditing*, *continuous assurance*, *advanced analytics*, AI, serta *real-time monitoring* memungkinkan *internal audit* memberikan keyakinan yang lebih cepat, lebih akurat, dan lebih relevan terhadap risiko yang berkembang secara dinamis. Dengan demikian, *internal audit* menjadi salah satu penggerak utama transformasi *governance* organisasi.

Berdasarkan sintesis berbagai pemikiran yang berkembang dalam Konferensi Auditor internal 2026, paradigma *Governance 5.0* dikembangkan melalui kerangka *Governance 5.0 DNA*, yaitu enam elemen fundamental yang saling terintegrasi. keenam elemen tersebut meliputi *Governance Context*, yang menekankan pentingnya memahami perubahan lingkungan strategis; *Governance Evolution*, yang berfokus pada transformasi *governance* dan *AI*; *digital capability*, yang memperkuat strategi digital dan *digital trust*; *governance execution*, yang mengintegrasikan mekanisme *governance* melalui *three lines model* dan *continuous assurance*; *internal audit evolution*, yang mereposisi *internal audit* sebagai *strategic value creator*; serta *governance impact*, yang memastikan seluruh proses *governance* bermuara pada peningkatan kualitas kepemimpinan, akuntabilitas, penciptaan nilai publik, dan penguatan kepercayaan pemangku kepentingan.

Dengan demikian, *Governance 5.0* bukan sekadar konsep mengenai digitalisasi *governance*, melainkan suatu paradigma yang menghubungkan inovasi teknologi dengan kepemimpinan, integritas, manajemen risiko, *board oversight*, dan *internal audit* dalam satu kerangka yang utuh. Paradigma ini menegaskan bahwa organisasi yang mampu bertahan dan berkembang pada era *digital-first* bukanlah organisasi yang semata-mata memiliki teknologi paling canggih, tetapi organisasi yang mampu membangun kepercayaan melalui *governance* yang adaptif, bertanggung jawab, dan berorientasi pada penciptaan nilai jangka panjang.

Redefining Board Oversight in a Digital-First Era

Perkembangan *artificial intelligence*, transformasi digital, dan meningkatnya kompleksitas risiko global telah mengubah secara fundamental ekspektasi terhadap fungsi *board oversight*. Jika pada paradigma *governance* sebelumnya Dewan Komisaris lebih berfokus pada pengawasan kepatuhan (*compliance oversight*), evaluasi kinerja, dan pengendalian keuangan, maka pada era *digital-first* ruang lingkup pengawasan berkembang menjadi jauh lebih luas. Dewan kini dituntut mampu memastikan bahwa organisasi tidak hanya mencapai tujuan strategisnya, tetapi juga memiliki *governance* teknologi yang bertanggung jawab, ketahanan siber (*cyber resilience*), pengelolaan risiko yang adaptif, serta mekanisme pengambilan keputusan yang transparan dan akuntabel.

Transformasi tersebut dipengaruhi oleh semakin besarnya ketergantungan organisasi terhadap teknologi digital. Pemanfaatan *artificial intelligence*, *machine learning*, *cloud computing*, *big data analytics*, serta *digital ecosystem* memberikan peluang bagi organisasi untuk meningkatkan produktivitas dan kualitas keputusan. Namun di sisi lain, teknologi juga menghadirkan berbagai risiko baru, seperti *algorithmic bias*, *hallucination*, *deepfake*, *data leakage*, hingga risiko etika dalam penggunaan AI. Risiko-risiko tersebut sering kali berkembang lebih cepat dibandingkan kemampuan organisasi dalam mengendalikan dan mengawasinya. Oleh karena itu, fungsi pengawasan Dewan Komisaris harus berevolusi dari pendekatan yang bersifat periodik menjadi *dynamic oversight* yang mampu mengantisipasi perubahan secara berkelanjutan.

Dalam paradigma *Governance 5.0*, *board oversight* tidak lagi dipandang sebagai fungsi yang bersifat administratif, melainkan sebagai mekanisme strategis yang memastikan organisasi mampu menciptakan keseimbangan antara inovasi, pengelolaan risiko, dan penciptaan nilai (*value creation*). Dewan tidak hanya mengevaluasi apakah organisasi telah mematuhi regulasi, tetapi juga menilai apakah strategi digital yang diterapkan sejalan dengan tujuan organisasi, apakah implementasi AI telah memenuhi prinsip etika dan transparansi, serta apakah risiko-risiko strategis telah dikelola secara memadai. Dengan demikian, pengawasan Dewan

bergeser dari *backward-looking oversight* menuju *forward-looking oversight* yang berorientasi pada keberlanjutan organisasi.

Perubahan tersebut juga menuntut peningkatan kualitas informasi yang diterima Dewan Komisaris. Pengambilan keputusan tidak lagi dapat mengandalkan laporan periodik yang bersifat historis, tetapi memerlukan informasi yang lebih cepat, lebih akurat, dan lebih prediktif melalui pemanfaatan *real-time dashboard*, *continuous monitoring*, serta analitik berbasis data. Dewan diharapkan mampu memanfaatkan indikator risiko strategis (*key risk indicators*), indikator kinerja (*key performance indicators*), dan informasi berbasis AI sebagai dasar dalam melakukan *strategic oversight*. Dengan demikian, kualitas pengawasan tidak hanya ditentukan oleh frekuensi rapat, tetapi oleh kemampuan Dewan dalam memahami implikasi strategis dari perubahan lingkungan eksternal maupun internal.

Konferensi Auditor Internal 2026 menegaskan bahwa *board oversight* pada era *Governance 5.0* harus mencakup sedikitnya lima dimensi utama, yaitu *strategic oversight*, *AI oversight*, *digital trust oversight*, *risk oversight*, dan *leadership oversight*. Kelima dimensi tersebut saling melengkapi dalam memastikan bahwa organisasi mampu memanfaatkan teknologi secara optimal tanpa mengorbankan prinsip integritas, akuntabilitas, maupun kepercayaan publik. Dengan demikian, keberhasilan Dewan Komisaris tidak lagi hanya diukur dari efektivitas pengawasan terhadap kepatuhan, tetapi juga dari kemampuannya membangun organisasi yang adaptif, tangguh, dan dipercaya oleh para pemangku kepentingan.

Paradigma baru ini mempertegas bahwa *board oversight* bukan sekadar fungsi pengendalian, melainkan instrumen strategis dalam mengarahkan organisasi menghadapi masa depan. Dewan Komisaris menjadi penjaga keseimbangan antara inovasi dan kehati-hatian, antara percepatan transformasi digital dan perlindungan terhadap kepentingan para pemangku kepentingan, serta antara penciptaan nilai jangka pendek dan keberlanjutan organisasi dalam jangka panjang.

Internal Audit Repositioning

Transformasi *governance* pada era *Governance 5.0* tidak hanya mengubah peran Dewan Komisaris, tetapi juga mereposisi fungsi *internal audit*. Selama beberapa dekade, *internal audit* lebih dikenal sebagai penyedia *independent assurance* yang berfokus pada evaluasi efektivitas pengendalian internal, kepatuhan terhadap regulasi, dan keandalan pelaporan keuangan. Meskipun fungsi tersebut tetap menjadi fondasi profesi, dinamika lingkungan bisnis yang semakin kompleks menuntut *internal audit* untuk memperluas kontribusinya sebagai mitra strategis organisasi (*strategic partner*) yang mampu memberikan *assurance*, *insight*, dan *foresight* secara simultan.

Perubahan tersebut didorong oleh meningkatnya ekspektasi para pemangku kepentingan terhadap kualitas *governance* organisasi. Risiko yang dihadapi organisasi saat ini tidak lagi terbatas pada aspek operasional dan keuangan, tetapi juga mencakup risiko digital, keamanan siber, *governance* AI, perubahan geopolitik, serta gangguan terhadap kepercayaan publik. Sebagian besar risiko tersebut berkembang secara cepat sehingga tidak dapat lagi direspons melalui pendekatan audit yang bersifat periodik. Oleh karena itu, *internal audit* dituntut mampu melakukan pemantauan secara berkelanjutan (*continuous auditing*) dan memberikan *continuous assurance* melalui pemanfaatan teknologi digital, analitik data, serta kecerdasan buatan.

Dalam konteks tersebut, *internal audit* tidak lagi hanya bertugas mengidentifikasi kelemahan pengendalian setelah suatu peristiwa terjadi (*detective assurance*), tetapi juga membantu organisasi mengantisipasi risiko sebelum berdampak terhadap pencapaian tujuan strategis. Pendekatan ini menempatkan *internal audit* sebagai fungsi yang proaktif, adaptif, dan berorientasi masa depan. Pemanfaatan *continuous monitoring*, *real-time analytics*, *predictive analytics*, serta *artificial intelligence* memungkinkan auditor memberikan informasi yang lebih relevan bagi Dewan Komisaris dan manajemen dalam proses pengambilan keputusan.

Transformasi tersebut juga mengubah kompetensi yang diperlukan oleh auditor internal. Selain menguasai metodologi audit dan pengendalian internal, auditor masa depan harus memiliki literasi digital, kemampuan analitik, pemahaman terhadap *governance* AI, keamanan siber, serta kemampuan berpikir strategis. Auditor internal

tidak lagi cukup hanya menjadi *control tester*, tetapi berkembang menjadi *risk analyst*, *technology-enabled auditor*, *business advisor*, sekaligus *strategic communicator* yang mampu menerjemahkan risiko menjadi informasi yang bernilai bagi organisasi.

KAI 2026 juga menegaskan bahwa evolusi *internal audit* harus tetap menjaga prinsip independensi dan objektivitas. Keterlibatan auditor dalam proses transformasi digital bukan berarti mengambil alih fungsi manajemen, melainkan memberikan pandangan independen mengenai efektivitas *governance*, manajemen risiko, dan pengendalian. Dengan demikian, *internal audit* berperan sebagai *trusted advisor* yang mendukung pengambilan keputusan strategis tanpa mengurangi independensi profesinya.

Dalam paradigma *Governance 5.0*, kontribusi *internal audit* tidak lagi diukur berdasarkan jumlah temuan atau rekomendasi yang dihasilkan, tetapi berdasarkan kemampuannya meningkatkan kualitas *governance*, memperkuat ketahanan organisasi, membangun kepercayaan pemangku kepentingan, dan mendukung penciptaan nilai jangka panjang. Pergeseran inilah yang menandai transformasi *internal audit* dari *assurance provider* menjadi *strategic value creator*.

Benang Merah dan Simpulan

Rangkaian pembahasan dalam Konferensi Auditor Internal (KAI) 2026 dirancang sebagai suatu *knowledge architecture* yang saling terintegrasi untuk menjelaskan evolusi *governance* pada era *digital-first*. Konferensi diawali dengan pembahasan mengenai perubahan lingkungan strategis global melalui *keynote speech* dan *panel discussion* mengenai perkembangan *artificial intelligence*, transformasi digital, serta fragmentasi geopolitik yang membentuk konteks baru bagi *governance* organisasi. Selanjutnya, berbagai *general session* mengeksplorasi konsep *Governance 5.0*, evolusi peran *board oversight*, dan reposisi *internal audit* dalam menghadapi era AI. Pada tingkat implementasi, berbagai *track session* membahas strategi transformasi digital, pembangunan *digital trust*, *ethical governance*, *continuous auditing*, *continuous assurance*, serta penguatan kapabilitas organisasi dalam menghadapi risiko siber (*cyber resilience*). Diskusi kemudian diperkaya melalui *panel discussion* mengenai sinergi *Three Lines Model*, pengelolaan risiko strategis, penguatan

governance sektor publik, implementasi *Business Judgment Rule*, hingga pengembangan kepemimpinan yang adaptif dalam menghadapi kompleksitas risiko masa depan. Keseluruhan rangkaian tersebut menghasilkan *Executive Communiqué*, Rumusan dan Rekomendasi Konferensi, serta Pernyataan Bersama yang menjadi refleksi kolektif para peserta mengenai arah baru *governance* Indonesia di era *Artificial Intelligence*.

Benang merah yang menghubungkan seluruh sesi adalah kesepahaman bahwa tantangan utama organisasi pada masa depan bukan lagi semata-mata mengadopsi teknologi yang semakin canggih, melainkan membangun *governance* yang mampu memastikan teknologi digunakan secara bertanggung jawab, etis, dan berorientasi pada penciptaan nilai jangka panjang. Seluruh pembahasan mengarah pada satu simpulan bahwa *Governance 5.0* merupakan paradigma baru yang mereposisi Dewan Komisaris sebagai *strategic overseer* dan *internal audit* sebagai *strategic value creator* yang memberikan *assurance*, *insight*, *foresight*, dan *strategic advice*. Pada akhirnya, seluruh transformasi tersebut bermuara pada satu tujuan utama, yaitu membangun kepercayaan (*trust*) sebagai aset strategis organisasi. Dengan demikian, keberhasilan organisasi pada era *digital-first* tidak lagi ditentukan oleh tingkat adopsi teknologi semata, tetapi oleh kemampuannya mengintegrasikan kepemimpinan, *governance*, manajemen risiko, teknologi, integritas, dan *continuous assurance* ke dalam suatu sistem yang adaptif, resilien, dan dipercaya oleh seluruh pemangku kepentingan.

CONFERENCE SUBSTANCE INFOGRAPHIC

Konferensi Auditor Internal

GOVERNANCE 5.0 DNA

THE GENETIC BLUEPRINT FOR REDEFINING BOARD OVERSIGHT AND INTERNAL AUDIT IN A DIGITAL-FIRST ERA

PERSPECTIVE	GOVERNANCE 5.0 ELEMENT	CAPABILITY BUILT (SESSION IN KAI)		CONTRIBUTION TO GOVERNANCE 5.0
01 GOVERNANCE CONTEXT Organizations that failed to understand context risk making misaligned decisions.	• Global Awareness • Strategic Intelligence • Risk Foresight	**KEYNOTE SPEECH** Global Governance Trends and Indonesia's Readiness in a Digital-First Era	**PANEL DISCUSSION – 1** Navigating Strategic Risk in a Fragmented Geopolitical and Economic Landscape	Builds strategic awareness to navigate complex and uncertain environments
02 GOVERNANCE EVOLUTION Governance lagging behind technology and AI creates oversight gaps and ethical dilemmas.	• AI Governance • Ethical Governance • Digital Integrity	**GENERAL SESSION – 1** Redefining Governance in the Age of Agentic AI: Oversight Beyond Human Decision-Making	**TRACK 1-B** Ethical Governance & Integrity Culture in Digital Organizations	Ensures responsible AI adoption and strengthens ethical oversight
03 DIGITAL CAPABILITY Digital transformation without trust can lead to data risks, fraud, and loss of stakeholder trust.	• Digital Strategy • Transformation • Digital Trust	**TRACK 1-A** Digital Strategy & Transformation	**TRACK 2-A** Building Digital Trust in a Hyperconnected World	Creates idigital capabilities and trust as the foundation for sustainable value
04 GOVERNANCE EXƟLUTION Fragmented governance and weak collaboration increase inefficiency and risk exposure.	• Integrated Governance • Continuous Oversight • Real-Time Assurance	**PANEL DISCUSSION – 2** Strengthening Governance Through Synergy: The Three Lines Model in a Digital Era	**TRACK 2-B** Continuous Auditing & Continuous Assurance	Enables integrated governance and continuous oversight across the organization
05 INTERNAL AUDIT EVOLUTION Traditional audit approach is too slow to address emerging risks and technology disruptions.	• Internal Audit 5.0 • Technology-Enabled IA • Cyber Risk Readiness	**GENERAL SESSION 2** Internal Audit Repositioned: Driving Value and Strategy in Governance 5.0	**PANEL DISCUSSION – 3** Empowering Internal Auditors to Navigate Emerging Cyber Risks	Strengthens internal audit capability to manage emerging technology and cyber risks
06 GOVERNANCE IMPACT Weak leadership and poor decision quality undermine value creation and public confidence.	• Leadership & Decision Quality • Board Oversight • Accountability	**GENERAL SESSION – 3** Governance 5.0 and the Future of Public Sector Leadership: Governing Complexity in a Digital and Data-Driven Era	**ONE ON ONE DISCUSSION** Implementation of the Business Judgment Rule in SOEs in Indonesia: Challenges & Opportunities	Drives better decisions and accountability that create public value and impact

THE GOAL
A future-ready governance system that is adaptive, ethical, data-driven, and value-creating.

GOVERNANCE 5.0
Redefining Board Oversight and Internal Audit in a Digital-First Era

OUTCOMES
- Adaptive Governance
- Technology-Enabled Board Oversight
- Internal Audit 5.0
- Digital Trust & Public Confidence
- Organizational Resilience
- Sustainable Value Creation

Conference Substance Matrix

Perspective	Why Change? (Current Challenge)	Governance 5.0 Element	Capability Built (Session in KAI)	Contribution to Governance 5.0
01. Governance Context	*Organizations face increasing uncertainty from geopolitical shifts, digital disruption, and accelerating technological change.*	*- Global Awareness - Strategic Intelligence - Risk Foresight*	*- **Keynote Speech**: Global Governance Trends and Indonesia's Readiness in a Digital-First Era **- Panel Discussion 1**: Navigating Strategic Risk in a Fragmented Geopolitical and Economic Landscape*	*Builds strategic awareness to anticipate uncertainty and improve governance resilience.*
02. Governance Evolution	*Traditional governance models are no longer sufficient to oversee AI-enabled and autonomous decision environments.*	*- AI Governance - Ethical Governance - Digital Integrity*	*- **General Session 1**: Redefining Governance in the Age of Agentic AI: Oversight Beyond Human Decision-Making **- Track 1-B**: Ethical Governance & Integrity Culture in Digital Organizations*	*Ensures responsible AI adoption while strengthening ethical oversight and organizational integrity.*
03. Digital Capability	*Digital transformation without trust creates exposure to cyber threats, data misuse, and declining stakeholder confidence.*	*- Digital Strategy - Digital Transformation - Digital Trust*	*- **Track 1-A:** Digital Strategy & Transformation **- Track 2-A**: Building Digital Trust in a Hyperconnected World*	*Develops digital capabilities and trusted digital ecosystems that support sustainable value creation.*
04. Governance Execution	*Governance functions often operate in silos, limiting organizational agility and assurance effectiveness.*	*- Integrated Governance - Continuous Oversight - Real-Time Assurance*	*- **Panel Discussion 2**: Strengthening Governance Through Synergy: The Three Lines Model in a Digital Era **- Track 2-B**: Continuous Auditing & Continuous Assurance*	*Enables integrated governance, continuous monitoring, and real-time assurance across the organization.*
05. Internal Audit Evolution	*Internal audit must evolve beyond periodic assurance to address emerging technology and cyber risks.*	*- Internal Audit 5.0 - Technology-Enabled Internal Audit - Cyber Risk Readiness*	*- **General Session 2**: Internal Audit Repositioned: Driving Value and Strategy in Governance 5.0 **- Panel Discussion 3**: Empowering Internal Auditors to Navigate Emerging Cyber Risks*	*Repositions internal audit as a strategic value creator capable of managing emerging digital risks.*
06. Governance Impact	*Long-term organizational success depends on high-quality leadership, accountability, and sound business decisions.*	*- Leadership & Decision Quality - Board Oversight - Accountability*	*- **General Session 3**: Governance 5.0 and the Future of Public Sector Leadership: Governing Complexity in a Digital and Data-Driven Era **- One-on-One Discussion**: Implementation of the Business Judgment Rule in SOEs in Indonesia: Challenges & Opportunities*	*Strengthens leadership, accountability, and decision quality to create sustainable public value and organizational trust.*

"The Governance 5.0 DNA Matrix illustrates how each KAI 2026 session systematically builds the critical capabilities required to redefine board oversight and internal audit in a digital-first era, ultimately shaping a resilient, technology-enabled, and value-driven governance ecosystem."

Sekilas Mengenai KAI 2026

Konferensi Auditor Internal (KAI) 2026 mengusung tema *"Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era".* Konferensi ini menjadi forum strategis yang mempertemukan Dewan Komisaris, Direksi, Komite Audit, Auditor Internal, regulator, akademisi, praktisi, dan para pemimpin organisasi untuk membahas arah baru *governance* di tengah percepatan perkembangan *artificial intelligence*, transformasi digital, ancaman siber, serta meningkatnya kompleksitas risiko global.

Di era digital, tantangan organisasi tidak lagi sekadar bagaimana mengadopsi teknologi, melainkan bagaimana memastikan teknologi digunakan secara bertanggung jawab melalui *governance* yang baik, kepemimpinan yang berintegritas, pengambilan keputusan yang akuntabel, serta pengelolaan risiko yang adaptif. Oleh karena itu, KAI 2026 memperkenalkan *Governance 5.0* sebagai paradigma *governance* baru yang menempatkan kepercayaan (*trust*) sebagai fondasi utama keberlanjutan organisasi. Teknologi menjadi enabler, sementara manusia tetap menjadi pusat pengambilan keputusan (human-centered governance).

Istilah "*Redefining*" dalam tema *Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era* mencerminkan kebutuhan untuk mendefinisikan kembali paradigma *governance* organisasi di tengah perubahan yang bersifat fundamental. Perkembangan *artificial intelligence*, transformasi digital, ancaman siber, kompleksitas risiko global, serta meningkatnya ekspektasi terhadap transparansi dan akuntabilitas telah mengubah cara organisasi menciptakan nilai, mengelola risiko, dan mengambil keputusan. Dalam konteks tersebut, peran Dewan Komisaris, Direksi, Komite Audit, dan Internal Audit tidak lagi cukup berfokus pada fungsi pengawasan dan kepatuhan tradisional, tetapi perlu berevolusi menjadi penggerak *governance* yang adaptif, berbasis data, berorientasi masa depan, serta mampu membangun kepercayaan (trust) sebagai aset strategis organisasi. Semangat inilah yang menjadi landasan utama penyelenggaraan Konferensi Auditor Internal (KAI) 2026.

Sebagai benang merah seluruh rangkaian konferensi, materi KAI 2026 disusun berdasarkan *Governance 5.0 DNA*, yaitu enam elemen fundamental yang membentuk organisasi yang adaptif, berintegritas, dan dipercaya dalam menghadapi era digital.

1. *Perspective 1: Governance Context*

Building Strategic Awareness

Perubahan geopolitik, perkembangan *Artificial Intelligence*, disrupsi teknologi, serta ketidakpastian ekonomi global menuntut organisasi memiliki kemampuan membaca perubahan secara lebih dini. *Governance* tidak lagi dapat bersifat reaktif, tetapi harus dibangun di atas *strategic intelligence*, *global awareness*, dan *risk foresight* agar organisasi mampu mengantisipasi tantangan sebelum berkembang menjadi krisis. *Governance 5.0* menempatkan *governance Context* sebagai fondasi pertama dalam membangun *governance* yang adaptif.

Organisasi perlu mengembangkan *global awareness* untuk memahami dinamika eksternal yang memengaruhi pencapaian tujuan strategis, memperkuat strategic intelligence guna mengintegrasikan informasi, data, dan berbagai sinyal perubahan ke dalam proses

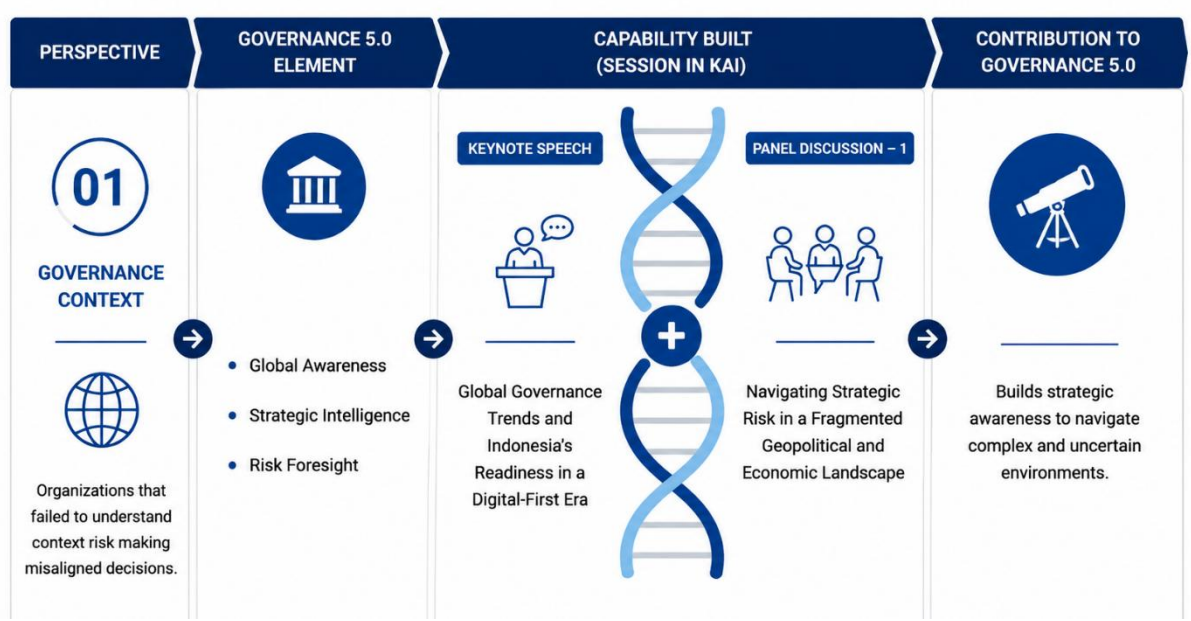
pengambilan keputusan, serta membangun *risk foresight* agar mampu mengidentifikasi *emerging risks* sebelum berkembang menjadi krisis.

Melalui kapabilitas tersebut, organisasi tidak hanya mampu merespons perubahan dengan lebih cepat, tetapi juga meningkatkan kualitas keputusan strategis, memperkuat ketahanan (*organizational resilience*), dan mengubah ketidakpastian menjadi peluang untuk menciptakan nilai jangka panjang.

Sesi terkait:

- *Keynote Speech: Global Governance Trends and Indonesia's Readiness in a Digital-First Era*
- *Panel Discussion 1: Navigating Strategic Risk in a Fragmented Geopolitical and Economic Landscape*

Gambar 1. Materi KAI Dalam Perspektif *Governance Context*



2. *Perspective 2: Governance Evolution*

Governing Artificial Intelligence Responsibly

Transformasi digital mengubah cara organisasi mengambil keputusan. *Artificial intelligence* menghadirkan peluang besar untuk meningkatkan efisiensi, kecepatan analisis, dan kualitas pengambilan keputusan, namun juga memunculkan tantangan baru terkait etika, akuntabilitas, transparansi, privasi data, serta integritas. Oleh karena itu, *Governance 5.0* menempatkan *AI Governance* sebagai bagian integral dari *governance* modern, dengan manusia tetap menjadi pengambil keputusan akhir (*human-in-the-loop*) guna memastikan bahwa setiap keputusan strategis mempertimbangkan aspek hukum, etika, dan kepentingan para pemangku kepentingan.

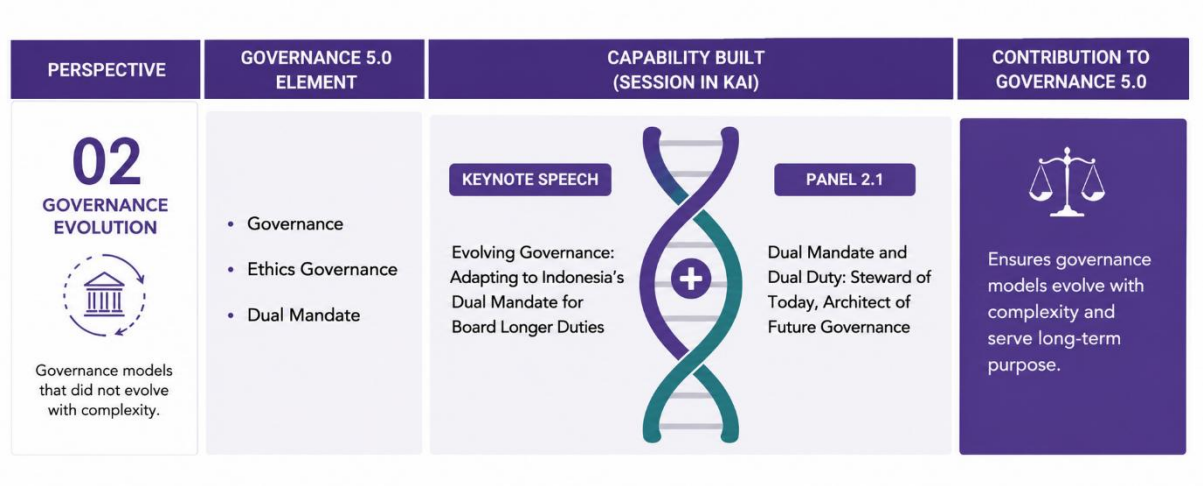
Lebih jauh, paradigma ini menekankan pentingnya *ethical governance*, yaitu *governance* yang tidak hanya menjamin kepatuhan terhadap regulasi, tetapi juga memastikan bahwa pemanfaatan teknologi dilakukan secara bertanggung jawab, adil, transparan, dan selaras dengan nilai-nilai organisasi. Dalam konteks tersebut, kepemimpinan organisasi menghadapi

dual mandate, yaitu menjaga stabilitas, akuntabilitas, dan kepercayaan terhadap *governance* yang berjalan saat ini (*steward of today*), sekaligus mendorong inovasi, transformasi digital, dan penciptaan nilai jangka panjang (*architect of the future*). Keseimbangan antara kedua mandat tersebut menjadi prasyarat agar organisasi mampu beradaptasi terhadap perubahan tanpa mengorbankan integritas dan kepercayaan publik.

Sesi terkait:

- *General Session 1: Redefining Governance in the Age of Agentic AI: Oversight Beyond Human Decision-Making*
- *Track 1-B: Ethical Governance & Integrity Culture in Digital Organizations*

Gambar 2. Materi KAI Dalam Perspektif *Governance Evolution*



3. *Perspective 3: Digital Capability*

Creating Trusted Digital Organizations

Transformasi digital yang tidak diiringi penguatan *digital trust* akan meningkatkan eksposur terhadap ancaman siber, penyalahgunaan data, kegagalan implementasi teknologi, serta menurunnya kepercayaan para pemangku kepentingan. Oleh karena itu, organisasi perlu membangun kapabilitas digital yang aman, tangguh, dan mampu menciptakan nilai secara berkelanjutan melalui *digital strategy*, *digital transformation*, dan penguatan *digital trust*. *Digital strategy* memberikan arah strategis mengenai bagaimana teknologi dimanfaatkan untuk mendukung tujuan organisasi, meningkatkan daya saing, dan menciptakan nilai bagi para pemangku kepentingan.

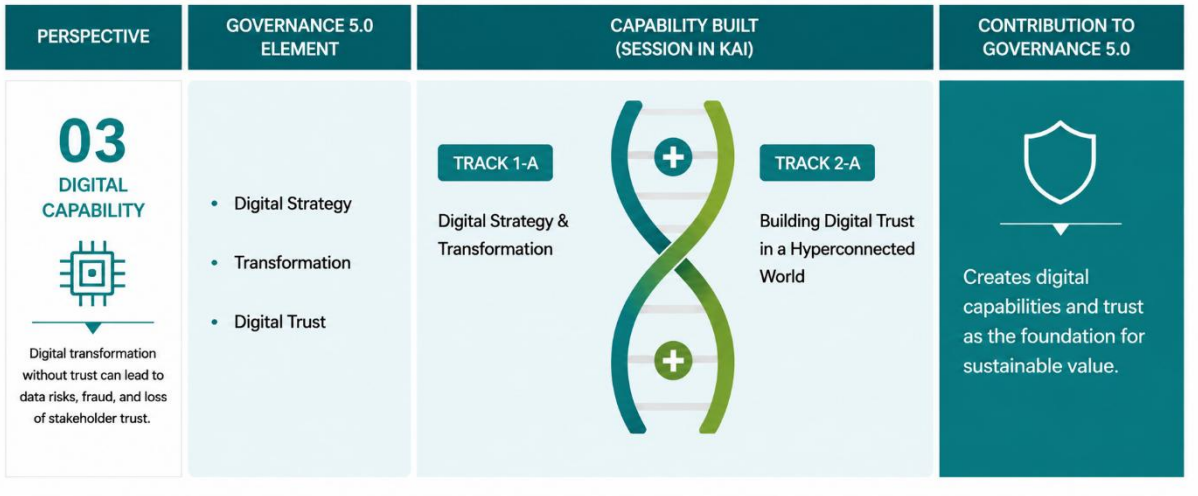
Selanjutnya, *digital transformation* menerjemahkan strategi tersebut ke dalam perubahan proses bisnis, model operasi, budaya organisasi, serta peningkatan kapabilitas sumber daya manusia agar organisasi mampu beradaptasi secara berkelanjutan terhadap perkembangan teknologi. Keseluruhan proses tersebut harus berlandaskan *digital trust*, yaitu keyakinan bahwa sistem, data, teknologi, dan proses digital dikelola secara aman, etis, transparan, serta akuntabel.

Dengan demikian, organisasi tidak hanya berhasil melakukan transformasi digital, tetapi juga membangun kepercayaan yang menjadi fondasi utama keberlanjutan, inovasi, dan penciptaan nilai jangka panjang dalam era *Governance 5.0*.

Sesi terkait:

- *Track 1-A: Digital Strategy & Transformation*
- *Track 2-A: Building Digital Trust in a Hyperconnected World*

Gambar 3. Materi KAI Dalam Perspektif *Digital Capability*



4. *Perspective 4: Governance Execution*

Connecting Governance Through Continuous Assurance

Governance yang efektif memerlukan sinergi seluruh lini organisasi. KAI 2026 menekankan pentingnya penerapan *Three Lines Model*, *continuous auditing*, *continuous assurance*, serta pengawasan berbasis data agar *governance* berjalan secara terintegrasi, *real-time*, dan mampu merespons perubahan secara cepat.

Paradigma *Governance 5.0* mendorong terwujudnya *integrated governance*, yaitu keterpaduan fungsi Dewan Komisaris, Direksi, manajemen risiko, kepatuhan, *internal audit*, serta seluruh unit operasional dalam satu sistem *governance* yang saling mendukung untuk mencapai tujuan organisasi. Melalui *governance* yang terintegrasi tersebut, organisasi dapat menerapkan *continuous oversight*, yakni mekanisme pengawasan yang berlangsung secara berkelanjutan dengan memanfaatkan data, teknologi digital, dan indikator risiko strategis sehingga pengawasan tidak lagi bergantung pada evaluasi periodik semata.

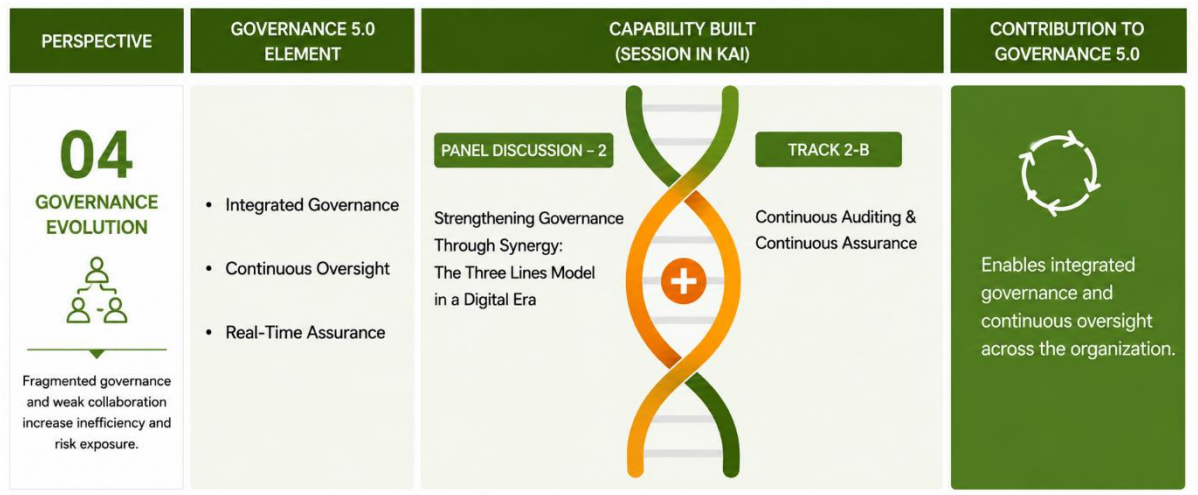
Pendekatan ini diperkuat dengan *real-time assurance*, yaitu pemberian keyakinan (*assurance*) secara lebih cepat melalui *continuous monitoring*, analitik data, dan otomatisasi, sehingga Dewan Komisaris dan manajemen memperoleh informasi yang relevan, tepat waktu, dan dapat segera digunakan dalam pengambilan keputusan. Dengan demikian, *governance* tidak hanya menjadi lebih responsif terhadap perubahan, tetapi juga mampu meningkatkan

kualitas keputusan, memperkuat ketahanan organisasi, serta menciptakan nilai secara berkelanjutan di era *digital-first*.

Sesi terkait:

- *Panel Discussion 2: Strengthening Governance Through Synergy: The Three Lines Model in a Digital Era*
- *Track 2-B*: *Continuous Auditing & Continuous Assurance*

Gambar 4. Materi KAI Dalam Perspektif *Governance Execution*



5. *Perspective 5: Internal Audit Evolution*

Repositioning Internal Audit as a Strategic Value Creator

Peran *Internal Audit* terus berevolusi dari fungsi *assurance* tradisional menjadi *strategic partner* yang memberikan *assurance*, *insight*, *foresight*, dan *strategic advice*. Auditor internal dituntut menguasai teknologi, memahami risiko digital dan keamanan siber, serta mampu mendukung kualitas pengambilan keputusan organisasi.

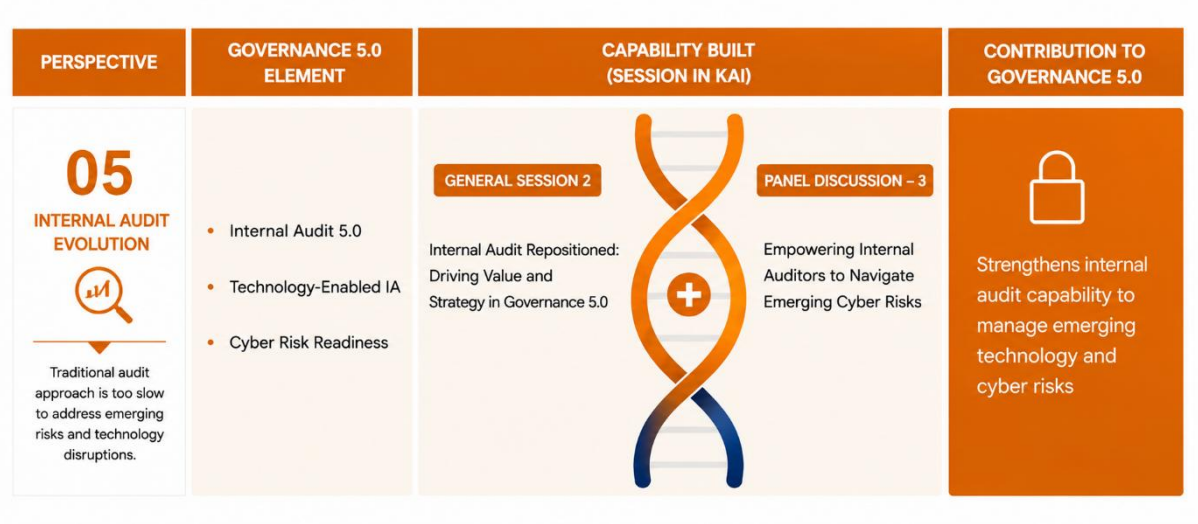
Dalam paradigma *internal audit* saat ini, auditor tidak lagi hanya berperan sebagai *watchdog*, tetapi berkembang menjadi *technology-enabled auditor* yang memanfaatkan *artificial intelligence*, *advanced analytics*, *automation*, dan *continuous assurance* untuk menghasilkan pengawasan yang lebih prediktif, adaptif, dan berbasis data.

Di sisi lain, meningkatnya ancaman terhadap infrastruktur digital menuntut organisasi membangun *cyber risk readiness*, yaitu kesiapan untuk mengidentifikasi, mengantisipasi, merespons, dan memulihkan dampak risiko siber secara efektif melalui penguatan *governance*, kapabilitas teknologi, serta kolaborasi lintas fungsi. Dengan demikian, *internal audit di era Governance 5.0* tidak hanya meningkatkan efektivitas *assurance*, tetapi juga menjadi penggerak utama dalam membangun organisasi yang resilien, terpercaya, dan siap menghadapi dinamika risiko pada era *artificial intelligence*.

Sesi terkait:

- *General Session 2: Internal Audit Repositioned: Driving Value and Strategy in Governance 5.0*
- *Panel Discussion 3*: *Empowering Internal Auditors to Navigate Emerging Cyber Risks*

Gambar 5. Materi KAI Dalam Perspektif *Internal Audit Evolution*



6. *Perspective 6: Governance Impact*

Building Sustainable Trust and Public Value

Pada akhirnya, keberhasilan *Governance 5.0* diukur dari kemampuannya menghasilkan keputusan yang berkualitas, memperkuat akuntabilitas, menciptakan nilai jangka panjang, serta membangun kepercayaan publik. Kepemimpinan yang berintegritas dan *Board Oversight* yang efektif menjadi fondasi utama organisasi yang tangguh, berdaya saing, dan dipercaya.

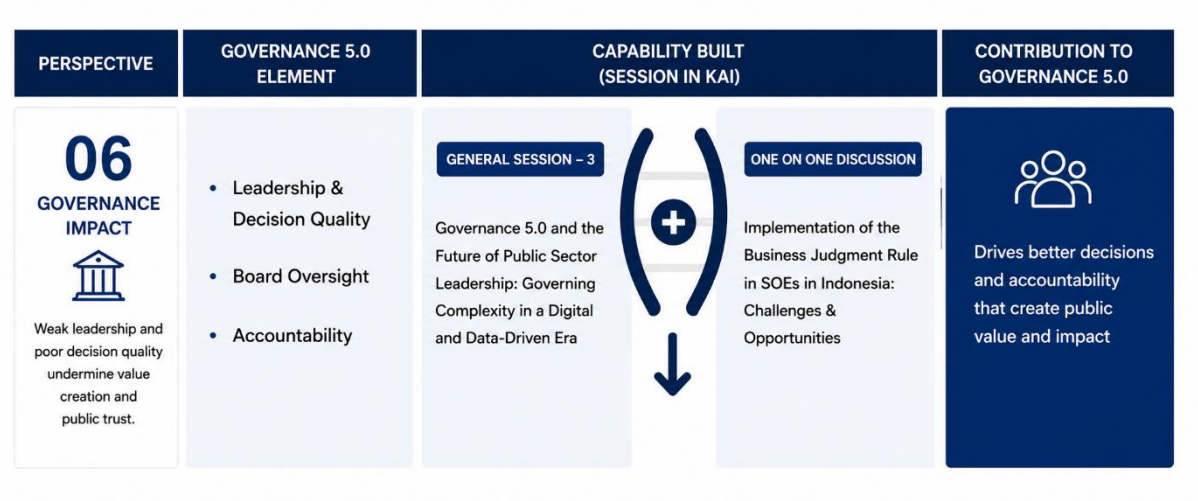
Lebih dari itu, dampak nyata *Governance 5.0* tercermin pada kemampuan organisasi untuk menyeimbangkan inovasi dengan pengelolaan risiko, mempercepat pengambilan keputusan tanpa mengurangi transparansi, serta menjaga keberlanjutan organisasi di tengah perubahan lingkungan yang semakin dinamis. Paradigma ini menempatkan *trust* sebagai *strategic asset* yang dibangun melalui *governance* yang konsisten, kepemimpinan yang beretika, pemanfaatan teknologi yang bertanggung jawab, dan kolaborasi yang efektif di seluruh lini organisasi.

Dengan demikian, keberhasilan *governance* tidak lagi hanya diukur melalui tingkat kepatuhan (*compliance*) atau kinerja finansial semata, tetapi juga melalui kemampuannya menciptakan *public value*, memperkuat *organizational resilience*, serta meningkatkan kepercayaan para pemangku kepentingan terhadap kualitas kepemimpinan dan proses pengambilan keputusan organisasi.

Sesi terkait:

- *General Session 3: Governance 5.0 and the Future of Public Sector Leadership*
- *One-on-One Discussion: Implementation of the Business Judgment Rule in SOEs in Indonesia: Challenges & Opportunities*

Gambar 6. Materi KAI Dalam Perspektif *Governance Impact*



Melalui KAI 2026, para peserta diharapkan mampu:

- meningkatkan kemampuan membaca perubahan strategis dan risiko global secara lebih proaktif;
- memperkuat penerapan *Governance 5.0* melalui AI Governance, Digital Trust, Cyber Governance, dan Ethical Governance;
- mengoptimalkan peran Dewan Komisaris, Direksi, Komite Audit, dan Internal Audit dalam menciptakan *governance* yang adaptif dan berorientasi masa depan;
- mengembangkan kapabilitas continuous auditing, continuous assurance, serta pemanfaatan data dan teknologi digital;
- membangun budaya integritas, kualitas pengambilan keputusan, dan kepercayaan sebagai fondasi keberlanjutan organisasi.

Dengan pendekatan *Governance 5.0 DNA*, KAI 2026 tidak hanya menjadi forum berbagi pengetahuan, tetapi juga menghadirkan sebuah kerangka berpikir yang komprehensif mengenai bagaimana organisasi membangun *trust* di era *Artificial Intelligence*. Setiap sesi konferensi dirancang sebagai bagian dari *"DNA" Governance 5.0* yang saling melengkapi, mulai dari memahami konteks perubahan, mengembangkan *governance* yang bertanggung jawab, memperkuat kapabilitas digital, mengintegrasikan mekanisme governance, mereposisi peran Internal Audit, hingga menghasilkan dampak nyata berupa organisasi yang adaptif, berintegritas, dan dipercaya.

Conference Output: Executive Communiqué

EXECUTIVE COMMUNIQUÉ
KONFERENSI AUDITOR INTERNAL (KAI) 2026
Membangun Kepercayaan Melalui *Governance 5.0*
Arah Baru Governance Indonesia di Era Artificial Intelligence
Yogyakarta, 9 Juli 2026

Latar Belakang

Konferensi Auditor Internal (KAI) 2026 menyimpulkan bahwa dunia sedang mengalami perubahan fundamental yang dipicu oleh perkembangan *artificial intelligence*, transformasi digital, ancaman siber, dinamika geopolitik, serta meningkatnya tuntutan masyarakat terhadap transparansi, akuntabilitas, dan integritas.

Perubahan tersebut tidak hanya mengubah teknologi, tetapi juga mengubah cara organisasi dipimpin, diawasi, mengelola risiko, dan mengambil keputusan. Dalam konteks tersebut, *governance* organisasi perlu memasuki paradigma baru yang mampu menjawab tantangan masa depan tanpa kehilangan nilai-nilai etika dan kemanusiaan.

Pesan Utama Konferensi

Konferensi Auditor Internal 2026 menyampaikan satu pesan utama:

> "Keunggulan organisasi di masa depan tidak lagi ditentukan oleh siapa yang memiliki teknologi paling canggih, tetapi oleh siapa yang paling dipercaya."

Kepercayaan merupakan modal utama organisasi. Kepercayaan lahir dari kepemimpinan yang berintegritas, *governance* yang baik, pengambilan keputusan yang bertanggung jawab, serta pemanfaatan teknologi yang beretika.

Governance 5.0

Konferensi memperkenalkan *Governance 5.0* sebagai paradigma *governance* yang mengintegrasikan: kepemimpinan yang visioner; *artificial intelligence* yang bertanggung jawab; pengelolaan risiko yang adaptif; keamanan siber yang tangguh; budaya etika dan integritas; pengawasan berbasis data; Internal Audit yang memberikan *assurance, insight, foresight,* dan *strategic advice.*

Governance 5.0 menempatkan manusia sebagai pusat pengambilan keputusan, sementara teknologi menjadi sarana untuk meningkatkan kualitas keputusan dan menciptakan nilai jangka panjang.

Lima Agenda Strategis

Konferensi merekomendasikan lima agenda nasional sebagai berikut:

1. Memperkuat *Governance*

Mengembangkan *Governance 5.0* sebagai kerangka *governance* organisasi Indonesia pada era digital.

2. Mengelola *Artificial Intelligence* secara Bertanggung Jawab

Mendorong penerapan AI Governance yang menjamin transparansi, akuntabilitas, keamanan, dan etika dalam penggunaan Artificial Intelligence.

3. Memperkuat *Board Oversight*

Meningkatkan kapasitas Dewan Komisaris, Direksi, dan Komite Audit dalam mengawasi risiko strategis, Artificial Intelligence, keamanan siber, serta transformasi digital.

4. Mereposisi Internal Audit

Menjadikan Internal Audit sebagai mitra strategis organisasi dalam mendukung *governance*, manajemen risiko, dan penciptaan nilai jangka panjang.

5. Membangun Budaya Integritas

Menjadikan integritas, transparansi, akuntabilitas, independensi, dan keberanian moral sebagai fondasi organisasi yang dipercaya.

Seruan Bersama

Konferensi Auditor Internal 2026 mengajak Pemerintah, regulator, BUMN, dunia usaha, perguruan tinggi, asosiasi profesi, dan seluruh organisasi di Indonesia untuk memperkuat kolaborasi dalam membangun *governance* yang adaptif, inovatif, berintegritas, dan berdaya saing.

Transformasi digital harus menghasilkan manfaat bagi masyarakat sekaligus memperkuat kepercayaan terhadap institusi publik maupun dunia usaha.

Pernyataan Penutup

Konferensi Auditor Internal 2026 meyakini bahwa:
- **Teknologi tanpa *governance* akan meningkatkan risiko.**
- ***Governance* tanpa integritas akan kehilangan kepercayaan.**
- **Kepercayaan merupakan fondasi utama keberlanjutan organisasi serta daya saing bangsa.**

Oleh karena itu, seluruh peserta Konferensi Auditor Internal 2026 berkomitmen mendorong implementasi ***Governance 5.0*** sebagai arah baru *governance* Indonesia dalam menghadapi era *Artificial Intelligence*.

"Kepercayaan adalah mata uang baru di era digital,
dan *Governance 5.0* adalah cara membangunnya."

Yogyakarta, 9 Juli 2026
Konferensi Auditor Internal (KAI) 2026
Yayasan Pendidikan Internal Audit (YPIA)

Conference Output: Rumusan dan Rekomendasi

PENDAHULUAN

Dengan menghaturkan puji syukur ke hadirat Tuhan Yang Maha Kuasa, Konferensi Auditor Internal (KAI) Tahun 2026 yang diselenggarakan oleh Yayasan Pendidikan Internal Audit (YPIA) pada tanggal 8–9 Juli 2026 di Yogyakarta telah berlangsung dengan baik melalui penyampaian *keynote speech, general session, panel discussion, one-on-one discussion*, serta pertukaran gagasan antara regulator, Dewan Komisaris, Direksi, Komite Audit, Auditor Internal, akademisi, praktisi, dan berbagai pemangku kepentingan.

Konferensi ini diselenggarakan pada saat dunia sedang mengalami perubahan yang sangat cepat akibat perkembangan Artificial Intelligence, transformasi digital, meningkatnya ancaman keamanan siber, fragmentasi geopolitik global, serta meningkatnya tuntutan terhadap transparansi, akuntabilitas, dan kualitas *governance* organisasi.

Peserta konferensi menyimpulkan bahwa tantangan terbesar organisasi pada masa depan bukan semata-mata bagaimana menguasai teknologi, melainkan bagaimana memastikan teknologi digunakan secara bertanggung jawab melalui *governance* yang baik, kepemimpinan yang berintegritas, serta pengambilan keputusan yang akuntabel. Oleh karena itu, peserta konferensi bersepakat bahwa kepercayaan (*trust*) harus menjadi tujuan utama *governance* organisasi pada era digital.

RUMUSAN HASIL KONFERENSI

Pertama
Perubahan Lingkungan Strategis Global

Peserta konferensi memahami bahwa *artificial intelligence*, digitalisasi, keamanan siber, perubahan geopolitik, perubahan model bisnis, serta meningkatnya ekspektasi masyarakat telah mengubah secara fundamental cara organisasi menciptakan nilai, mengelola risiko, mengambil keputusan, dan mempertanggungjawabkan kinerjanya kepada para pemangku kepentingan. Organisasi tidak lagi menghadapi perubahan yang bersifat bertahap, tetapi menghadapi perubahan yang berlangsung cepat, saling terhubung, dan makin rumit (kompleks).

Kedua

Paradigma Baru *Governance*

Peserta konferensi berpendapat bahwa *governance* organisasi harus berevolusi mengikuti perubahan tersebut. *Governance* tidak lagi cukup berorientasi pada kepatuhan terhadap peraturan, tetapi harus mampu memberikan wawasan strategis, mengantisipasi risiko masa depan, memperkuat kualitas pengambilan keputusan, serta menciptakan nilai yang berkelanjutan.

Transformasi digital bukan lagi sekadar proyek teknologi informasi, tetapi telah menjadi bagian integral dari strategi organisasi dan tanggung jawab Dewan Komisaris, Direksi, serta seluruh jajaran manajemen.

Ketiga

Implementasi *Global Standard*

Peserta konferensi meyakini bahwa peran Internal Audit makin strategis dalam mendukung keberhasilan organisasi. Sejalan dengan implementasi *Global Internal Audit Standards (GIAS)*, auditor internal tidak lagi hanya memberikan *assurance* atas kepatuhan, tetapi juga menghasilkan *insight*, *foresight*, dan *strategic advice* melalui *continuous auditing*, *continuous assurance*, pemanfaatan *advanced analytics*, serta penguatan *digital trust* dan *cyber resilience* untuk mendukung terwujudnya *Governance 5.0*.

Keempat

Etika sebagai Fondasi *Governance*

Peserta konferensi menegaskan bahwa kemajuan teknologi harus selalu diimbangi dengan penguatan etika, integritas, transparansi, akuntabilitas, independensi, dan penghormatan terhadap nilai-nilai kemanusiaan.

Artificial intelligence harus digunakan secara bertanggung jawab, dapat dipertanggungjawabkan, dapat diaudit, dan tetap menempatkan manusia sebagai pengambil keputusan akhir. Budaya integritas merupakan fondasi utama dalam membangun organisasi yang dipercaya.

Kelima

Transformasi Peran Dewan Komisaris, Direksi dan Internal Audit

Peserta konferensi meyakini bahwa Dewan Komisaris, Direksi, dan Internal Audit memiliki peran yang semakin strategis dalam menghadapi era digital.

Board dituntut memperkuat pengawasan terhadap *Artificial Intelligence*, keamanan siber, pengelolaan data, risiko strategis, dan keberlanjutan organisasi.

Internal Audit tidak lagi hanya memberikan *assurance* atas kepatuhan, tetapi berkembang menjadi mitra strategis yang memberikan ***assurance, insight, foresight*,** serta mendukung pengambilan keputusan melalui *continuous auditing, continuous assurance,* dan pemanfaatan teknologi digital.

Keenam

Kepemimpinan dan Pengambilan Keputusan

Peserta konferensi berpandangan bahwa kualitas *governance* sangat ditentukan oleh kualitas kepemimpinan dan kualitas pengambilan keputusan.

Penerapan prinsip *Business Judgment Rule*, didukung oleh informasi yang andal, *governance* yang baik, pengelolaan risiko yang efektif, serta integritas para pemimpin organisasi merupakan fondasi bagi terciptanya keputusan yang akuntabel, berorientasi jangka panjang,

dan mampu menciptakan nilai yang berkelanjutan. Peserta konferensi berpandangan bahwa dalam rangka memberikan kepastian hukum dan kepastian bisnis, **memandang perlu pembentukan lembaga independen atau Dewan/Badan *Advokasi* terkait *Business Judgment Rule*** yang berfungsi memberikan kajian, pendapat profesional, advokasi, dan penyelesaian sengketa sehingga tercipta keadilan bisnis, kepastian bagi pengambil keputusan yang beritikad baik, serta iklim investasi yang lebih kondusif.

Ketujuh

***Governance 5.0* sebagai Arah Baru *Governance* Indonesia**

Berdasarkan seluruh pembahasan yang berkembang selama konferensi, peserta bersepakat bahwa Indonesia perlu mengembangkan ***Governance 5.0***, yaitu paradigma *governance* yang: berpusat pada manusia (human-centered); memanfaatkan teknologi dan *artificial intelligence* secara bertanggung jawab; menjunjung tinggi etika, integritas, dan akuntabilitas; memperkuat pengawasan Dewan berbasis risiko, data, dan teknologi; memperkuat manajemen risiko, keamanan siber, dan *digital trust;* mengembangkan *continuous assurance*; memperkuat kolaborasi melalui *Three Lines Model*; menciptakan nilai jangka panjang; meningkatkan daya saing organisasi dan bangsa; membangun kepercayaan publik sebagai fondasi keberlanjutan.

REKOMENDASI KONFERENSI

Konferensi Auditor Internal Tahun 2026 merekomendasikan kepada seluruh pemangku kepentingan untuk:

1. Pemerintah Republik Indonesia

Mengembangkan ***National Governance 5.0 Framework*** sebagai arah transformasi *governance* sektor publik dan dunia usaha Indonesia.

2. Regulator

Menyusun kebijakan yang memperkuat *AI Governance, Cyber Governance, Data Governance*, dan *Digital Trust*, sekaligus memberikan kepastian hukum terhadap pengambilan keputusan yang dilakukan dengan itikad baik.

3. Dewan Komisaris, Direksi, dan Komite Audit

Memperkuat kapasitas *Board Oversight* terhadap *Artificial Intelligence*, keamanan siber, risiko strategis, pengelolaan data, dan keberlanjutan organisasi.

4. Dunia Usaha

Menjadikan *governance* organisasi, inovasi, budaya integritas, dan transformasi digital sebagai satu kesatuan strategi untuk meningkatkan daya saing organisasi.

5. Internal Audit

Mereposisi fungsi Internal Audit sebagai mitra strategis organisasi melalui pengembangan kompetensi *Artificial Intelligence, data analytics, cyber assurance, continuous assurance,* dan *strategic foresight*.

6. Perguruan Tinggi dan Asosiasi Profesi

Mengembangkan kurikulum, penelitian, sertifikasi, dan pendidikan berkelanjutan yang mendukung lahirnya pemimpin dan Auditor Internal yang siap menghadapi era *Governance 5.0*.

7. Seluruh Pemangku Kepentingan

Memperkuat kolaborasi lintas profesi dan lintas sektor untuk membangun ekosistem *governance* Indonesia yang adaptif, berintegritas, inovatif, dan dipercaya masyarakat.

PENUTUP

Konferensi Auditor Internal Tahun 2026 meyakini bahwa keberhasilan organisasi pada era *artificial intelligence* tidak lagi hanya ditentukan oleh kecanggihan teknologi yang dimiliki, tetapi oleh kemampuan organisasi membangun kepercayaan melalui *governance* yang baik, kepemimpinan yang berintegritas, pengambilan keputusan yang bertanggung jawab, serta budaya organisasi yang menjunjung tinggi etika.

Dengan semangat kolaborasi seluruh pemangku kepentingan, Konferensi Auditor Internal Tahun 2026 mengajak seluruh organisasi di Indonesia menjadikan ***Governance 5.0*** sebagai arah transformasi menuju organisasi yang adaptif, tangguh, berdaya saing, dan dipercaya.

Rumusan dan Rekomendasi ini menjadi dasar bagi setiap pemangku kepentingan untuk menindak lanjuti dan diharapkan menjadi referensi bagi Pemerintah, regulator, dunia usaha, perguruan tinggi, asosiasi profesi, serta seluruh organisasi dalam memperkuat praktik *governance* Indonesia di era digital.

PERNYATAAN KONFERENSI

"Kami meyakini bahwa teknologi tanpa *governance* akan meningkatkan risiko. *Governance* tanpa etika akan kehilangan kepercayaan. Dan kepercayaan adalah fondasi utama keberlanjutan organisasi. Oleh karena itu, kami berkomitmen mendorong *Governance 5.0* sebagai paradigma baru *governance* Indonesia di era *artificial intelligence* demi terwujudnya organisasi yang berintegritas, berdaya saing, dan dipercaya."

Yogyakarta, 9 Juli 2026

Atas nama Peserta Konferensi Auditor Internal (KAI) 2026

PRESS RELEASE KAI 2026

KONFERENSI AUDITOR INTERNAL (KAI) 2026

Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era

Yogyakarta, 8-9 Juli 2026

Konferensi Auditor Internal 2026 Serukan Transformasi *Governance* Menuju Organisasi yang Berintegritas dan Dipercaya di Era *Artificial Intelligence*

Yogyakarta, 9 Juli 2026

Konferensi Auditor Internal (KAI) Tahun 2026 yang diselenggarakan oleh **Yayasan Pendidikan Internal Audit (YPIA)** pada tanggal **8–9 Juli 2026** di Yogyakarta telah menghasilkan kesepahaman bersama mengenai arah baru *governance* organisasi Indonesia dalam menghadapi era ***artificial intelligence* (AI), transformasi digital, meningkatnya ancaman keamanan siber, serta dinamika geopolitik global**.

Konferensi yang mengangkat tema **"*Governance 5.0: Redefining Board Oversight and Internal Audit in a Digital-First Era*"** dihadiri oleh pimpinan organisasi, Dewan Komisaris, Direksi, Komite Audit, Auditor Internal, regulator, akademisi, praktisi *governance*, manajemen risiko, serta pakar teknologi dari berbagai sektor.

Setelah mengikuti seluruh rangkaian keynote speech, general session, panel discussion, dan forum diskusi, peserta konferensi menyimpulkan bahwa **tantangan terbesar organisasi pada masa depan bukan semata-mata bagaimana menguasai teknologi, tetapi bagaimana memastikan teknologi digunakan secara bertanggung jawab melalui *governance* yang baik, kepemimpinan yang berintegritas, dan pengambilan keputusan yang akuntabel.**

Peserta konferensi menegaskan bahwa **kepercayaan (*trust*)** merupakan aset strategis yang akan menentukan keberhasilan dan keberlanjutan organisasi pada era digital. Oleh karena itu, transformasi digital harus berjalan seiring dengan penguatan *governance*, etika, integritas, manajemen risiko, keamanan siber, serta pengawasan yang efektif.

Sebagai hasil konferensi, peserta memperkenalkan konsep ***Governance 5.0***, yaitu paradigma *governance* yang mengintegrasikan kepemimpinan yang visioner, pemanfaatan *Artificial Intelligence* secara bertanggung jawab, pengelolaan risiko yang adaptif, keamanan siber yang tangguh, budaya integritas yang kuat, serta fungsi Internal Audit yang mampu memberikan ***assurance, insight, foresight*, dan *strategic advice*** bagi organisasi.

Konferensi juga menegaskan bahwa perkembangan *Artificial Intelligence* harus selalu berada dalam kendali manusia (*human-centered governance*). Pemanfaatan teknologi harus dilaksanakan secara transparan, dapat dipertanggungjawabkan, dapat diaudit, serta menjunjung tinggi etika dan kepentingan publik.

Dalam bidang *governance* korporasi, peserta konferensi menilai bahwa peran Dewan Komisaris, Direksi, Komite Audit, dan Internal Audit perlu terus diperkuat agar mampu mengantisipasi berbagai risiko baru, termasuk risiko Artificial Intelligence, keamanan siber, pengelolaan data, serta dinamika geopolitik global. Internal Audit dipandang tidak lagi hanya berfungsi sebagai pemberi assurance atas kepatuhan, tetapi berkembang menjadi mitra strategis organisasi dalam mendukung kualitas pengambilan keputusan dan penciptaan nilai jangka panjang.

Konferensi juga menekankan bahwa kualitas *governance* merupakan salah satu faktor utama dalam meningkatkan daya saing organisasi maupun daya saing bangsa. Organisasi yang mampu mengintegrasikan inovasi, *governance* yang baik, budaya integritas, dan kepemimpinan yang bertanggung jawab akan lebih siap menghadapi perubahan serta memperoleh kepercayaan dari masyarakat, investor, regulator, dan seluruh pemangku kepentingan.

Sebagai penutup, peserta menyepakati Kesepakatan Yogyakarta 2026 yang memuat komitmen bersama untuk mendorong terwujudnya organisasi Indonesia yang: berintegritas dan menjunjung tinggi etika; adaptif terhadap perkembangan teknologi; bertanggung jawab dalam pemanfaatan Artificial Intelligence; tangguh menghadapi ancaman keamanan siber; memperkuat kualitas kepemimpinan dan pengambilan keputusan; membangun kepercayaan publik melalui *governance* yang baik.

Konferensi juga menyampaikan rekomendasi kepada Pemerintah, regulator, dunia usaha, BUMN, perguruan tinggi, dan asosiasi profesi agar bersama-sama mempercepat pengembangan *Governance 5.0*, memperkuat *AI Governance, Cyber Governance, Ethical Governance*, serta meningkatkan kompetensi kepemimpinan dan profesi Auditor Internal dalam menghadapi tantangan masa depan.

Peserta konferensi berpandangan penerapan prinsip *Business Judgment Rule*, yang didukung informasi yang andal, *governance* yang baik, pengelolaan risiko yang efektif, serta integritas para pemimpin organisasi, merupakan fondasi bagi terciptanya keputusan yang akuntabel, berorientasi jangka panjang, dan mampu menciptakan nilai yang berkelanjutan. Dalam rangka memberikan kepastian hukum dan kepastian bisnis, peserta konferensi juga memandang perlunya pembentukan lembaga independen atau Dewan/Badan Advokasi terkait *Business Judgment Rule* yang berfungsi memberikan kajian, pendapat profesional, advokasi, dan penyelesaian sengketa sehingga tercipta keadilan bisnis, kepastian bagi pengambil keputusan yang beritikad baik, serta iklim investasi yang lebih kondusif.

Melalui hasil konferensi ini, Yayasan Pendidikan Internal Audit berharap dapat memberikan kontribusi nyata dalam memperkuat *governance* organisasi Indonesia sehingga makin adaptif, berintegritas, inovatif, berdaya saing, dan dipercaya oleh seluruh pemangku kepentingan.

Pernyataan Konferensi

"Teknologi akan terus berkembang, namun kepercayaan tetap menjadi fondasi utama keberhasilan organisasi. *Artificial Intelligence* memerlukan *governance*, *governance* memerlukan integritas, dan integritas akan melahirkan kepercayaan. Itulah esensi *Governance 5.0*."

Yogyakarta, 9 Juli 2026
Panitia Konferensi Auditor Internal (KAI) 2026
Yayasan Pendidikan Internal Audit (YPIA)

SUPPLEMENTARY DOCUMENT

KEYNOTE SPEECH

Global Governance Trends and Indonesia's Readiness in a Digital-First Era

Gita Wirjawan, MPA., MBA., CPA., CFA
Menteri Perdagangan Republik Indonesia (2011-2014)

ABSTRAK

Perkembangan kecerdasan artifisial (*Artificial Intelligence/AI*) telah mengubah lanskap ekonomi, geopolitik, tata kelola, dan daya saing global secara fundamental. AI tidak lagi dipandang sebagai sekadar inovasi teknologi, melainkan sebagai infrastruktur strategis yang menentukan produktivitas, kapasitas inovasi, ketahanan nasional, serta posisi suatu negara dalam rantai nilai global. Di tengah perubahan tersebut, Indonesia menghadapi tantangan besar untuk bertransformasi dari sekadar pengguna (*technology adopter*) menjadi pemangku kepentingan (*stakeholder*) yang mampu berkontribusi dalam pembentukan arah perkembangan AI global. Namun demikian, kesiapan tersebut masih menghadapi berbagai keterbatasan, antara lain kapasitas energi listrik, ruang fiskal, investasi, kualitas sumber daya manusia, serta kemampuan menghasilkan inovasi berbasis ilmu pengetahuan dan teknologi. Materi keynote ini menyoroti berbagai tren global yang membentuk era *Digital-First*, termasuk meningkatnya kebutuhan komputasi akibat AI generatif, pentingnya pembangunan infrastruktur energi, dinamika investasi asing, pilihan model pengembangan AI *open-source* dan *closed-source*, serta urgensi penguatan pendidikan tinggi dan kemampuan *critical thinking*. Seluruh faktor tersebut dipandang sebagai prasyarat bagi terciptanya ekosistem AI nasional yang berkelanjutan. Dalam konteks tata kelola, keberhasilan transformasi digital tidak hanya ditentukan oleh adopsi teknologi, tetapi juga oleh kualitas kepemimpinan, arah kebijakan publik, kapasitas institusi, dan kemampuan mengelola risiko strategis.

Kata Kunci: A*rtificial Intelligence, Digital-First Era, Global Governance*

PEMBAHASAN

Perkembangan *Artificial Intelligence* (AI) telah mengubah paradigma pembangunan global dari ekonomi berbasis sumber daya menuju ekonomi berbasis pengetahuan, komputasi, dan data. AI tidak lagi diposisikan sebagai sekadar teknologi pendukung, melainkan sebagai infrastruktur strategis yang menentukan produktivitas, inovasi, daya saing industri, serta posisi geopolitik suatu negara. Negara-negara yang mampu mengembangkan ekosistem AI secara mandiri akan memiliki keunggulan dalam menciptakan nilai tambah ekonomi sekaligus memengaruhi arah perkembangan teknologi dunia. Sebaliknya, negara yang hanya berperan sebagai pengguna teknologi akan semakin bergantung pada inovasi yang dihasilkan pihak lain. Oleh karena itu, tantangan utama Indonesia pada era *Digital-First* bukan hanya mempercepat adopsi teknologi digital, tetapi juga membangun kapasitas nasional agar mampu menjadi bagian dari pembentukan ekosistem AI global. Upaya tersebut memerlukan

sinergi antara pembangunan infrastruktur, penguatan kapasitas ekonomi, peningkatan kualitas sumber daya manusia, serta tata kelola yang adaptif sehingga Indonesia dapat bertransformasi dari *technology adopter* menjadi *technology stakeholder*.

Percepatan perkembangan AI tidak dapat dilepaskan dari meningkatnya kebutuhan komputasi dan pemanfaatan data dalam skala yang sangat besar. Volume data global terus mengalami pertumbuhan eksponensial seiring berkembangnya media sosial, *cloud computing*, layanan digital, hingga lahirnya AI generatif. Peningkatan tersebut menyebabkan kebutuhan komputasi meningkat secara signifikan, bahkan sebuah permintaan pada *ChatGPT* memerlukan daya komputasi sekitar sepuluh kali lebih besar dibandingkan pencarian melalui mesin pencari konvensional. Kebutuhan tersebut meningkat lebih tinggi lagi pada AI pengolah gambar maupun video yang memerlukan kapasitas komputasi jauh lebih besar. Fenomena ini menunjukkan bahwa perkembangan AI tidak hanya ditentukan oleh kualitas algoritma, tetapi juga oleh ketersediaan pusat data, prosesor berperforma tinggi, jaringan digital, dan kemampuan pemrosesan data secara berkelanjutan. Dengan demikian, kemampuan membangun infrastruktur komputasi menjadi salah satu indikator kesiapan suatu negara dalam memasuki era AI.

Besarnya kebutuhan komputasi tersebut secara langsung meningkatkan kebutuhan energi listrik sebagai fondasi utama transformasi digital. Tingkat konsumsi listrik per kapita menunjukkan hubungan yang erat dengan tingkat modernitas suatu negara karena hampir seluruh aktivitas ekonomi digital bergantung pada pasokan energi yang stabil. Negara-negara dengan tingkat konsumsi listrik tinggi memiliki kapasitas yang lebih besar dalam mengembangkan industri digital, pusat data, maupun teknologi AI. Sebaliknya, negara dengan kapasitas energi yang terbatas akan menghadapi kendala dalam membangun ekosistem digital yang kompetitif. Selain tingkat konsumsi listrik, kemampuan meningkatkan kapasitas pembangkit listrik setiap tahun juga menjadi faktor penting dalam mendukung kebutuhan komputasi yang terus meningkat. Oleh sebab itu, pembangunan infrastruktur ketenagalistrikan tidak lagi dipandang semata sebagai pembangunan sektor energi, melainkan sebagai investasi strategis yang menentukan keberhasilan transformasi digital dan pengembangan AI pada masa mendatang.

Kesiapan suatu negara dalam membangun ekosistem AI juga dipengaruhi oleh kapasitas ekonominya. Ruang ekonomi (*economic space*) yang tercermin melalui *tax ratio*, rasio jumlah uang beredar terhadap produk domestik bruto (*M2 to GDP*), serta kemampuan menarik *Foreign Direct Investment* (FDI) menentukan besarnya kapasitas pembiayaan pembangunan jangka panjang. Perbandingan berbagai negara di Asia Tenggara menunjukkan bahwa investasi, stabilitas ekonomi, dan kemampuan fiskal menjadi faktor yang mendukung

pembangunan infrastruktur digital, penelitian, inovasi, dan pengembangan teknologi. Semakin besar kemampuan suatu negara menyediakan ruang fiskal dan menarik investasi, semakin besar pula peluang untuk membangun ekosistem AI yang berkelanjutan. Oleh karena itu, pembangunan ekonomi dan transformasi digital merupakan dua agenda yang saling berkaitan dan harus dikembangkan secara simultan agar mampu menghasilkan daya saing yang berkelanjutan.

Pengembangan AI juga dipengaruhi oleh model inovasi yang diterapkan. Pendekatan *open-source* memungkinkan kolaborasi yang lebih luas melalui keterbukaan kode sumber sehingga mendorong percepatan inovasi, pertukaran pengetahuan, dan partisipasi berbagai pihak dalam pengembangan teknologi. Sebaliknya, pendekatan *closed-source* menitikberatkan pada pengembangan teknologi secara tertutup dengan orientasi komersial dan perlindungan terhadap kepemilikan intelektual. Kedua pendekatan tersebut menunjukkan bahwa keberhasilan AI tidak hanya bergantung pada kemampuan teknis, tetapi juga pada strategi pengembangan, model kolaborasi, dan tata kelola inovasi yang diterapkan. Pemilihan pendekatan yang tepat akan memengaruhi kecepatan inovasi, daya saing industri, serta kemampuan suatu negara dalam membangun kemandirian teknologi pada masa depan. Di balik perkembangan teknologi yang semakin pesat, kualitas manusia tetap menjadi faktor penentu keberhasilan transformasi digital. AI memiliki kemampuan menghasilkan informasi secara cepat, namun tidak selalu menghasilkan keluaran yang akurat karena dapat mengalami *hallucination*, yaitu menghasilkan informasi yang tampak meyakinkan tetapi tidak sepenuhnya sesuai dengan fakta. Selain itu, keluaran AI juga dipengaruhi oleh kualitas data pelatihan yang digunakan sehingga berpotensi menghasilkan bias maupun kecenderungan tertentu. Kondisi tersebut menunjukkan bahwa pemanfaatan AI tidak dapat menggantikan kemampuan manusia dalam melakukan analisis, penalaran, dan pengambilan keputusan. Oleh karena itu, kemampuan *critical thinking* menjadi kompetensi yang semakin penting agar pengguna mampu mengevaluasi informasi secara objektif, melakukan verifikasi, serta memanfaatkan AI secara bertanggung jawab dalam mendukung proses pengambilan keputusan.

Pentingnya *critical thinking* berkaitan erat dengan kualitas sistem pendidikan dan pengembangan sumber daya manusia. Tingkat pendidikan tinggi (*tertiary education attainment*) menjadi salah satu indikator kesiapan suatu negara dalam menghasilkan tenaga kerja yang mampu beradaptasi terhadap perkembangan teknologi. Di sisi lain, kualitas tenaga pendidik juga menentukan kemampuan menghasilkan lulusan yang memiliki kompetensi riset, inovasi, dan penguasaan teknologi. Oleh karena itu, investasi pada sektor pendidikan harus dipandang sebagai investasi strategis yang akan menentukan kemampuan suatu negara membangun ekosistem AI secara berkelanjutan. Pengembangan teknologi tanpa diikuti

peningkatan kualitas pendidikan berpotensi menciptakan ketergantungan terhadap inovasi dari negara lain, sedangkan pembangunan sumber daya manusia yang unggul akan memperkuat kapasitas nasional dalam menghasilkan inovasi dan membangun daya saing global.

Perkembangan *Artificial Intelligence* tidak mengurangi pentingnya pendidikan, tetapi justru semakin menegaskan peran *critical thinking* sebagai kompetensi utama pada era digital. Model *large language models* dapat menghasilkan *hallucination*, yaitu keluaran yang tampak logis dan meyakinkan, tetapi tidak selalu didasarkan pada fakta atau informasi yang akurat. Selain itu, respons yang dihasilkan AI juga dipengaruhi oleh data yang digunakan selama proses pelatihan sehingga berpotensi mencerminkan bias atau kecenderungan tertentu, termasuk preferensi terhadap *political correctness* dibandingkan penyajian kebenaran yang sepenuhnya objektif. Kondisi tersebut menunjukkan bahwa AI tidak dapat dijadikan satu-satunya sumber pengambilan keputusan, melainkan harus didukung oleh kemampuan manusia untuk melakukan verifikasi, mengevaluasi kredibilitas informasi, serta menganalisis berbagai perspektif secara kritis. Oleh karena itu, penguatan sistem pendidikan yang mampu membentuk kemampuan berpikir analitis, penalaran logis, dan literasi digital menjadi prasyarat penting agar pemanfaatan AI dapat memberikan manfaat yang optimal sekaligus meminimalkan risiko kesalahan informasi dan pengambilan keputusan.

Kesiapan Indonesia memasuki era *Digital-First* pada akhirnya ditentukan oleh kemampuan mengintegrasikan seluruh prasyarat tersebut ke dalam strategi pembangunan nasional. AI bukan hanya persoalan teknologi, melainkan perpaduan antara kapasitas komputasi, ketersediaan energi, kekuatan ekonomi, investasi, model inovasi, kualitas pendidikan, dan kemampuan berpikir kritis masyarakat. Seluruh komponen tersebut saling melengkapi dalam membentuk ekosistem yang mampu menghasilkan inovasi secara berkelanjutan. Oleh karena itu, transformasi digital memerlukan kebijakan yang terintegrasi, investasi jangka panjang, serta kolaborasi antara pemerintah, dunia usaha, akademisi, dan masyarakat agar Indonesia tidak hanya menjadi pengguna teknologi, tetapi mampu mengambil peran sebagai salah satu aktor yang berkontribusi dalam membentuk perkembangan AI dan ekonomi digital global.

SESI TANYA JAWAB

Pertanyaan 1 (Ibu Endang dari PT Kawasan Industri Medan)

Seberapa besar optimisme Bapak terhadap peluang Indonesia untuk menjadi *stakeholder* dalam perkembangan *Artificial Intelligence* (AI) global, bukan hanya sebagai pengguna teknologi?

Jawaban:

Optimisme harus disertai dengan kesadaran bahwa tantangannya yang dihadapi Indonesia tidak ringan. Saat ini dunia bergerak menuju tatanan geopolitik yang semakin multipolar, di mana pusat kekuatan ekonomi, teknologi, dan politik tidak lagi didominasi oleh satu atau dua negara. Kondisi tersebut membuat kerja sama multilateral menjadi semakin kompleks karena setiap negara memiliki kepentingan strategis masing-masing, terutama dalam penguasaan teknologi AI. Dalam situasi seperti ini, Indonesia tidak dapat hanya menunggu perkembangan yang terjadi di negara lain, tetapi harus membangun kapasitasnya sendiri melalui penguatan sumber daya manusia, pendidikan, infrastruktur, investasi, dan ekosistem inovasi. Apabila fondasi tersebut dapat dibangun secara konsisten, Indonesia memiliki peluang untuk menjadi salah satu pemangku kepentingan dalam perkembangan AI global.

Pertanyaan 2: Sumaryo (Bank DKI)

Salah satu syarat daya dukung AI adala electricity & energy yang mana salah satu sumbernya. Salah satu prasyarat utama pengembangan AI adalah ketersediaan energi listrik dalam jumlah besar. Mengingat Indonesia masih banyak mengandalkan batu bara sebagai sumber energi, apakah kebutuhan energi tersebut dapat terpenuhi? Bagaimana pandangan Bapak mengenai pemanfaatan energi nuklir sebagai salah satu alternatif?

Jawaban:

Menurut saya, fokus utamanya bukan terletak pada apakah sumber energinya berasal dari batu bara, nuklir, atau energi alternatif lainnya, melainkan pada kemampuan menyediakan pasokan energi yang memadai, andal, dan berkelanjutan. Saat ini perkembangan energi terbarukan berlangsung sangat pesat. Selain peningkatan pemanfaatan tenaga surya, perkembangan teknologi **penyimpanan energi (*energy storage*)**, khususnya baterai, juga mengalami kemajuan yang signifikan dengan biaya yang terus menurun. Ketika biaya pembangkitan listrik dari energi terbarukan dan biaya penyimpanannya semakin kompetitif, akan tercipta **paritas ekonomi**, sehingga transisi menuju energi yang lebih bersih akan terjadi secara alami karena lebih menguntungkan secara bisnis. Dalam kondisi tersebut, pelaku usaha, termasuk industri yang selama ini bergantung pada batu bara, akan memiliki insentif ekonomi untuk beralih ke sumber energi yang lebih efisien dan berkelanjutan. Adapun energi nuklir dapat menjadi salah satu alternatif yang dapat dipertimbangkan, selama didukung oleh kesiapan teknologi, aspek keselamatan, regulasi, dan penerimaan masyarakat sebagai bagian dari bauran energi nasional.

GENERAL SESSION 1

Redefining Governance in the Age of Agentic AI: Oversight Beyond Human Decision-Making

Prof. Dr. Ir. Hammam Riza, MSc., IPU
Ketua Umum Kolaborasi Riset dan Inovasi Industri Kecerdasan Artifisial (KORIKA)
dan Ketua Umum Ikatan Auditor Teknologi Indonesia (IATI)

ABSTRAK

Penggunaan *Artificial Intelligence* (AI) bukan lagi sesuatu yang akan dimulai pada masa depan, melainkan telah menjadi kebutuhan sehari-hari karena organisasi saat ini telah memanfaatkan AI dalam berbagai aktivitas bisnis. Namun, penggunaan AI juga menimbulkan berbagai risiko yang harus dimitigasi melalui tata kelola yang memadai. Kemampuan prediktif yang dimiliki *Agentic AI* memungkinkan sistem menyelesaikan tugas secara lebih cepat dan otonom. Meskipun demikian, organisasi tetap harus memastikan bahwa data yang dihasilkan akurat, bebas dari bias, serta memiliki mekanisme pengendalian terhadap kolaborasi antarsistem (*agent-to-agent collaboration*). Oleh karena itu, tata kelola (*governance*) perlu bertransformasi seiring berkembangnya kapabilitas *Agentic AI*. Semakin cerdas AI, semakin tinggi pula kebutuhan untuk mengendalikannya. AI bahkan mampu menghasilkan *coding* menggunakan bahasa alami (*natural language*) sehingga berperan sebagai orkestrator atas data yang dimiliki organisasi. Dalam konteks tersebut, audit akan berkembang menjadi *continuous auditing* karena *Agentic AI* bekerja secara berkelanjutan. Namun demikian, organisasi tetap harus menetapkan secara jelas pihak yang memiliki kewenangan mengambil keputusan, apakah manusia atau AI. Apa pun teknologi yang digunakan, keandalan data harus tetap menjadi prioritas utama sehingga hasil yang dihasilkan *Agentic AI* dapat dipercaya. *AI Governance* menekankan pentingnya pengembangan AI yang bertanggung jawab dan berdaulat. Organisasi tidak cukup hanya menjadi pengguna AI, tetapi perlu membangun kapasitas sebagai kreator yang mampu mengembangkan AI sesuai kebutuhan organisasi. Tata kelola AI harus dibangun melalui regulasi, pengelolaan data yang berdaulat, serta mekanisme pengendalian yang memadai. AI tidak menggantikan auditor, tetapi auditor harus memastikan bahwa algoritma yang digunakan telah memiliki *assurance* yang memadai sehingga menghasilkan data dan keputusan yang akurat, dapat dipercaya, dan sesuai dengan prinsip tata kelola yang baik.

Kata kunci: *No Governance, No Trust, No Adaptation*

PEMBAHASAN

Pengertian umum *AI Governance* adalah kerangka kerja berupa kebijakan, prosedur, dan standar etika yang dirancang untuk memastikan bahwa sistem *Artificial Intelligence* (AI) dikembangkan, diterapkan, dan dioperasikan secara aman, adil, transparan, serta mematuhi regulasi yang berlaku. *Agentic AI* merupakan sistem kecerdasan buatan otonom yang tidak sekadar merespons perintah, tetapi juga mampu menetapkan tujuan, menyusun rencana

langkah demi langkah, serta mengambil tindakan secara proaktif untuk menyelesaikan tugas-tugas kompleks dengan intervensi manusia yang minimal.
Berbeda dengan AI generatif (*Generative AI*) yang berfokus menghasilkan konten atau Jawaban:, *Agentic AI* mampu merencanakan, mengambil keputusan, mengeksekusi tindakan, berkolaborasi dengan agen lain, serta terus belajar secara mandiri dengan keterlibatan manusia yang semakin terbatas.

Tantangan utama pada masa depan bukan lagi membangun AI yang semakin cerdas, melainkan membangun tata kelola yang mampu mengendalikan AI secara efektif. Teknologi ini memiliki dampak yang sangat besar terhadap organisasi sehingga berpotensi menimbulkan risiko reputasi, kerugian finansial, maupun konsekuensi hukum apabila diimplementasikan tanpa mekanisme pengendalian yang memadai. AI tidak lagi sekadar menjadi alat otomatisasi, tetapi merupakan sistem yang belajar dari data dan menghasilkan keputusan yang dapat memengaruhi kehidupan manusia secara langsung.

Perjalanan tata kelola AI mengalami evolusi yang signifikan. Pada tahun 2015, AI berfungsi sebagai *AI tools* yang membantu manusia dalam melakukan analisis dan otomatisasi. Tahun 2022 ditandai dengan berkembangnya *Generative AI* yang mampu menghasilkan konten, rekomendasi, dan *insight*. Memasuki tahun 2025, *Agentic AI* berkembang dengan kemampuan *plan, decide, execute, learn,* dan *collaborate autonomously*. Selanjutnya, pada tahun 2030 diproyeksikan akan berkembang menuju *autonomous organization*, yaitu organisasi yang digerakkan oleh AI dengan *human oversight* sebagai pengendali strategis.
Paradigma tata kelola tradisional (*traditional governance*) dinilai tidak lagi sepenuhnya efektif karena seluruh proses masih berpusat pada manusia. Pengambilan keputusan dilakukan berdasarkan informasi yang tersedia, pelaksanaan aktivitas dijalankan oleh manusia dan sistem, sedangkan audit baru dilakukan setelah suatu kejadian berlangsung (*post-event audit*). Sebaliknya, paradigma tata kelola baru (*new governance paradigm*) mengintegrasikan manusia dan AI dalam seluruh proses organisasi. AI berperan dalam mendukung pengambilan keputusan, pelaksanaan, evaluasi, dan optimalisasi proses, sedangkan manusia tetap menjalankan fungsi *human oversight* dengan menetapkan arah, melakukan pengawasan, menjaga nilai-nilai organisasi, dan memastikan akuntabilitas.
Empat tantangan utama dalam *AI Governance* meliputi:

1. ***Accountability***, yaitu siapa yang bertanggung jawab ketika keputusan diambil oleh AI. PertanggungJawaban: dapat melibatkan pengembang, operator, maupun organisasi, sementara kerangka akuntabilitasnya masih terus berkembang.

2. ***Explainability***, yaitu kemampuan menjelaskan alasan AI menghasilkan suatu keputusan. Tantangan utama berasal dari fenomena *black box*, kompleksitas model AI, serta kebutuhan akan AI yang dapat diinterpretasikan dan dijelaskan.
3. ***Transparency***, yaitu kemampuan untuk memahami proses kerja AI melalui transparansi algoritma, *data lineage*, ketertelusuran data, serta *auditability*.
4. ***Risk Management***, yaitu pengelolaan risiko apabila AI menghasilkan keputusan yang keliru, termasuk risiko *bias*, *fairness*, *safety*, *security*, *unintended consequences*, dan *systemic risk*.

Dengan berkembangnya *Agentic AI*, organisasi akan memiliki *personal assistant* digital yang mampu melaksanakan berbagai tugas secara cepat dan mandiri. Namun demikian, semakin cerdas AI, semakin tinggi pula tuntutan agar manusia mampu mengendalikannya secara bertanggung jawab. Audit akan berkembang menjadi lebih *seamless* melalui penerapan *continuous auditing* yang didukung *Agentic AI*. Meskipun demikian, AI tetap harus berpusat pada manusia (*human-centered AI*) dengan memastikan bahwa algoritma telah memenuhi prinsip *compliance*, *trustworthiness*, dan tata kelola yang baik sehingga organisasi siap memasuki era *Governance 5.0*.

SESI TANYA JAWAB (Q&A)

Pertanyaan 1 (Bapak Mushaf dari PT PLN Persero):

Dalam pengembangan *Agentic AI*, bagaimana menyikapi tantangan terkait teknologinya? Dari sisi kemampuan individu, kompetensi sudah cukup memadai dan berbagai aplikasi dapat dipelajari. Namun, pada tahap pengujian (*testing*), dibutuhkan kapasitas komputasi yang tinggi sehingga *response time* menjadi cukup lama. Apakah organisasi harus berinvestasi membangun infrastruktur sendiri atau terdapat bentuk kolaborasi tertentu sehingga kebutuhan komputasi tersebut dapat dipenuhi?

Jawaban:

Membangun AI bukanlah sesuatu yang dapat dilakukan begitu saja. AI merupakan salah satu *emerging technology* sehingga organisasi perlu memahami seluruh siklus (*lifecycle*) AI, memahami proses bisnis, serta memastikan *business alignment*. Organisasi tidak harus langsung membangun *data center* atau membeli *server* berkapasitas besar. Terdapat tahapan-tahapan yang perlu dilakukan, termasuk pemanfaatan *regulatory sandbox*, sehingga organisasi dapat memahami kebutuhan AI berdasarkan proses bisnis yang benar-benar ingin diselesaikan. Tidak semua proses bisnis harus langsung menggunakan AI. Organisasi perlu terlebih dahulu mengidentifikasi permasalahan yang ingin diselesaikan, kemudian membangun algoritma yang sesuai. Selanjutnya dilakukan proses ekstraksi data, pemilihan

data yang relevan, hingga pembangunan *AI model* yang sesuai dengan kebutuhan organisasi. Prinsip *Data is the new oil* menunjukkan bahwa data merupakan aset utama, sedangkan algoritma merupakan mesin yang mengolah nilai dari data tersebut. Oleh karena itu, *AI Governance* harus menjadi bagian yang tidak terpisahkan dari tata kelola perusahaan, termasuk melalui penerapan *regulatory sandbox*.

Pertanyaan 2 (Bapak Givary dari PT Hutama Karya):
Dalam praktiknya, organisasi sering kali terjebak pada semangat inovasi sehingga hanya mengikuti tren penggunaan AI tanpa memastikan kesiapan *governance*. Kondisi tersebut berpotensi menghasilkan *destructive intelligence*. Bagaimana langkah yang tepat agar organisasi tetap inovatif, tetapi sejalan dengan penerapan *AI Governance*?

Jawaban:
Inovasi harus mampu menciptakan nilai (*value creation*). Untuk menghasilkan nilai tersebut, tata kelola harus dibangun sejak tahap awal pengembangan AI. Organisasi perlu memastikan bahwa *security by design*, pengendalian, dan integrasi sistem telah dirancang secara terpadu, bukan sebagai proses yang berjalan sendiri-sendiri. Selain itu, organisasi tidak perlu menunggu regulasi yang lengkap karena AI telah memiliki berbagai prinsip *Trustworthy AI* yang dapat dijadikan pedoman dalam pengembangannya.

AI tidak dirancang untuk menggantikan manusia, melainkan untuk mendukung manusia dalam menghasilkan keputusan yang lebih baik. Oleh karena itu, pendekatan *human-centered AI* harus menjadi landasan utama pengembangan AI, dengan memastikan bahwa AI bersifat *responsible*, akuntabel, serta tetap memberikan ruang bagi *human oversight* dalam setiap keputusan yang bersifat penting dan strategis.

PANEL DISCUSSION - 1

Navigating Strategic Risk in a Fragmented Geopolitical and Economic Landscape

Ir. Laksamana Sukardi
Ekonom dan Menteri BUMN (1999-2004)

Aisha Rasyidila Kusumasomantri, S.Sos., M.Sc.
Director of Cooperation and External Affairs, Indo Pacific Strategic Intelligence

ABSTRAK

Lanskap geopolitik global sedang mengalami perubahan yang sangat mendasar. Dunia tidak lagi berada dalam era globalisasi yang relatif stabil, melainkan memasuki era fragmentasi geopolitik yang ditandai oleh meningkatnya rivalitas antarnegara, perang dagang, kompetisi teknologi, restrukturisasi rantai pasok global, serta berkembangnya tatanan dunia multipolar. Perubahan tersebut menyebabkan sumber risiko organisasi bergeser dari faktor-faktor internal menuju faktor eksternal yang semakin sulit diprediksi. Risiko geopolitik bukan lagi isu hubungan internasional semata, tetapi telah menjadi risiko bisnis dan risiko strategis yang secara langsung memengaruhi investasi, pembiayaan, rantai pasok, reputasi, hingga keberlangsungan organisasi. Oleh karena itu, Dewan Komisaris, Direksi, dan Auditor Internal dituntut untuk mengubah paradigma tata kelola dari pendekatan yang reaktif menjadi prediktif, adaptif, dan berbasis intelijen risiko. Governance 5.0 menjadi kerangka baru yang mengintegrasikan *foresight, scenario planning, continuous risk intelligence*, dan *adaptive decision making* agar organisasi memiliki ketahanan menghadapi ketidakpastian global.

Kata Kunci: *Geopolitik, Governance 5.0, Strategic Risk*

PEMBAHASAN

Dunia telah mengalami perubahan struktural yang tidak lagi bersifat sementara. Jika sebelumnya globalisasi mendorong integrasi ekonomi, kini dunia bergerak menuju fragmentasi yang ditandai oleh meningkatnya rivalitas geopolitik, perang dagang, persaingan teknologi, restrukturisasi rantai pasok, ketahanan energi dan pangan, serta penggunaan sanksi ekonomi sebagai instrumen politik.

Perubahan tersebut merupakan *regime change*, bukan sekadar siklus ekonomi. Perdagangan internasional masih tumbuh, tetapi aturan global semakin terfragmentasi. Tarif perdagangan, kontrol ekspor, *industrial policy*, dan kebijakan teknologi kini menjadi instrumen persaingan

antarnegara. Di sisi lain, berkembangnya BRICS+, meningkatnya pengaruh *Global South*, dan munculnya berbagai standar teknologi yang berbeda menunjukkan bahwa dunia sedang bergerak menuju sistem multipolar yang lebih kompleks.

Perubahan geopolitik menyebabkan profil risiko organisasi mengalami transformasi yang signifikan. Jika sebelumnya organisasi lebih fokus pada risiko operasional, keuangan, dan kepatuhan, kini risiko utama justru berasal dari luar organisasi, seperti risiko geopolitik, risiko negara (*country risk*), risiko teknologi, risiko kebijakan, dan risiko kepercayaan (*confidence risk*).

Empat pendorong utama fragmentasi adalah *weaponisasi* perdagangan, pembentukan blok teknologi dan sumber daya strategis, berkembangnya tatanan multipolar, serta *digital sovereignty.* Kombinasi faktor-faktor tersebut menciptakan ketidakpastian yang jauh lebih tinggi dibandingkan sebelumnya.

Guncangan geopolitik memiliki mekanisme transmisi yang sangat nyata terhadap dunia usaha. Konflik internasional memengaruhi kebijakan pemerintah, mengubah persepsi risiko negara, memengaruhi arus modal, nilai tukar, pasar obligasi, dan pasar saham yang pada akhirnya berdampak terhadap investasi, pertumbuhan ekonomi, serta kinerja korporasi.

Dinamika geopolitik tersebut dapat diterjemahkan ke dalam bahasa manajemen risiko organisasi melalui beberapa kategori risiko utama, yaitu:

- *Trade and Tariff Risk*
- *Supply Chain Concentration Risk*
- *Regulatory and Cross-Jurisdiction Risk*
- *Reputational and Political Risk*
- *Capital and Financing Risk*

Dengan demikian, geopolitik tidak lagi menjadi isu eksternal yang jauh dari organisasi, melainkan telah menjadi bagian dari *enterprise risk management*.

Dalam kondisi ketidakpastian global, kepercayaan (trust) menjadi aset strategis yang sangat menentukan keberlangsungan organisasi. Pasar tidak hanya menilai kondisi perusahaan saat ini, tetapi juga prospek masa depan. Hilangnya kepercayaan menyebabkan meningkatnya biaya modal, mahalnya pembiayaan, tertundanya investasi, dan meningkatnya ketidakpastian bisnis. Karena itu, kemampuan menjaga reputasi, kredibilitas, dan konsistensi tata kelola menjadi faktor penting dalam mempertahankan kepercayaan investor, regulator, maupun masyarakat.

Perubahan lingkungan eksternal menuntut perubahan mendasar dalam fungsi pengawasan Dewan. *Dashboard* tradisional yang berfokus pada laba, arus kas, dan pendapatan tidak lagi memadai. Dewan perlu memperhatikan indikator-indikator masa depan seperti *country risk, policy risk, geopolitical intelligence, supply chain risk, capital flow*, dan *market confidence*.

Konsep *Governance* 5.0 menekankan bahwa pengambilan keputusan harus bergeser dari reaktif menuju prediktif melalui:

- *strategic foresight;*
- *scenario planning;*
- *early warning indicators;*
- *continuous risk intelligence; dan*
- *adaptive decision making.*

Pendekatan tersebut dapat dilengkapi dengan penggunaan *scenario planning* yang mempertimbangkan berbagai tingkat eskalasi geopolitik sehingga organisasi memiliki kesiapan menghadapi berbagai kemungkinan kondisi masa depan.

Salah satu pesan terpenting dari materi ini adalah perlunya redefinisi peran Internal Audit. Internal Audit tidak lagi hanya berfungsi sebagai pemberi *assurance* atas kepatuhan dan efektivitas pengendalian, tetapi berkembang menjadi:

- penyedia intelijen risiko independen;
- advisor terhadap emerging risks;
- mitra sistem peringatan dini (early warning);
- pemberi assurance atas risiko strategis; dan
- katalis peningkatan tata kelola organisasi.

Dalam konteks Governance 5.0, auditor internal diharapkan mampu membantu Dewan dan Manajemen memahami implikasi geopolitik terhadap strategi bisnis, mengevaluasi ketahanan organisasi, serta memberikan rekomendasi yang bersifat *forward-looking*.

Materi ini memberikan pesan bahwa dunia sedang memasuki era geopolitik baru yang ditandai oleh fragmentasi, kompetisi antarblok, dan meningkatnya ketidakpastian global. Risiko organisasi tidak lagi didominasi oleh faktor internal, tetapi oleh dinamika eksternal yang memengaruhi investasi, rantai pasok, teknologi, regulasi, dan kepercayaan pasar.

Dalam menghadapi kondisi tersebut, organisasi perlu membangun Governance 5.0, yaitu tata kelola yang berorientasi ke depan melalui *strategic foresight, scenario planning, continuous risk intelligence*, dan *adaptive decision making*. Dewan Komisaris harus memperluas fokus pengawasannya dari kinerja historis menuju antisipasi risiko masa depan, sementara Internal

Audit harus berevolusi menjadi mitra strategis yang menyediakan assurance sekaligus intelijen risiko bagi organisasi. Dengan demikian, organisasi tidak hanya mampu bertahan menghadapi ketidakpastian, tetapi juga meningkatkan ketahanan dan daya saing dalam lanskap geopolitik yang semakin kompleks.

SESI TANYA JAWAB:

Pertanyaan 1 (Ibu **Ledya dari PT Kompas Gramedia):**

Selama ini organisasi lebih berfokus pada risiko internal yang relatif dapat dikendalikan. Namun saat ini risiko eksternal, khususnya risiko geopolitik, justru menjadi semakin dominan. Kondisi tersebut menuntut organisasi untuk lebih adaptif dan resilien.

- Apakah perusahaan saat ini sudah siap menghadapi perubahan tersebut?
- Jika belum, apa yang harus dipersiapkan?
- Mengingat banyak dampak geopolitik berasal dari faktor di luar kendali perusahaan, seperti kebijakan pemerintah maupun perubahan nilai tukar, seharusnya seperti apa peran pemerintah dalam membantu perusahaan menghadapi risiko tersebut?

Jawaban:

Saya melihat tantangan ini tidak hanya berasal dari geopolitik, tetapi juga dari perubahan teknologi. Sebagai contoh, dahulu sebuah *publishing company* seperti Kompas memperoleh pendapatan yang sangat besar dari iklan cetak. Namun saat ini pola pemasaran telah berubah sepenuhnya akibat media sosial dan perkembangan *artificial intelligence*. Bahkan seluruh proses *publishing* dari awal hingga akhir kini dapat dilakukan oleh satu orang dengan bantuan AI. Contoh lainnya adalah PT Pos Indonesia. Dahulu PT Pos memiliki jaringan yang sangat luas dan menjadi tulang punggung layanan pengiriman uang maupun surat. Namun perkembangan teknologi digital menyebabkan model bisnis tersebut berubah secara drastis. Padahal, apabila memiliki *foresight*, PT Pos sebenarnya memiliki peluang besar berkembang menjadi tulang punggung logistik *e-commerce*. Hal tersebut menunjukkan bahwa organisasi tidak boleh hanya bersifat reaktif, tetapi harus mampu mengantisipasi perubahan sejak dini.

Di sinilah pentingnya *governance*. Risiko tata kelola dapat menjadi sangat fatal. Sebagus apa pun sistem pengendalian internal dan sebanyak apa pun sertifikasi auditor internal yang dimiliki, apabila organisasi tidak memahami risiko geopolitik dan perubahan teknologi, dampaknya tetap dapat mengancam keberlangsungan perusahaan.

Ke depan, manajemen perlu mulai menganalisis faktor-faktor eksternal secara sistematis. Saat ini AI telah menyediakan berbagai *tools* yang dapat membantu memprediksi berbagai kemungkinan kondisi di masa depan melalui *scenario analysis*. Oleh karena itu, organisasi juga harus memperbarui *tools* yang digunakan untuk menganalisis risiko eksternal karena pendekatan lama tidak lagi memadai.

Memang isu eksternal bukan berada dalam kendali perusahaan. Namun dampaknya tetap akan dirasakan oleh perusahaan. Contohnya adalah bisnis *pager* yang hilang akibat perkembangan teknologi, ataupun *BlackBerry* yang kehilangan pangsa pasar karena

munculnya *smartphone*. Tata kelola internal mereka mungkin baik, tetapi perubahan eksternal menyebabkan model bisnisnya tidak lagi relevan.

Karena itu, peran pemerintah tetap sangat penting. Namun di sisi lain, manajemen juga harus membangun evolusi fungsi audit internal agar tidak hanya mengaudit risiko internal, tetapi juga mampu memberikan *assurance* atas *external risk*.

Pertanyaan 2 (Bapak Amri dari BPKH):

Dalam dunia yang semakin konfliktif dengan meningkatnya berbagai peperangan, strategi dan kebijakan apa yang sebaiknya dilakukan Indonesia untuk menghadapi kondisi tersebut?

Jawaban:

Baik pada tingkat mikro maupun makro, prinsip *governance* pada dasarnya sama. *Micro governance* maupun *macro governance* sama-sama menuntut kompetensi manajemen, pengelolaan *conflict of interest*, independensi, dan profesionalisme dalam proses pengambilan keputusan. Dalam konteks negara, proses tersebut melibatkan berbagai institusi seperti Bappenas, DPR RI, BPK RI, dan BPKP. Apabila institusi-institusi tersebut melemah, maka risiko makro akan meningkat. Hal inilah yang menjadi perhatian para investor ketika menilai kualitas *governance* suatu negara.

Pada tingkat perusahaan juga berlaku prinsip yang sama. Dalam era *Governance 5.0*, batas antara *governance* pemerintah dan perusahaan semakin menyatu. Perusahaan multinasional menerapkan standar tata kelola yang memperhatikan kondisi makro dan mikro secara bersamaan. Oleh karena itu, keterkaitan (*interlinkage*) antara *macro governance* dan *micro governance* menjadi perhatian utama investor.

Pada akhirnya, kualitas suatu keputusan, baik pada tingkat negara maupun perusahaan, sangat ditentukan oleh kualitas proses pengambilan keputusan itu sendiri. Apabila prosesnya buruk, maka hasil keputusannya juga akan buruk. Proses tersebut pada hakikatnya adalah *governance*, dan inilah yang juga menjadi perhatian berbagai *rating agency*.

Mengenai apakah beban mitigasi harus menjadi tanggung jawab perusahaan atau negara, pada dasarnya setiap perusahaan memiliki kapasitas yang berbeda. Namun dampak konflik geopolitik, seperti perang Iran, memengaruhi seluruh aspek kehidupan, terutama sektor energi. Pemerintah telah mengalokasikan sekitar Rp130 triliun untuk subsidi BBM agar harga energi tetap terkendali. Di sisi lain, kebijakan tersebut juga memiliki konsekuensi berupa berkurangnya ruang fiskal untuk pembangunan infrastruktur maupun pertumbuhan ekonomi jangka panjang. Dengan demikian, stabilitas ekonomi dan politik menjadi faktor yang saling berkaitan.

Respons terhadap risiko eksternal harus dilakukan melalui pendekatan *whole-of-government*. Di sisi lain, perusahaan yang mampu bertahan adalah perusahaan yang tidak hanya bersifat reaktif, tetapi juga melakukan mitigasi risiko secara proaktif. Dalam konteks tersebut, AI dan *cybersecurity* menjadi dua aspek yang semakin penting untuk diperhatikan.

Dalam menghadapi dunia yang semakin berkonflik, Indonesia perlu memperkuat ketahanan nasional melalui diversifikasi sumber dan bauran energi, meningkatkan kapasitas penyimpanan energi, memperkuat diplomasi melalui ASEAN sebagai *shock breaker*, meningkatkan kapasitas intelijen serta *early warning system*, dan membangun komunikasi pemerintah yang mampu menjaga kepercayaan masyarakat maupun dunia usaha. Pendekatan yang dibutuhkan adalah strategi yang bersifat prediktif, bukan sekadar reaktif.

TRACK 1-A

DIGITAL STRATEGY AND TRANSFORMATION

Sigit Puspito Wigati Jarot, M.Eng, Ph.D.
Head of National Telematics Infrastructure at Mastel Founding
Chairman of Indonesia 5G Forum Senior ICT Standardisation Expert at GIST
CEO at Cloudtech

ABSTRAK

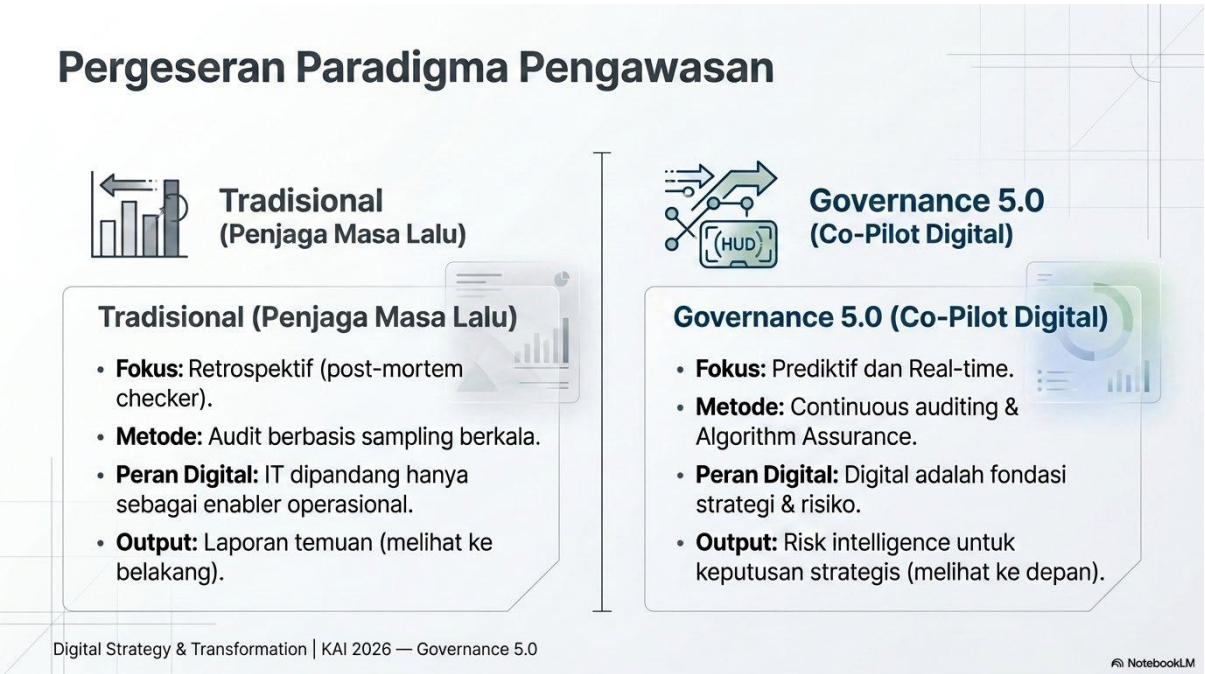
Evolusi profesi auditor internal di era digital telah bergeser dari sekadar *enabler* menjadi fondasi *Governance 5.0* melalui peran sebagai *digital co-pilot*. Transformasi tersebut ditandai oleh integrasi ruang siber dan ruang fisik (*cyber-physical integration*) yang berorientasi pada manusia (*human-centric*). Di sisi lain, kesenjangan talenta dan tingkat maturitas digital yang sangat tinggi menyebabkan pendekatan *oversight* tidak lagi dapat menggunakan prinsip *one size fits all*. Selain itu, keberadaan *legacy systems*, *data silo*, dan infrastruktur yang telah usang menyebabkan penyediaan *real-time dashboard* bagi *board* masih menjadi sebuah ambisi di banyak organisasi. Dalam konteks tersebut, auditor internal sebagai lini ketiga berperan sebagai *digital co-pilot* yang memberikan pengawasan digital secara independen terhadap lini pertama dan lini kedua melalui pemanfaatan data *real-time*. Dengan demikian, auditor mampu menyediakan informasi yang dibutuhkan manajemen untuk mengambil keputusan secara cepat dan tepat. Auditor juga memiliki peran baru sebagai pemberi *assurance* atas algoritma dengan memastikan bahwa algoritma menghasilkan informasi yang akurat, andal, dan mampu memberikan nilai tambah bagi perusahaan.

Kata Kunci: Internal Auditor Role, *Co-pilot* transformasi digital, *Cyber-physical integration*

PEMBAHASAN

Perjalanan profesi auditor mengalami transformasi dari fungsi *compliance* menuju *co-pilot* strategi digital sebagai fondasi *Governance 5.0*. Pada masa lalu, teknologi digital dipandang hanya sebagai *enabler* yang mendukung proses operasional, sedangkan keputusan strategis tetap didasarkan pada pertimbangan manusia dan laporan yang bersifat periodik. Saat ini, digital telah menjadi fondasi organisasi (*digital-first*), di mana teknologi dan data menjadi dasar model bisnis, model risiko, serta model pengawasan.

Perubahan tersebut mendorong evolusi tata kelola menuju model yang *insight-driven*, *predictive*, dan *technology-enabled*, dengan manusia tetap menjadi pusat pengambilan keputusan. Oleh karena itu, fondasi digital harus terus diperkuat karena kegagalan pada aspek tersebut akan menurunkan keandalan data dan informasi yang menjadi dasar pengambilan keputusan organisasi.



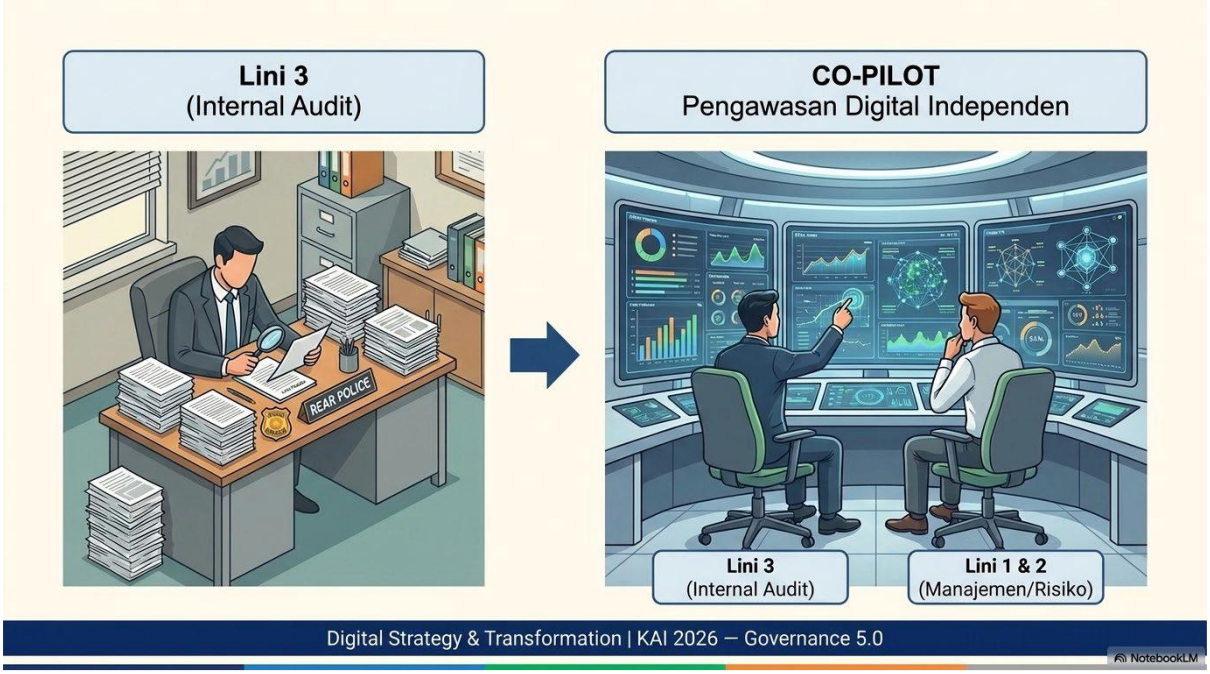
Evolusi profesi audit internal menurut Deloitte berkembang dari Audit 3.0 menuju Audit 4.0 hingga Audit 5.0 yang mengedepankan *continuous assurance*. *Governance 5.0* bukan merupakan satu standar tunggal, melainkan titik temu berbagai perkembangan global yang menempatkan teknologi sebagai objek pengawasan dari aspek *design*, akuntabilitas, serta dampaknya terhadap manusia. Pendekatan tersebut juga selaras dengan konsep *Society 5.0* Jepang yang menekankan integrasi ruang siber dan ruang fisik secara *human-centric*.

Namun demikian, kesenjangan talenta dan tingkat maturitas digital yang sangat ekstrem menyebabkan pendekatan *oversight* tidak dapat disamaratakan (*one size fits all*). Kondisi tersebut diperparah oleh keberadaan *legacy systems*, *data silo*, serta infrastruktur yang sudah usang sehingga penyediaan *real-time dashboard* bagi *board* masih menjadi tantangan besar. Berdasarkan *Governance 5.0 Maturity Matrix*, sebagian besar organisasi di Indonesia masih berada pada Level 1 (*Digitized*) dan Level 2 (*Connected*), serta belum banyak yang mencapai Level 3 (*Insight-Driven*) maupun Level 4 (*Predictive Adaptive*) sebagai karakteristik *Governance 5.0*. Oleh karena itu, auditor internal sebagai lini ketiga perlu bertransformasi menjadi *digital co-pilot* yang mampu memberikan pengawasan digital secara independen terhadap lini pertama dan lini kedua.

Tantangan struktural dalam mewujudkan *real-time dashboard* masih sangat besar sehingga implementasinya belum menjadi kenyataan. Beberapa tantangan utama meliputi:

1. **Kesenjangan talenta**, yaitu pasokan *data scientist* dan spesialis AI yang masih jauh di bawah kebutuhan organisasi.
2. ***Legacy systems***, *data silo*, dan sistem yang belum terintegrasi sehingga menghambat orkestrasi data secara *real-time*.

3. ***Post-mortem position***, yaitu kondisi ketika auditor internal belum dilibatkan sejak fase *design* sistem dan pengembangan algoritma sehingga fungsi *assurance* baru dilakukan setelah sistem berjalan.



Tiga Pesan Kunci

1. **Digitalisasi merupakan strategi korporasi, bukan lagi sekadar proyek teknologi informasi (*IT project*).** *Board* dan auditor yang tidak memahami arsitektur digital organisasinya akan kehilangan kapasitas *oversight*.
2. **Governance 5.0 berorientasi pada masa depan**, yaitu pergeseran dari *assurance* atas peristiwa masa lalu menuju *continuous assurance*, *predictive analytics*, dan *real-time risk intelligence*.
3. **Indonesia memiliki momentum regulasi yang terbuka**, ditandai dengan GIAS 2024, *draft* Etika AI, serta berbagai regulasi OJK dan Bank Indonesia. Kondisi tersebut menuntut auditor internal untuk menjadi *trusted advisor* yang mampu bergerak lebih cepat daripada perkembangan regulasi.

Auditor tidak lagi hanya memberikan *assurance* atas proses bisnis, tetapi juga menjadi pemberi *assurance* atas algoritma. Auditor harus mampu menilai apakah algoritma telah menghasilkan informasi yang akurat, andal, dan dapat dipercaya sehingga mampu memberikan nilai tambah bagi perusahaan.

Terdapat tiga pesan utama yang perlu menjadi perhatian. Pertama, digitalisasi merupakan strategi korporasi, bukan lagi sekadar proyek teknologi informasi (*IT project*). *Board* dan auditor yang tidak memahami arsitektur digital organisasinya akan kehilangan kapasitas *oversight*. Kedua, *Governance 5.0* berorientasi pada masa depan melalui pergeseran dari *assurance* atas kejadian masa lalu menuju *continuous*, *predictive*, *real-time risk intelligence*.

Ketiga, Indonesia memiliki momentum regulasi yang terbuka melalui GIAS 2024, *draft* Etika AI, serta berbagai regulasi OJK dan Bank Indonesia sehingga auditor internal dituntut menjadi *trusted advisor* yang mampu bergerak lebih cepat dibandingkan perkembangan regulasi.
Dalam paradigma baru tersebut, auditor tidak hanya memberikan *assurance* atas proses bisnis, tetapi juga menjadi pemberi *assurance* atas algoritma dengan memastikan bahwa algoritma menghasilkan informasi yang akurat, dapat dipercaya, dan mendukung penciptaan nilai bagi organisasi. Oleh karena itu, mandat baru auditor internal bukan lagi sekadar menjaga masa lalu, melainkan menjadi *co-pilot* transformasi digital organisasi.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Bardi dari Asuransi BRI Life):
Selama ini auditor sebagai lini ketiga berperan sebagai penjaga (*watchdog*) sehingga memiliki jarak dengan manajemen. Namun apabila auditor berperan sebagai *co-pilot*, fungsinya menjadi berbeda karena seolah-olah ikut menerbangkan pesawat bersama manajemen dan terlibat dalam operasional. Bukankah kondisi tersebut berpotensi membuat auditor ikut dalam pengambilan keputusan? Mohon penjelasannya.

Jawaban:
Sebagai *co-pilot*, auditor tidak mengambil alih pengambilan keputusan manajemen. Peran auditor adalah memiliki kemampuan untuk membaca kondisi secara *real-time* dan memberikan informasi yang bersifat prediktif. Apabila terdapat jeda antara informasi yang diterima dan proses pengambilan keputusan, organisasi akan kehilangan momentum dalam merespons perubahan. Untuk meyakinkan direksi, auditor harus mampu menyediakan data *real-time*. Dengan demikian, hasil yang diberikan auditor tidak hanya menunjukkan tingkat kepatuhan (*compliance*), tetapi juga menyajikan informasi prediktif yang dapat digunakan sebagai dasar pengambilan keputusan secara cepat dan tepat.

Pertanyaan 2 (Bapak Irfan dari Penjaminan Infrastruktur Indonesia)
Kondisi geopolitik saat ini memberikan tekanan yang cukup besar terhadap perusahaan sehingga kemampuan finansial menjadi semakin terbatas. Bagaimana meyakinkan jajaran direksi agar tetap memperkuat fungsi *monitoring* sehingga implementasinya dapat dilakukan secara komprehensif dan efektif?

Jawaban:
Direksi membutuhkan data *real-time* sebagai dasar pengambilan keputusan. Oleh karena itu, hasil yang disampaikan auditor tidak lagi cukup hanya menunjukkan tingkat kepatuhan (*compliance*), tetapi juga harus mampu memberikan informasi prediktif. Dengan tersedianya data *real-time*, direksi dapat mengambil keputusan secara lebih cepat sehingga organisasi tidak kehilangan momentum dalam merespons risiko maupun memanfaatkan peluang yang muncul.

TRACK 1-B

Ethical Governance & Integrity Culture in Digital Organizations

Sri Sutanto, S.E., M.Si
Inspektur Badan Siber dan Sandi Negara (BSSN)

ABSTRAK

Transformasi digital telah mengubah cara organisasi menjalankan proses bisnis, mengambil keputusan, dan memberikan layanan kepada masyarakat. Pemanfaatan *big data*, *artificial intelligence* (AI), *digital platforms*, dan *process automation* mampu meningkatkan efisiensi, produktivitas, dan inovasi, namun pada saat yang sama juga memunculkan tantangan baru yang berkaitan dengan etika, transparansi, akuntabilitas, perlindungan data, dan keamanan siber. Perkembangan teknologi yang semakin kompleks menunjukkan bahwa keberhasilan transformasi digital tidak cukup hanya ditopang oleh kepatuhan terhadap regulasi (*compliance*), tetapi juga memerlukan tata kelola yang berlandaskan nilai-nilai etika (*ethical governance*) serta budaya integritas (*integrity culture*) yang terinternalisasi dalam seluruh proses organisasi. Artikel ini membahas konsep *ethical governance* sebagai fondasi organisasi digital, faktor-faktor yang menyebabkan digitalisasi memperbesar risiko etika, lima pilar utama *integrity culture*, berbagai tantangan etika dalam ekosistem digital, *Digital Integrity Maturity Model* sebagai kerangka peningkatan kematangan organisasi, serta pentingnya kepemimpinan dalam membangun budaya integritas. Pembahasan juga menguraikan praktik-praktik terbaik dan pembelajaran dari berbagai kasus keberhasilan maupun kegagalan implementasi tata kelola digital. Pada akhirnya, organisasi digital dituntut untuk membangun sistem yang tidak hanya patuh terhadap regulasi, tetapi juga mampu menciptakan kepercayaan publik melalui penerapan nilai-nilai etika yang konsisten dalam setiap pengambilan keputusan dan pemanfaatan teknologi digital.

Kata Kunci: *Ethical Governance, Integrity Culture, Tata Kelola Digital*

PEMBAHASAN

Transformasi digital telah mengubah secara fundamental cara organisasi menjalankan aktivitas operasional, menyusun kebijakan, mengelola data, serta berinteraksi dengan pemangku kepentingan. Pemanfaatan teknologi seperti *big data*, *artificial intelligence* (AI), *digital platforms*, dan *process automation* membuka peluang yang besar untuk meningkatkan efisiensi, kualitas layanan, serta inovasi organisasi. Namun demikian, digitalisasi juga menghadirkan tantangan baru yang jauh lebih kompleks dibandingkan transformasi organisasi pada era sebelumnya. Persoalan etika, transparansi, perlindungan data pribadi, keamanan informasi, serta akuntabilitas dalam pengambilan keputusan berbasis teknologi menjadi isu strategis yang harus dikelola secara sistematis. Kondisi tersebut menunjukkan bahwa transformasi digital bukan sekadar perubahan teknologi, melainkan juga perubahan

tata kelola dan budaya organisasi yang harus mampu menjaga integritas di tengah perkembangan teknologi yang berlangsung sangat cepat.

Realitas tersebut tercermin dari berbagai indikator yang menunjukkan meningkatnya risiko etika pada organisasi digital. Sebagian besar organisasi pemerintah pernah mengalami insiden siber dalam beberapa tahun terakhir, sementara korupsi digital berkembang jauh lebih cepat dibandingkan pola korupsi konvensional. Di sisi lain, masih banyak aparatur yang merasa belum memiliki pedoman etika digital yang memadai sebagai acuan dalam menghadapi berbagai dilema penggunaan teknologi. Fakta tersebut memperlihatkan bahwa digitalisasi tanpa disertai penguatan integritas justru berpotensi mempercepat munculnya krisis kepercayaan publik. Oleh karena itu, keberhasilan transformasi digital tidak hanya diukur dari tingkat adopsi teknologi, tetapi juga dari kemampuan organisasi membangun sistem tata kelola yang mampu memastikan teknologi digunakan secara bertanggung jawab, transparan, dan berorientasi pada kepentingan publik.

Dalam konteks tersebut, paradigma tata kelola perlu bergeser dari pendekatan *compliance* menuju *ethical governance*. Pendekatan *compliance* berorientasi pada kepatuhan terhadap regulasi sehingga organisasi cenderung bertindak reaktif terhadap pelanggaran dan berfokus pada pemenuhan persyaratan administratif maupun dokumentasi. Sebaliknya, *ethical governance* menempatkan nilai integritas sebagai landasan utama dalam setiap proses pengambilan keputusan. Organisasi tidak hanya berupaya menghindari pelanggaran, tetapi juga secara proaktif membangun sistem etika, menginternalisasi nilai-nilai organisasi, mempertimbangkan dampak setiap keputusan terhadap masyarakat, serta menjaga kepercayaan publik sebagai aset yang paling penting. Pergeseran paradigma tersebut menunjukkan bahwa tata kelola digital yang efektif tidak berhenti pada pertanyaan mengenai apakah suatu tindakan telah sesuai aturan, tetapi juga apakah tindakan tersebut merupakan keputusan yang benar secara etis.

Risiko etika pada organisasi digital semakin meningkat karena karakteristik teknologi yang memiliki kecepatan, skala, dan kompleksitas yang jauh melampaui mekanisme pengawasan konvensional. Keputusan berbasis algoritma dapat dihasilkan dalam hitungan milidetik, sementara satu keputusan digital dapat berdampak kepada jutaan pengguna secara bersamaan. Selain itu, jejak digital dapat dimodifikasi maupun dihapus apabila organisasi tidak memiliki *audit trail* yang kuat. Di sisi lain, teknologi tidak pernah bersifat sepenuhnya netral karena algoritma selalu dipengaruhi oleh nilai, preferensi, asumsi, maupun kualitas data yang digunakan selama proses pengembangannya. Akibatnya, berbagai bentuk bias dapat muncul tanpa disadari dan menghasilkan keputusan yang tidak adil ataupun diskriminatif. Oleh karena itu, organisasi perlu memastikan bahwa perkembangan teknologi selalu disertai

dengan penguatan tata kelola, pengendalian internal, dan mekanisme pengawasan yang memadai agar risiko etika dapat diminimalkan.

Pembangunan organisasi digital yang berintegritas memerlukan fondasi budaya yang kuat melalui lima pilar utama *integrity culture*, yaitu transparansi, akuntabilitas, kejujuran, independensi, dan keberanian moral. Transparansi diwujudkan melalui keterbukaan informasi serta proses pengambilan keputusan yang dapat dipertanggungjawabkan. Akuntabilitas memastikan bahwa setiap individu bertanggung jawab atas konsekuensi dari setiap keputusan yang diambil. Kejujuran diwujudkan melalui penyampaian data dan informasi yang akurat tanpa manipulasi, sedangkan independensi menjaga objektivitas organisasi dari berbagai tekanan maupun konflik kepentingan. Pilar terakhir, yaitu keberanian moral, mendorong setiap individu untuk berani menyampaikan keberatan, melaporkan pelanggaran, dan mengambil tindakan ketika nilai-nilai organisasi dilanggar. Kelima pilar tersebut saling melengkapi dalam membangun budaya organisasi yang mampu mempertahankan integritas di tengah perubahan teknologi yang sangat dinamis.

Implementasi *ethical governance* juga menghadapi berbagai tantangan etika yang khas pada ekosistem digital. Tantangan tersebut meliputi konflik kepentingan dalam pemanfaatan akses digital, integritas data dan informasi, perlindungan privasi serta keamanan siber, akuntabilitas algoritma dan AI, serta penguatan *whistleblowing* dan *speak-up culture*. Konflik kepentingan dapat muncul ketika akses terhadap sistem informasi dimanfaatkan untuk kepentingan pribadi atau kelompok tertentu. Integritas data menghadapi ancaman berupa fabrikasi, falsifikasi, plagiarisme data, maupun bias sistemik pada algoritma. Sementara itu, perlindungan privasi harus diseimbangkan dengan tuntutan transparansi publik melalui penerapan prinsip *least privilege* dan *full accountability*. Dalam penggunaan AI, setiap keputusan yang dihasilkan algoritma harus dapat dijelaskan (*explainability*), melibatkan validasi manusia pada keputusan berisiko tinggi (*human-in-the-loop*), serta diaudit secara berkala untuk mengidentifikasi potensi bias algoritmik. Selain itu, organisasi juga perlu membangun sistem pelaporan pelanggaran yang aman melalui mekanisme pelaporan anonim, perlindungan terhadap pelapor, transparansi proses tindak lanjut, serta budaya yang mendorong setiap individu berani menyampaikan pelanggaran tanpa rasa takut terhadap pembalasan.

Untuk memastikan budaya integritas berkembang secara berkelanjutan, organisasi perlu mengukur tingkat kematangannya melalui *Digital Integrity Maturity Model*. Model tersebut menggambarkan empat tahapan perkembangan organisasi, dimulai dari tingkat reaktif yang hanya merespons ketika terjadi pelanggaran, kemudian meningkat menjadi tahap kepatuhan terhadap regulasi, berlanjut menuju tahap proaktif melalui pembangunan sistem etika dan mekanisme pengawasan, hingga mencapai tingkat budaya di mana integritas telah menjadi

bagian dari DNA organisasi dan melekat pada setiap pengambilan keputusan. Perjalanan menuju tingkat kematangan yang lebih tinggi memerlukan komitmen jangka panjang, penguatan tata kelola, pembelajaran berkelanjutan, serta evaluasi secara periodik terhadap efektivitas kebijakan dan budaya organisasi.

Keberhasilan membangun *ethical governance* pada akhirnya sangat ditentukan oleh kualitas kepemimpinan organisasi. Integritas tidak dimulai dari kebijakan tertulis, melainkan dari perilaku pimpinan yang menjadi teladan bagi seluruh anggota organisasi. Pemimpin yang secara konsisten menunjukkan transparansi, menolak praktik yang tidak etis, melaporkan potensi konflik kepentingan, memberikan apresiasi terhadap perilaku berintegritas, serta menegakkan aturan secara konsisten akan membentuk budaya organisasi yang kuat. Berbagai praktik terbaik menunjukkan bahwa keberhasilan sistem digital tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada desain tata kelola yang menjadikan perilaku etis sebagai pilihan yang paling mudah dilakukan. Sebaliknya, berbagai kasus kebocoran data, penyalahgunaan akses sistem, maupun manipulasi informasi menunjukkan bahwa kegagalan teknologi pada umumnya berakar pada lemahnya budaya integritas dan tata kelola organisasi. Oleh karena itu, organisasi digital perlu membangun *ethical governance* sebagai fondasi utama transformasi digital agar inovasi teknologi berjalan seiring dengan peningkatan kepercayaan publik, akuntabilitas, dan keberlanjutan organisasi.

Transformasi digital memberikan peluang yang sangat besar bagi organisasi untuk meningkatkan efisiensi, kualitas pelayanan, dan inovasi. Namun, kemajuan teknologi pada hakikatnya hanya memperluas kapasitas organisasi dalam menjalankan proses bisnis, sehingga teknologi dapat menjadi penguat integritas maupun memperbesar risiko penyimpangan, bergantung pada nilai-nilai yang mendasari pemanfaatannya. Oleh karena itu, pembangunan organisasi digital tidak dapat berhenti pada penyediaan teknologi, penyusunan regulasi, ataupun penerapan pengendalian internal semata, tetapi harus disertai dengan penguatan *ethical governance* yang mampu menginternalisasikan integritas ke dalam setiap proses pengambilan keputusan. Penerapan lima pilar *integrity culture*, pengelolaan tantangan etika dalam ekosistem digital, peningkatan tingkat kematangan organisasi melalui *Digital Integrity Maturity Model*, serta implementasi langkah-langkah strategis dalam membangun budaya integritas menjadi fondasi penting dalam mewujudkan tata kelola digital yang terpercaya, akuntabel, dan berkelanjutan.

Keberhasilan transformasi digital pada akhirnya tidak ditentukan oleh kecanggihan teknologi yang dimiliki, melainkan oleh kualitas manusia dan budaya organisasi yang mengelolanya. Organisasi yang mampu menjadikan integritas sebagai bagian dari DNA kerja akan lebih siap menghadapi berbagai tantangan etika, menjaga kepercayaan publik, serta memanfaatkan

teknologi secara bertanggung jawab. Sebaliknya, sistem digital yang paling modern sekalipun tidak akan mampu menghasilkan tata kelola yang baik apabila digunakan oleh individu yang tidak menjunjung tinggi nilai-nilai etika. Dengan demikian, *ethical governance* harus dipandang sebagai fondasi utama organisasi digital, di mana transparansi menjadi aset yang membangun kepercayaan, setiap individu berperan sebagai penjaga nilai, dan teknologi dimanfaatkan sebagai instrumen untuk memperkuat integritas, bukan sekadar mempercepat proses kerja.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Sugiyanto dari PT Solusi Bangun Indonesia Tbk.):

Terkait *ethical governance* dan *integrity culture*, tata kelola (*governance*) tidak hanya mencakup aspek proses (*process*), tetapi juga struktur (*structure*). Meskipun materi yang disampaikan masih bersifat konseptual, bagaimana Bapak melihat penerapan model *Three Lines* dalam mendukung *ethical governance* di organisasi?

Jawaban:
Pada prinsipnya, kerangka tata kelola yang baik telah mengakomodasi keterpaduan antara aspek people, process, dan technology, sebagaimana tercermin dalam berbagai standar internasional, termasuk standar ISO. Ketiga aspek tersebut harus berjalan secara seimbang karena efektivitas tata kelola tidak hanya ditentukan oleh struktur organisasi atau proses yang terdokumentasi dengan baik, tetapi juga oleh kompetensi sumber daya manusia serta pemanfaatan teknologi yang mendukung penerapan nilai-nilai integritas. Dalam konteks tersebut, model *Three Lines* dapat dipahami sebagai mekanisme yang memastikan setiap fungsi organisasi menjalankan perannya secara jelas dalam menjaga tata kelola, manajemen risiko, pengendalian internal, dan budaya integritas.

Pertanyaan 2 (Bapak Alexander dari Badan Pengawas Obat dan Makanan/BPOM)

Dalam praktiknya, berbagai infrastruktur digital saat ini semakin terintegrasi ke dalam satu aplikasi sehingga kompleksitas aspek keamanan informasi juga semakin meningkat. Apabila instansi memerlukan dukungan atau koordinasi terkait audit keamanan siber, unit mana di BSSN yang dapat menjadi mitra koordinasi? Selain itu, bagaimana pandangan Bapak mengenai fenomena *shadow AI* di organisasi sektor publik dan langkah yang perlu dilakukan auditor internal untuk mengelola risiko tersebut?

Jawaban:

Penguatan tata kelola data dan keamanan digital memerlukan kolaborasi lintas instansi. Salah satu inisiatif yang sedang dikembangkan adalah pembentukan Badan Perantara Identitas, yang bertujuan memperkuat tata kelola identitas digital sehingga masyarakat tidak perlu lagi berulang kali menyerahkan dokumen identitas, seperti KTP, kepada berbagai penyedia layanan. Inisiatif ini masih dalam tahap pengembangan sebagai bagian dari penguatan *data governance*. Selain itu, BSSN juga terus membangun kolaborasi dengan berbagai pemangku kepentingan, termasuk Masyarakat Anti Fitnah Indonesia (MAFINDO), dalam rangka memperkuat literasi digital, keamanan informasi, dan tata kelola ruang siber. Terkait *shadow AI*, organisasi perlu memperkuat kebijakan tata kelola AI, meningkatkan literasi digital pegawai, serta memastikan penggunaan AI berada dalam mekanisme pengendalian dan pengawasan yang memadai agar pemanfaatannya tetap aman, akuntabel, dan sejalan dengan tujuan organisasi.

GENERAL SESSION 2

Internal Audit Repositioned: Driving Value and Strategy in Governance 5.0

Ahmad Hidayat, MBA
Managing Director Internal Audit Danantara Indonesia

ABSTRAK

Perubahan lanskap bisnis, perkembangan teknologi digital, serta meningkatnya kompleksitas risiko telah mendorong terjadinya transformasi mendasar terhadap fungsi audit internal. Pada era *Governance 5.0*, auditor internal tidak lagi hanya berperan sebagai penyedia *assurance* atas kepatuhan, tetapi juga sebagai mitra strategis yang mampu memberikan wawasan, menciptakan nilai (*value creation*), dan mendukung pencapaian tujuan organisasi. Transformasi tersebut ditandai oleh meningkatnya pemanfaatan *Artificial Intelligence* (AI), *machine learning*, *robotic process automation* (RPA), analisis data, dan teknologi digital lainnya dalam proses audit. Namun, penggunaan teknologi harus tetap diimbangi dengan pertimbangan profesional (*professional judgment*), skeptisisme auditor, serta penguatan tata kelola data agar hasil audit tetap berkualitas dan dapat dipercaya. Artikel ini membahas evolusi peran audit internal, kompetensi yang dibutuhkan auditor pada masa depan, tantangan yang muncul dalam lingkungan *Governance 5.0*, serta berbagai strategi yang dapat diterapkan organisasi untuk meningkatkan efektivitas fungsi audit internal. Pembahasan menekankan pentingnya penerapan *data governance*, peningkatan kompetensi digital auditor, pembangunan budaya organisasi yang adaptif terhadap perubahan, pemanfaatan analisis data secara *real-time*, serta transformasi pola pikir auditor dari pendekatan yang berorientasi kepatuhan menuju pemberian nilai strategis bagi organisasi. Dengan demikian, reposisi audit internal merupakan kebutuhan yang tidak dapat dihindari agar fungsi audit tetap relevan dalam menghadapi dinamika risiko organisasi yang semakin kompleks dan mendukung keberlanjutan tata kelola pada era digital.

Kata Kunci: *Governance 5.0*, *Professional Judgment*, *Value Creation*

PEMBAHASAN

Perkembangan teknologi digital, meningkatnya ekspektasi pemangku kepentingan, serta kompleksitas risiko organisasi telah mendorong terjadinya reposisi fungsi audit internal pada era *Governance 5.0*. Audit internal tidak lagi dipandang hanya sebagai fungsi yang memberikan *assurance* atas kepatuhan terhadap kebijakan dan peraturan, tetapi berkembang menjadi mitra strategis yang mampu memberikan wawasan (*insight*), pandangan ke depan (*foresight*), serta nilai tambah (*value creation*) bagi organisasi. Perubahan tersebut

merupakan respons terhadap transformasi lingkungan bisnis yang semakin dinamis, di mana organisasi membutuhkan fungsi audit yang adaptif, berbasis risiko, dan mampu mendukung pengambilan keputusan strategis. Oleh karena itu, relevansi audit internal pada masa depan sangat ditentukan oleh kemampuannya untuk bertransformasi mengikuti perkembangan teknologi, model bisnis, dan karakteristik risiko yang terus berubah.

Reposisi tersebut menuntut perubahan kompetensi auditor internal secara signifikan. Berdasarkan proyeksi kebutuhan keterampilan pada beberapa tahun mendatang, kompetensi teknologi seperti *Artificial Intelligence* (AI), *big data*, jaringan, keamanan siber, dan literasi teknologi menjadi kemampuan yang semakin dominan. Namun demikian, perkembangan teknologi tidak mengurangi pentingnya kompetensi nonteknis yang meliputi kemampuan berpikir kreatif, berpikir analitis, kepemimpinan, komunikasi, rasa ingin tahu untuk terus belajar, serta kemampuan beradaptasi terhadap perubahan. Kombinasi antara penguasaan teknologi dan keterampilan interpersonal menjadi prasyarat bagi auditor internal untuk tetap mampu memberikan penilaian yang objektif dan bernilai tambah di tengah perubahan lingkungan bisnis yang semakin kompleks.

Perubahan ekspektasi tersebut juga tercermin dari prioritas para *Chief Audit Executive* (CAE) dalam mengembangkan fungsi audit internal. Teknologi dipandang sebagai sarana untuk memperluas cakupan audit, meningkatkan efektivitas proses audit, serta menghasilkan wawasan yang lebih mendalam, terutama ketika organisasi menghadapi keterbatasan sumber daya dan lingkungan risiko yang berubah dengan cepat. Auditor masa depan diharapkan tidak hanya menjadi pemeriksa (*assurance provider*), tetapi juga berperan sebagai *risk expert*, *business partner*, *data analyst*, *communicator*, dan pengguna teknologi yang memiliki literasi digital yang baik. Dengan demikian, fungsi audit internal berkembang menjadi fungsi multidisiplin yang mengintegrasikan kompetensi bisnis, teknologi, komunikasi, dan manajemen risiko secara bersamaan.

Meningkatnya pemanfaatan AI dalam dunia audit tidak menghilangkan relevansi profesi auditor internal, melainkan mengubah cara kerja dan pendekatan audit. AI berfungsi sebagai *enabler* yang membantu auditor meningkatkan efisiensi proses analisis data, identifikasi anomali, serta pengolahan informasi dalam jumlah besar. Namun demikian, AI tidak dapat menggantikan *professional judgment*, skeptisisme profesional, maupun kemampuan auditor dalam memahami konteks bisnis dan mempertimbangkan berbagai aspek yang tidak dapat diinterpretasikan secara otomatis oleh teknologi. Oleh karena itu, pemanfaatan AI harus ditempatkan sebagai alat pendukung yang memperkuat kualitas proses audit, bukan sebagai pengganti pertimbangan profesional auditor.

Pada era *Governance 5.0*, auditor internal juga menghadapi lingkungan risiko yang semakin kompleks. Risiko organisasi tidak lagi hanya terbatas pada aspek keuangan, tetapi berkembang mencakup risiko siber, *Environmental, Social, and Governance* (ESG), geopolitik, serta disrupsi teknologi. Di sisi lain, kualitas data masih menjadi tantangan karena banyak organisasi menghadapi data yang tidak terstruktur, tersebar di berbagai sistem, dan belum memiliki standar yang seragam. Kompleksitas tersebut diperburuk oleh budaya organisasi yang masih resisten terhadap transformasi digital, pola pikir auditor yang masih berorientasi pada kepatuhan (*compliance-oriented*), serta meningkatnya ketergantungan terhadap AI tanpa disertai proses validasi yang memadai. Kondisi tersebut berpotensi menurunkan skeptisisme profesional apabila auditor terlalu mengandalkan hasil yang dihasilkan oleh teknologi.

Menghadapi tantangan tersebut, organisasi perlu memperkuat tata kelola data (*data governance*) sebagai fondasi utama transformasi audit internal. Pengelolaan data harus dimulai dengan penetapan kualitas data, kejelasan kepemilikan data, serta mekanisme untuk menjaga integritas data melalui instrumen validasi yang memadai. Selain itu, prinsip *trust but verify* perlu diterapkan dalam mengevaluasi data maupun keluaran AI sehingga setiap informasi yang digunakan dalam proses audit tetap dapat diverifikasi. Penguatan kualitas data juga harus didukung oleh penerapan *audit trail* yang memungkinkan seluruh proses pengolahan data dan keluaran AI dapat ditelusuri kembali apabila diperlukan. Pendekatan tersebut akan meningkatkan reliabilitas informasi yang menjadi dasar dalam penyusunan simpulan audit.

Transformasi audit internal juga memerlukan investasi berkelanjutan pada pengembangan kompetensi auditor dan pemanfaatan teknologi analitik. Auditor perlu memperkuat kemampuan analisis data, literasi kecerdasan buatan, serta pemahaman terhadap proses bisnis agar mampu menginterpretasikan informasi secara lebih komprehensif. Pada saat yang sama, organisasi perlu membangun *real-time risk visibility* melalui pemanfaatan *predictive analytics*, *dynamic audit planning*, serta penyusunan *risk-based* dan *integrated audit universe*. Pendekatan tersebut memungkinkan fungsi audit internal memberikan respons yang lebih cepat terhadap perubahan risiko sekaligus meningkatkan kualitas rekomendasi strategis yang diberikan kepada manajemen dan dewan pengawas. Selain itu, pembangunan budaya *data-driven* dan *continuous learning* menjadi elemen penting agar auditor mampu terus beradaptasi terhadap perkembangan teknologi dan dinamika lingkungan bisnis.

Pada akhirnya, reposisi audit internal pada era *Governance 5.0* merupakan transformasi paradigma yang menempatkan auditor sebagai mitra strategis organisasi dalam menciptakan nilai dan mendukung pencapaian tujuan organisasi. Lingkungan risiko yang semakin

kompleks menuntut fungsi audit untuk bersikap lebih adaptif, proaktif, dan berorientasi pada pemberian wawasan strategis, bukan sekadar memastikan kepatuhan terhadap regulasi. Pemanfaatan AI, *machine learning*, *robotic process automation* (RPA), dan analisis data harus dilakukan secara bertanggung jawab untuk memperkuat *professional judgment*, sementara transformasi pola pikir auditor menjadi faktor kunci dalam menghasilkan *value creation*. Dengan demikian, transformasi bukan lagi sebuah pilihan, melainkan prasyarat agar audit internal tetap relevan, tangguh, dan mampu memberikan kontribusi strategis bagi keberhasilan tata kelola organisasi di masa depan.

Reposisi audit internal pada era *Governance 5.0* merupakan konsekuensi dari meningkatnya kompleksitas risiko, percepatan transformasi digital, serta perubahan ekspektasi para pemangku kepentingan terhadap fungsi audit. Audit internal tidak lagi hanya berperan sebagai penyedia *assurance* atas kepatuhan, tetapi berkembang menjadi mitra strategis yang mampu memberikan *insight*, *foresight*, dan *value creation* bagi organisasi. Transformasi tersebut memerlukan penguatan kompetensi auditor pada aspek teknologi, analisis data, pemahaman bisnis, komunikasi, serta kemampuan berpikir kritis tanpa mengesampingkan pentingnya *professional judgment* dan skeptisisme profesional. Di sisi lain, organisasi juga perlu memperkuat *data governance*, membangun budaya pembelajaran berkelanjutan, serta mengoptimalkan pemanfaatan teknologi digital sebagai pendukung proses audit yang lebih efektif, adaptif, dan berbasis risiko.

Dengan demikian, Internal Audit Repositioned: Driving Value and Strategy in Governance 5.0 mencerminkan perubahan paradigma bahwa keberhasilan fungsi audit internal tidak lagi diukur semata dari kemampuannya menemukan ketidaksesuaian, tetapi dari kontribusinya dalam mendukung pencapaian tujuan strategis organisasi dan memperkuat tata kelola yang berkelanjutan. Pemanfaatan teknologi seperti *Artificial Intelligence*, *machine learning*, *robotic process automation*, dan analisis data harus diposisikan sebagai *enabler* untuk meningkatkan kualitas pengambilan keputusan, bukan sebagai pengganti pertimbangan profesional auditor. Melalui perpaduan antara kompetensi digital, tata kelola data yang baik, pendekatan audit berbasis risiko, dan orientasi pada penciptaan nilai, audit internal akan semakin relevan sebagai fungsi strategis yang mampu memperkuat ketahanan organisasi dan mendukung implementasi *Governance 5.0* di tengah lingkungan bisnis yang terus berubah.

PANEL DISCUSSION 2

Strengthening Governance Through Synergy: The Three Lines Model in a Digital Era

Teguh Widhi Harsono
Director of Finance & Risk Management PT PLN Nusantara Power
Deni Hendra Permana
Senior Vice President IT Audit PT Bank Mandiri (Persero) Tbk

ABSTRAK

Percepatan transformasi digital telah mengubah cara organisasi menjalankan proses bisnis, mengambil keputusan, serta mengelola risiko. Pemanfaatan *artificial intelligence* (AI), *big data*, *cloud computing*, *Internet of Things* (IoT), *digital platforms*, dan berbagai teknologi digital lainnya menciptakan peluang untuk meningkatkan efisiensi, inovasi, dan kualitas layanan, namun secara bersamaan juga menghadirkan risiko baru berupa ancaman siber, penyalahgunaan data, *algorithmic bias*, pelanggaran privasi, hingga menurunnya kepercayaan pemangku kepentingan. Kondisi tersebut menuntut organisasi tidak hanya memperkuat pengendalian internal, tetapi juga membangun tata kelola yang adaptif melalui sinergi yang efektif antara fungsi operasional, manajemen risiko dan kepatuhan, serta audit internal sesuai dengan *The Three Lines Model*. Artikel ini membahas perubahan lanskap risiko digital, pentingnya *ethical governance* sebagai fondasi *digital trust*, tantangan tata kelola pada era kecerdasan buatan, serta penguatan sinergi antarlini dalam mendukung *governance*, *risk management*, *compliance*, dan *internal audit*. Selain itu, pembahasan menguraikan implementasi tata kelola digital melalui penguatan *Single Source of Truth* (SSOT), *data governance*, *control by design*, *cyber resilience*, *continuous assurance*, serta penerapan enam prinsip tata kelola teknologi informasi dan digital. Dengan memperkuat kolaborasi antarlini, organisasi diharapkan mampu menghasilkan keputusan yang lebih cepat, berbasis data, akuntabel, dan berkelanjutan, sekaligus meningkatkan kepercayaan pemangku kepentingan terhadap tata kelola organisasi di era digital.

Kata Kunci: *Three Lines Model,* Tata Kelola Digital*, Digital Trust*

PEMBAHASAN

Transformasi digital telah mengubah secara fundamental cara organisasi menjalankan proses bisnis, mengambil keputusan, dan memberikan layanan kepada para pemangku kepentingan. Pemanfaatan *artificial intelligence* (AI), *big data*, *cloud computing*, *Internet of Things* (IoT), *blockchain*, *robotic process automation* (RPA), serta ekosistem digital yang saling terhubung telah meningkatkan efisiensi, kecepatan, dan kemampuan organisasi dalam menghasilkan nilai. Namun, di balik berbagai peluang tersebut muncul lanskap risiko baru yang semakin kompleks, seperti ancaman siber, penyalahgunaan data, *algorithmic bias*, kurangnya

transparansi dalam pengambilan keputusan otomatis, hingga potensi penyalahgunaan teknologi. Kondisi ini menunjukkan bahwa transformasi digital harus diiringi dengan penguatan tata kelola agar pemanfaatan teknologi tetap berlangsung secara bertanggung jawab, transparan, dan akuntabel.

Perubahan lingkungan digital tersebut juga mengubah karakteristik risiko yang dihadapi organisasi. Berbagai kajian global menunjukkan bahwa *misinformation and disinformation*, *cyber insecurity*, serta dampak negatif penggunaan AI menjadi risiko strategis yang semakin dominan dalam beberapa tahun ke depan. Ketergantungan organisasi terhadap sistem digital meningkatkan eksposur terhadap *phishing*, *ransomware*, *cloud breach*, *deepfake*, *data leakage*, hingga kesalahan keputusan yang dihasilkan algoritma. Oleh karena itu, tata kelola organisasi tidak lagi cukup berorientasi pada kepatuhan terhadap regulasi, tetapi juga harus mampu mengantisipasi risiko-risiko digital melalui penguatan pengendalian, pengawasan, serta koordinasi yang efektif di seluruh lini organisasi.

Dalam menghadapi dinamika tersebut, *ethical governance* menjadi fondasi utama dalam membangun *digital trust*. Kepercayaan terhadap sistem digital hanya dapat diwujudkan apabila teknologi dikembangkan dan dimanfaatkan berdasarkan prinsip keandalan (*reliability*), akuntabilitas (*accountability*), pengawasan manusia (*human oversight*), transparansi (*explicability*), keamanan, perlindungan data pribadi, serta keadilan dalam pemanfaatan AI. Berbagai kebijakan nasional mengenai tata kelola AI juga menegaskan pentingnya penerapan nilai-nilai Pancasila, kemanfaatan, transparansi, keamanan, serta kemampuan sistem AI untuk dipertanggungjawabkan dan diaudit. Dengan demikian, tata kelola digital harus mampu memastikan bahwa inovasi teknologi berjalan seiring dengan perlindungan terhadap kepentingan masyarakat dan peningkatan kepercayaan para pemangku kepentingan.

Penguatan tata kelola digital memerlukan sinergi yang jelas antar fungsi organisasi melalui penerapan *The Three Lines Model*. Lini pertama sebagai pemilik proses bertanggung jawab menjaga kualitas data, menjalankan pengendalian operasional, serta memastikan seluruh proses bisnis berjalan sesuai desain pengendalian. Lini kedua menjalankan fungsi manajemen risiko, kepatuhan, dan tata kelola teknologi informasi dengan menetapkan standar, melakukan pemantauan indikator risiko dan pengendalian, serta memberikan *challenge* terhadap efektivitas pengelolaan risiko. Selanjutnya, lini ketiga melalui fungsi audit internal memberikan *independent assurance* untuk mengevaluasi efektivitas pengendalian, integritas data, pengendalian siber, serta kepatuhan organisasi secara objektif. Sinergi antarlini tersebut menjadi prasyarat agar tata kelola organisasi mampu merespons perubahan lingkungan digital secara lebih adaptif dan terintegrasi.

Implementasi sinergi tersebut didukung oleh pembangunan fondasi *digital governance* yang terintegrasi melalui *Single Source of Truth* (SSOT), *data lake*, *enterprise data warehouse*, integrasi aplikasi, *data loss prevention*, *identity and access management*, serta pemanfaatan AI dan *big data analytics*. Pendekatan ini menghubungkan proses bisnis, data, risiko, kepatuhan, pengendalian, bukti audit, dan pengambilan keputusan dalam satu ekosistem yang saling terintegrasi. Hasil yang diharapkan adalah tersedianya data yang valid, pengendalian yang tertanam (*control by design*), pemantauan risiko secara berkelanjutan melalui indikator risiko utama, proses *assurance* berbasis bukti (*evidence-based assurance*), serta terbentuknya organisasi yang semakin terpercaya dan berkelanjutan.

Penguatan tata kelola digital juga memerlukan penerapan prinsip-prinsip tata kelola teknologi informasi yang komprehensif. Organisasi perlu memastikan kualitas data dan informasi, interoperabilitas teknologi, keamanan informasi berbasis risiko, struktur organisasi yang mendukung *segregation of duties*, kepemimpinan yang memahami model bisnis digital, serta kepatuhan terhadap ketentuan internal maupun regulasi eksternal. Keenam prinsip tersebut saling melengkapi dalam membangun sistem tata kelola yang mampu menjaga kerahasiaan, integritas, dan ketersediaan informasi sekaligus mendukung efektivitas proses bisnis di era digital. Dengan demikian, tata kelola teknologi informasi tidak hanya menjadi tanggung jawab unit teknologi informasi, tetapi merupakan tanggung jawab seluruh organisasi.

Digitalisasi pada hakikatnya merupakan *double-edged sword* yang menghadirkan peluang sekaligus ancaman bagi organisasi. Di satu sisi, digitalisasi meningkatkan efisiensi operasional, mempercepat proses bisnis, memperkuat integritas data, dan meningkatkan konektivitas antar sistem. Namun di sisi lain, organisasi menghadapi ancaman berupa penyalahgunaan akses, transaksi fiktif, serangan siber, kebocoran data, pelanggaran regulasi, serta berbagai bentuk fraud digital. Oleh karena itu, organisasi perlu menerapkan pendekatan mitigasi risiko yang komprehensif melalui *Security Operation Center*, *penetration testing*, *endpoint detection and response*, *multi-factor authentication*, *role-based access control*, *Data Loss Prevention*, pemantauan kepatuhan secara berkelanjutan, serta mekanisme *backup* dan *recovery* untuk meningkatkan ketahanan digital organisasi.

Pada akhirnya, penguatan tata kelola di era digital tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada kemampuan organisasi membangun sinergi yang efektif antara fungsi operasional, manajemen risiko, kepatuhan, dan audit internal. Kepemimpinan memiliki peran sebagai katalis dalam menetapkan arah, nilai, dan arsitektur tata kelola digital, sementara setiap lini menjalankan peran sesuai tanggung jawabnya dalam menciptakan pengendalian yang efektif dan saling melengkapi. Melalui sinergi *The Three Lines Model*, organisasi dapat memperkuat integritas data, meningkatkan kualitas pengambilan keputusan,

menjaga kepercayaan pemangku kepentingan, serta menciptakan tata kelola yang adaptif, tangguh, dan berkelanjutan di tengah percepatan transformasi digital.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Tri Wibowo dari PT Hutama Karya):

Bagaimana perusahaan menjaga keseimbangan antara kecepatan transformasi digital dengan kesiapan organisasi, budaya kerja, dan pengendalian internal? Indikator apa yang perlu digunakan untuk mengetahui bahwa digitalisasi sudah mendapatkan kepercayaan stakeholder maupun berdampak pada pertumbuhan yang berkelanjutan?

Jawaban:

Keberhasilan transformasi digital tidak hanya ditentukan oleh kecepatan implementasi teknologi, tetapi juga oleh kesiapan organisasi dalam mengelola perubahan. Oleh karena itu, transformasi digital perlu dilaksanakan secara bertahap dengan memastikan adanya penyelarasan antara proses bisnis, pengembangan kompetensi sumber daya manusia, penguatan budaya kerja, serta pengendalian internal yang memadai. Penerapan prinsip *control by design* menjadi penting agar setiap inovasi digital telah disertai mekanisme pengendalian sejak tahap perancangan, bukan ditambahkan setelah sistem berjalan. Dengan demikian, organisasi dapat mempercepat transformasi tanpa mengorbankan tata kelola, manajemen risiko, maupun kepatuhan. Keberhasilan transformasi digital tidak cukup diukur dari jumlah aplikasi atau tingkat otomatisasi, tetapi dari nilai yang dihasilkan bagi organisasi dan para pemangku kepentingan. Indikator yang dapat digunakan antara lain peningkatan kualitas dan keandalan data, percepatan proses pengambilan keputusan, penurunan tingkat kesalahan dan insiden operasional, meningkatnya kepatuhan terhadap regulasi, berkurangnya temuan pengendalian, serta meningkatnya kepuasan pengguna dan kepercayaan pemangku kepentingan.

Pertanyaan 2 (Bapak Deni Kusmawan dari PT. Hutama Karya):

Dalam penerapan *three lines model, third line* kadang diminta untuk validasi yang sebenarnya masuk dalam second line, bagaimana solusinya? Kemudian Pada sektor konstruksi, digitalisasi sering berhenti di tengah jalan, bagaimana solusinya?

Jawaban:

Penerapan *Three Lines Model* memerlukan kejelasan peran dan tanggung jawab masing-masing lini agar independensi tetap terjaga. Fungsi lini kedua bertanggung jawab membangun kerangka pengendalian, melakukan pemantauan, dan memberikan pembinaan, sedangkan lini ketiga memberikan *independent assurance* atas efektivitas pengendalian tersebut. Apabila audit internal terlalu sering mengambil alih aktivitas yang menjadi tanggung jawab lini kedua, terdapat risiko berkurangnya independensi auditor pada saat melakukan evaluasi. Oleh karena itu, organisasi perlu memperjelas pembagian peran melalui kebijakan, *governance framework*, dan koordinasi yang baik sehingga setiap lini dapat menjalankan fungsinya secara optimal tanpa terjadi tumpang tindih. Keberlanjutan transformasi digital memerlukan komitmen jangka panjang dari pimpinan serta integrasi dengan strategi bisnis organisasi. Digitalisasi sebaiknya tidak diposisikan sebagai proyek teknologi, melainkan sebagai bagian dari transformasi proses bisnis yang memiliki tujuan, indikator kinerja, serta tata kelola yang jelas.

TRACK 2-A

Building Digital Trust in the Hyperconnected World

Dr. Eng. Hary Budiarto, M.Kom., QGIA
Pusat Pengembangan Aparatur Komdigi, BPSDM Komdigi

ABSTRAK

Transformasi digital telah mengubah cara masyarakat, dunia usaha, dan pemerintah menjalankan aktivitasnya. Konektivitas yang semakin tinggi menghadirkan berbagai peluang inovasi, namun sekaligus memperbesar risiko keamanan siber, kebocoran data, penyalahgunaan kecerdasan buatan, dan penyebaran informasi palsu. Oleh karena itu, keberhasilan transformasi digital tidak hanya bergantung pada teknologi, tetapi juga pada tingkat kepercayaan (*digital trust*) yang dimiliki pengguna terhadap sistem digital. Materi ini menjelaskan konsep *digital trust*, faktor-faktor pembentuknya, *framework* implementasi, strategi organisasi, serta pentingnya tata kelola dan kolaborasi untuk menciptakan ekosistem digital yang aman, transparan, dan berkelanjutan.

Kata Kunci: *Digital Trust, Cybersecurity*, Tata Kelola TI, Privasi Data, Audit Internal

PEMBAHASAN

Era *hyperconnected* ditandai oleh meningkatnya konektivitas antara manusia, perangkat, aplikasi, dan layanan digital. Aktivitas ekonomi, pemerintahan, pendidikan, kesehatan, hingga komunikasi sehari-hari bergantung pada *platform* digital. Kondisi ini menciptakan efisiensi dan inovasi, tetapi juga membuka peluang munculnya berbagai ancaman seperti *ransomware*, *phishing*, *malware*, *carding*, pencurian identitas, kebocoran data pribadi, *deepfake* berbasis AI, serta penyebaran misinformasi, disinformasi, dan malinformasi. Dampak ancaman tersebut tidak hanya berupa kerugian finansial, tetapi juga hilangnya reputasi organisasi, menurunnya kepercayaan masyarakat, dan terganggunya keberlangsungan layanan.

Kepercayaan digital merupakan faktor penentu keberhasilan transformasi digital. Pengguna semakin memperhatikan bagaimana organisasi mengelola data pribadi, melindungi transaksi digital, dan menjamin keamanan layanannya. Ketika organisasi gagal menjaga keamanan informasi, kepercayaan publik akan menurun sehingga berdampak pada loyalitas pelanggan, keberlanjutan bisnis, dan citra organisasi. Oleh karena itu, *cybersecurity* tidak lagi dipandang

hanya sebagai isu teknologi, tetapi telah menjadi bagian dari strategi bisnis, tata kelola, dan manajemen risiko.

Digital Trust adalah kepercayaan masyarakat terhadap keamanan, privasi, integritas, transparansi, dan keandalan teknologi digital. *Digital trust* menjadi fondasi utama ekonomi digital modern karena mendorong masyarakat menggunakan layanan *e-commerce*, *fintech*, pemerintahan digital, dan berbagai inovasi berbasis data. Kepercayaan tersebut juga meningkatkan adopsi teknologi, memperkuat loyalitas pengguna, menjaga keberlangsungan ekosistem digital, dan memberikan nilai tambah bagi organisasi.

Framework yang dipaparkan dalam materi menempatkan beberapa pilar utama, yaitu *safety*, *cybersecurity*, *privacy*, *transparency*, *accountability*, *auditability*, *fairness*, *interoperability*, dan *redressability*. Pilar-pilar tersebut didukung oleh *governance*, *application security*, *data security and privacy*, *risk management*, *vulnerability management*, *threat management*, *compliance*, dan *audit readiness*. Seluruh komponen saling melengkapi untuk memastikan organisasi mampu mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan diri dari ancaman digital sekaligus mempertahankan kepercayaan pengguna.

Strategi membangun *digital trust* berfokus pada tiga aspek utama. Pertama, transparansi melalui kebijakan privasi yang jelas, keterbukaan penggunaan data, audit berkala, dan komunikasi yang akuntabel. Kedua, keamanan dengan menerapkan enkripsi *end-to-end*, autentikasi multifaktor, pemantauan ancaman berbasis AI, peningkatan kesadaran keamanan siber, serta penyusunan *disaster recovery plan*. Ketiga, integritas melalui *penetration testing*, *vulnerability assessment*, kontrol akses, audit internal, serta penerapan tata kelola dan etika teknologi agar sistem digital tetap akurat, andal, dan bebas manipulasi.

Materi juga menekankan pentingnya *IT Governance* dan *Enterprise Architecture* agar strategi bisnis, proses, aplikasi, data, dan infrastruktur teknologi berjalan secara terintegrasi. *Digital trust* hanya dapat diwujudkan melalui kolaborasi pemerintah sebagai regulator, industri sebagai inovator, akademisi sebagai pengembang kompetensi, dan masyarakat sebagai pengguna yang memiliki literasi digital. Dalam konteks ini, auditor internal memiliki peran strategis untuk memberikan *assurance* dan *advisory* atas efektivitas tata kelola TI, keamanan siber, perlindungan data pribadi, kepatuhan terhadap regulasi, manajemen risiko digital, serta kesiapan organisasi menghadapi insiden siber.

Digital Trust merupakan fondasi keberhasilan transformasi digital pada era *hyperconnected*. Kepercayaan tersebut dibangun melalui kombinasi tata kelola yang baik, keamanan siber yang kuat, perlindungan data pribadi, transparansi, integritas, kepatuhan, serta kolaborasi lintas pemangku kepentingan. Organisasi yang berhasil membangun *digital trust* tidak hanya mampu melindungi aset digitalnya, tetapi juga meningkatkan kepercayaan masyarakat,

memperkuat daya saing, dan menciptakan inovasi yang berkelanjutan. Bagi auditor internal, *digital trust* menjadi salah satu area *assurance* yang semakin penting karena berkaitan langsung dengan keberlangsungan organisasi di era digital.

Inti dari materi ini adalah bahwa teknologi saja tidak cukup untuk memenangkan kepercayaan publik. Kepercayaan dibangun melalui kombinasi antara kepemimpinan, budaya organisasi, pengendalian internal, tata kelola teknologi informasi, serta komitmen terhadap perlindungan data dan keamanan siber. Oleh karena itu, pembangunan *digital trust* harus menjadi bagian dari strategi organisasi, bukan sekadar proyek teknologi informasi. Dengan demikian, organisasi dapat memanfaatkan peluang ekonomi digital sekaligus meminimalkan risiko yang muncul dalam ruang digital global.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Alif dari Bank Tabungan Negara/BTN)

Terkait *digital trust*, dari pemerintah Indonesia apakah sudah ada *rating digital trust* untuk perusahan-perusahaan di Indonesia karena bank sangat membutuhkan itu untuk pertimbangan saat kerjasama *business to business* terutama dalam membangun teknologi digital kami.

Jawaban:

Hingga saat ini Indonesia belum memiliki *rating digital trust* nasional yang secara khusus menilai tingkat kepercayaan digital suatu organisasi. Namun demikian, berbagai parameter pendukung sebenarnya telah tersedia, misalnya penilaian keamanan siber (*cybersecurity*) yang diterbitkan oleh lembaga internasional maupun oleh Badan Siber dan Sandi Negara (BSSN). Ke depan, parameter-parameter tersebut dapat menjadi dasar untuk membangun sistem *rating digital trust* di Indonesia.

Digital trust sangat dipengaruhi oleh transparansi organisasi dalam mengelola data dan sistem informasinya. Organisasi harus mampu menjelaskan tata kelola data, proses bisnis, serta mekanisme perlindungan keamanan informasi yang diterapkan. Selain itu, penerapan standar seperti ISO/IEC 27001 dan publikasi sertifikasi tersebut dapat menjadi salah satu indikator yang meningkatkan kepercayaan para pemangku kepentingan.

Ke depan, pengembangan Indeks Pemerintah Digital (Pem-D) diharapkan dapat menjadi salah satu referensi dalam mengukur tata kelola digital, termasuk aspek *Enterprise Architecture*, *roadmap* teknologi informasi, tata kelola keamanan (*security*), dan komponen tata kelola digital lainnya. Untuk BUMN maupun perusahaan swasta, mekanisme penilaian

serupa masih memerlukan pengembangan lebih lanjut. Di sisi lain, seluruh Penyelenggara Sistem Elektronik (PSE) telah diwajibkan mendaftar ke Kementerian Komunikasi dan Digital (Komdigi), sehingga pada tahap berikutnya asesmen terhadap penyelenggara sistem elektronik dapat dikembangkan menjadi dasar penyusunan *rating digital trust*.

Pertanyaan 2 (Ibu Waskita Rini dari PT Berdikari):

Apakah *digital trust* dapat diukur secara kuantitatif? Jika ya, indikator apa yang paling tepat untuk menilai tingkat kepercayaan masyarakat terhadap layanan digital suatu organisasi?

Jawaban:

Digital trust pada prinsipnya dapat diukur melalui berbagai indikator tata kelola digital. Beberapa parameter yang dapat digunakan antara lain tingkat kematangan tata kelola data, penerapan standar keamanan informasi, kepatuhan terhadap regulasi, transparansi proses bisnis, kualitas pengelolaan risiko siber, serta penerapan standar internasional seperti ISO/IEC 27001.

Apabila ke depan Indonesia memiliki sistem *rating digital trust*, indikator-indikator tersebut dapat diintegrasikan menjadi suatu mekanisme penilaian yang memberikan gambaran mengenai tingkat kepercayaan terhadap suatu layanan digital. Dengan demikian, masyarakat maupun organisasi akan memiliki dasar yang lebih objektif dalam menentukan tingkat kepercayaan terhadap penyelenggara layanan digital.

TRACK 2-B

Continuous Auditing & Continuous Assurance

Dr. Hery Subowo, SE, MPM, Ak.
Staf Ahli Bidang Manajemen Risiko - Badan Pemeriksa Keuangan RI

ABSTRAK

Perkembangan teknologi digital telah mengubah paradigma audit internal dari pendekatan periodik menuju pengawasan yang bersifat berkelanjutan (*continuous*), berbasis data, dan didukung teknologi digital. Organisasi tidak lagi cukup mengandalkan audit yang dilakukan secara berkala setelah suatu aktivitas selesai, tetapi memerlukan mekanisme pemantauan, evaluasi, dan pemberian *assurance* secara terus-menerus agar risiko dapat diidentifikasi dan dimitigasi sedini mungkin. Konsep *Continuous Auditing* dan *Continuous Assurance* menjadi bagian penting dalam transformasi fungsi audit internal yang memanfaatkan *big data analytics*, *artificial intelligence*, *real-time dashboard*, *robotic process automation*, dan integrasi sistem untuk meningkatkan efektivitas pengawasan. Materi ini membahas konsep *continuous monitoring*, *continuous auditing*, dan *real-time assurance* beserta perbedaan konseptual maupun implementasinya, keterkaitannya dengan *Global Internal Audit Standards (GIAS) 2024*, tantangan implementasi dari aspek teknologi, sumber daya manusia, budaya, dan tata kelola, berbagai praktik baik (*good practices*) dalam pemantauan transaksi, risiko, pengendalian, serta analitik data, faktor-faktor keberhasilan implementasi, dan kontribusi setiap lini dalam *Three Lines Model*. Penerapan *Continuous Auditing* dan *Continuous Assurance* diharapkan mampu meningkatkan kualitas *assurance*, mempercepat pengambilan keputusan, memperkuat tata kelola, mendeteksi *fraud* secara lebih dini, serta menciptakan nilai tambah yang berkelanjutan bagi organisasi.

Kata Kunci: *Continuous Auditing, Continuous Assurance, Real-Time Assurance*

PEMBAHASAN

Transformasi digital telah mengubah secara fundamental cara organisasi menjalankan fungsi pengawasan dan audit internal. Pendekatan audit tradisional yang bersifat periodik dan berfokus pada pengujian setelah suatu aktivitas selesai dinilai tidak lagi memadai dalam menghadapi lingkungan bisnis yang bergerak cepat, kompleks, dan menghasilkan data dalam jumlah sangat besar. Oleh karena itu, fungsi audit internal juga mengalami transformasi melalui penerapan *Continuous Auditing* dan *Continuous Assurance* yang memanfaatkan teknologi digital, *big data analytics*, *artificial intelligence* (AI), *real-time dashboard*, serta *Data Analytics Center of Excellence*. Transformasi tersebut merupakan bagian dari praktik terbaik audit internal modern yang juga mencakup penguatan tata kelola, *ESG assurance*, *Fraud Risk*

Management, penguatan *Internal Control over Financial Reporting* (ICoFR), serta peningkatan peran auditor internal sebagai *strategic business partner*.

Implementasi *Continuous Auditing* tidak dapat dipisahkan dari konsep *Continuous Monitoring* dan *Real-Time Assurance* karena ketiganya memiliki fungsi yang saling melengkapi dalam sistem pengawasan organisasi. *Continuous Monitoring* dilaksanakan oleh lini pertama dan lini kedua melalui pemantauan berkelanjutan terhadap transaksi, proses bisnis, indikator kinerja, risiko, dan pengendalian untuk mendeteksi penyimpangan sejak dini. Selanjutnya, auditor internal sebagai lini ketiga melaksanakan *Continuous Auditing* dengan memanfaatkan analitik data, AI, dan pengujian terhadap seluruh populasi data untuk memberikan penilaian independen atas efektivitas pengendalian maupun proses pemantauan yang dilakukan manajemen. Pada tingkat yang lebih maju, *Real-Time Assurance* memungkinkan auditor memberikan keyakinan secara langsung ketika aktivitas sedang berlangsung sehingga tindakan korektif dapat dilakukan sebelum risiko berkembang menjadi kerugian yang lebih besar.

Penerapan *Continuous Monitoring*, *Continuous Auditing*, dan *Continuous Assurance* dapat dilakukan pada berbagai objek pengawasan dalam organisasi. Pada area transaksi, sistem mampu melakukan pemantauan transaksi secara *real-time*, mendeteksi transaksi anomali, *duplicate payment*, aktivitas di luar jam operasional, maupun lonjakan volume transaksi yang tidak wajar. Pada pengelolaan *master data*, pemantauan dilakukan terhadap validitas data pelanggan, perubahan data vendor, integritas identitas, serta konsistensi data lintas sistem. Sementara itu, pada aspek *fraud* dan kepatuhan, organisasi dapat mengembangkan *Fraud Detection System*, *dashboard fraud*, pemantauan *Anti-Money Laundering/Anti Pendanaan Terorisme* (AML/APU-PPT), *whistleblowing system*, serta penerapan autentikasi biometrik dan prinsip *zero trust* untuk memperkuat keamanan sistem.

Pendekatan pengawasan berkelanjutan juga diterapkan pada proses bisnis dan pengelolaan risiko organisasi. Audit tidak lagi terbatas pada pemeriksaan lapangan, tetapi dapat dilakukan melalui *desk audit* berbasis analisis data, pemantauan *Key Performance Indicator* (KPI), pengawasan piutang (*days sales outstanding*), monitoring proyek yang sedang berjalan, serta *probity audit* yang dilakukan selama proses berlangsung. Pada sisi manajemen risiko, organisasi dapat mengembangkan *dashboard* risiko, *continuous control monitoring*, *automated exception monitoring*, *early warning system*, dan pemantauan faktor-faktor penggerak risiko (*risk driver monitoring*). Keseluruhan mekanisme tersebut didukung oleh *big data analytics*, AI, integrasi *application programming interface* (API), *robotic process automation* (RPA), dan *dashboard* audit yang memungkinkan proses *assurance* berlangsung secara cepat dan berbasis data.

Dalam perspektif standar profesi, *Global Internal Audit Standards* (GIAS) 2024 memang tidak secara khusus mengatur satu standar mengenai *Continuous Auditing*. Namun, konsep tersebut tersebar dalam berbagai standar yang menekankan pentingnya fungsi audit internal yang adaptif, berbasis risiko, dan didukung teknologi. GIAS mengharuskan *Chief Audit Executive* (CAE) untuk melakukan pemantauan risiko secara berkelanjutan dan menyesuaikan rencana audit sesuai perkembangan organisasi. Selain itu, fungsi audit internal didorong memanfaatkan teknologi, *data analytics*, dan otomatisasi sebagai *enabler* utama pelaksanaan audit yang lebih efektif, sekaligus menerapkan pendekatan *Agile Auditing* melalui *rolling risk assessment*, *continuous monitoring*, *continuous auditing*, serta *Quality Assurance and Improvement Program* (QAIP). Integrasi seluruh komponen tersebut pada akhirnya diarahkan untuk menghasilkan *Continuous Assurance* yang memberikan nilai tambah lebih besar bagi organisasi.

Meskipun menawarkan berbagai manfaat, implementasi *Continuous Auditing* masih menghadapi sejumlah tantangan. Dari sisi teknologi, organisasi masih menghadapi fragmentasi data (*data silo*), integrasi sistem yang belum optimal, kualitas data yang belum memadai, serta belum tersedianya *single source of truth* maupun *early warning system* yang andal. Dari sisi sumber daya manusia, kompetensi auditor dalam bidang analitik data, AI, dan audit teknologi informasi masih perlu ditingkatkan melalui pelatihan dan pengembangan kapasitas. Tantangan budaya juga muncul dalam bentuk resistensi terhadap transformasi digital, ketergantungan pada pendekatan audit tradisional berbasis *sampling*, rendahnya kepercayaan terhadap AI, serta belum optimalnya kolaborasi antar *Three Lines*. Di samping itu, implementasi masih memerlukan kerangka tata kelola yang seragam, pengelolaan risiko AI, serta investasi teknologi yang tidak sedikit.

Apabila diterapkan secara efektif, *Continuous Auditing* dan *Continuous Assurance* memberikan berbagai manfaat strategis bagi organisasi. Pengawasan yang dilakukan secara berkelanjutan memungkinkan deteksi dini terhadap *fraud*, transaksi mencurigakan, penyimpangan proyek, manipulasi laporan keuangan, serta berbagai bentuk anomali operasional sebelum berkembang menjadi kerugian yang signifikan. Pendekatan ini juga meningkatkan keandalan pelaporan keuangan melalui validasi berkelanjutan terhadap *red flags*, mempercepat respons organisasi terhadap risiko operasional maupun siber melalui *early warning system*, meningkatkan efektivitas audit melalui otomatisasi dan pengujian seluruh populasi data, memperkuat perlindungan aset organisasi, serta mendorong perubahan budaya pengawasan dari pendekatan yang reaktif (*post-audit*) menjadi lebih proaktif, prediktif, dan adaptif. Dampak akhirnya adalah meningkatnya resiliensi organisasi, penguatan tata kelola, serta terciptanya *sustainable value*.

Keberhasilan implementasi *Continuous Auditing* ditentukan oleh sejumlah faktor kunci yang saling berkaitan. Organisasi harus memiliki data yang berkualitas, teknologi yang terintegrasi, kerangka kerja analitik yang kuat, serta sumber daya manusia yang memiliki kompetensi dalam *data analytics* dan analisis risiko. Implementasi juga perlu difokuskan pada area yang memiliki risiko tinggi, diintegrasikan ke seluruh siklus audit mulai dari perencanaan hingga pelaporan, serta didukung komitmen manajemen dalam penyediaan investasi dan pengembangan kapabilitas. Selain itu, keberhasilan hanya dapat dicapai apabila organisasi membangun budaya kerja berbasis data, menerapkan tata kelola AI yang memperhatikan aspek keamanan, privasi, etika, dan mitigasi bias, serta menjaga kejelasan pembagian peran sesuai *Three Lines Model*. Dalam model tersebut, lini pertama bertanggung jawab melaksanakan *continuous monitoring*, lini kedua mengembangkan metodologi dan melakukan pengawasan risiko, lini ketiga memberikan *independent assurance* melalui *Continuous Auditing* dan *Real-Time Assurance*, sedangkan *governing body* menggunakan hasil *assurance* sebagai dasar pengambilan keputusan strategis dan penguatan tata kelola organisasi.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Alexander dari BPOM)

Dalam implementasi *Continuous Auditing*, banyak proses bisnis di instansi kami yang datanya belum tersedia secara *real-time*. Dengan kondisi tersebut, bagaimana *Continuous Auditing* dapat diterapkan secara efektif?

Jawaban:

Continuous Auditing tidak harus menunggu seluruh data organisasi tersedia secara *real-time*. Implementasinya dapat dilakukan secara bertahap sesuai tingkat kematangan digital organisasi. Tahap awal dapat dimulai dengan membangun *continuous monitoring* pada proses bisnis yang datanya sudah terdigitalisasi, kemudian secara bertahap memperluas cakupan seiring meningkatnya integrasi sistem dan kualitas data. Yang terpenting adalah memastikan kualitas data, membangun mekanisme *data governance*, serta mengembangkan indikator risiko dan pengendalian yang dapat dipantau secara berkelanjutan. Seiring berkembangnya transformasi digital, frekuensi dan cakupan *Continuous Auditing* akan semakin meningkat hingga mampu mendekati *real-time assurance*.

Pertanyaan 2 (Ibu Dirga dari PT Bank Mandiri Persero):

Dalam penerapan *Continuous Auditing*, bagaimana auditor dapat mengidentifikasi *root cause* apabila organisasi memiliki jutaan transaksi setiap hari (contoh pada Bank Mandiri terdapat jutaan transaksi setiap harinya)? Bukankah kondisi tersebut justru membuat proses analisis menjadi semakin kompleks?

Jawaban:

Tujuan *Continuous Auditing* bukan untuk menelusuri seluruh transaksi secara manual, melainkan memanfaatkan *data analytics*, *artificial intelligence* (AI), dan *rule-based monitoring* untuk menyaring transaksi yang mengandung anomali atau memiliki indikator risiko tertentu. Auditor kemudian memfokuskan analisis pada transaksi-transaksi yang telah ditandai (*flagged transactions*) sehingga proses identifikasi *root cause* menjadi lebih efektif dan efisien. Dengan pendekatan tersebut, auditor tidak lagi menghabiskan waktu untuk memilih sampel transaksi, tetapi lebih berfokus pada analisis penyebab utama, evaluasi efektivitas pengendalian, serta penyusunan rekomendasi perbaikan yang bersifat preventif dan memberikan nilai tambah bagi organisasi.

PANEL DISCUSSION – 3

Empowering Internal Auditors to Navigate Emerging Cyber Risks: Governance 5.0 and Cyber Resilience

Yulianto Setiawan
SEVP Satuan Kerja Audit Intern, PT Bank Rakyat Indonesia (Persero) Tbk.
Taufikurrahman
Country Ambassador, Sagana Capital; Member of British Chamber of Commerce in Indonesia; Head of Policy Research HIPPG FIA Universitas Indonesia; Dosen Binus University
Ishfihana Hafny Noer
VP Portfolio & Emerging Risk Management, PT Pertamina (Persero)

ABSTRAK

Tiga narasumber memaparkan bagaimana transformasi digital yang masif, implementasi kecerdasan buatan (AI), dan interkoneksi ekosistem bisnis telah membawa perubahan fundamental pada lanskap risiko korporasi, menggeser *cyber risk* dari sekadar masalah teknis TI menjadi risiko strategis tingkat perusahaan (*enterprise risk* dan *boardroom*). Diskusi ini menyoroti lonjakan eksponensial insiden siber di Indonesia dan dunia, kerentanan rantai pasok digital pihak ketiga, ancaman deepfake serta social engineering berbasis AI, hingga adanya kesenjangan (*assurance gap*) antara persepsi risiko dengan alokasi rencana audit operasional organisasi. Para narasumber sepakat bahwa dalam membangun ketahanan siber (*cyber resilience*) yang berkelanjutan, fungsi audit internal harus bertransformasi dari sekadar pemeriksa kepatuhan tradisional (*compliance checker*) menjadi penasihat risiko strategis (*strategic risk advisor* atau *trusted advisor*). Hal ini dicapai melalui restrukturisasi pengawasan menggunakan The IIA Three Lines Model yang adaptif, penguatan kapabilitas *cybersecurity risk assessment*, penguasaan standar global seperti NIST *Cybersecurity Framework*, serta penerapan continuous auditing berbasis data.

Kata Kunci: *Governance 5.0, Cyber resilience, Internal Audit, Human Firewall, Three Lines Model, Emerging Risk, NIST CSF*

PEMBAHASAN

Evolusi Lanskap Ancaman dan Pergeseran Paradigma *Cyber Risk* Menjadi Risiko Strategis Enterprise

Era *Governance 5.0* ditandai oleh transformasi digital yang masif, ekspansi kecerdasan buatan (*Artificial Intelligence*), serta hiperkonektivitas melalui *Cloud Computing*, IoT, dan API. Dinamika ini secara fundamental mengubah lanskap risiko korporasi lintas industri, baik perbankan, energi, maupun sektor strategis lainnya, di mana *cyber risk* telah bermutasi dari sekadar masalah teknis TI menjadi risiko strategis tingkat perusahaan (*Enterprise and Boardroom Risk*). Transformasi ini tercermin nyata dalam sektor perbankan yang kini

berevolusi menuju *Bank 5.0 (intelligent banking)*. Mengutip pemikiran Brett King, industri perbankan masa kini pada hakikatnya adalah perusahaan teknologi yang kebetulan memiliki lisensi perbankan (*"Bank is a technology company with a banking license"*). Evolusi ini menggeser profil ancaman konvensional seperti pemalsuan cek, *card skimming*, dan *data breach* berbasis *phishing*, menjadi ancaman mutakhir berupa *API risk, third-party risk*, hingga kejahatan siber berbasis AI dan manipulasi biometrik. Konteks risiko ini menjadi sangat kritikal jika melihat skala operasi institusi besar seperti PT Bank Rakyat Indonesia (Persero) Tbk. yang per Kuartal I-2026 mengelola lebih dari 167 juta nasabah, 47 juta pengguna BRImo, dan 4,6 juta titik QRIS, di mana ketahanan siber menjadi pilar mutlak untuk menjaga kepercayaan publik (*trust*).

Data empiris global dari *Allianz Risk Barometer 2026* mempertegas urgensi ini dengan menempatkan *cyber risk* sebagai risiko bisnis nomor satu di dunia (42%) dan memuncaki peringkat di kawasan Asia Pasifik (36%). Di Indonesia, eskalasi ancaman ini terekam lewat catatan Badan Siber dan Sandi Negara (BSSN) yang mendeteksi 5,5 miliar serangan siber sepanjang tahun 2025, sebuah lonjakan eksponensial sebesar 714% dibanding rata-rata periode 2020–2024. Dampak dari serangan siber modern ini tidak lagi sekadar gangguan operasional sesaat, melainkan kerugian finansial langsung, tuntutan hukum, denda regulasi, hingga kehancuran reputasi korporasi secara permanen. Total kerugian nasional di Indonesia akibat *fraud* berbasis AI diperkirakan telah menembus Rp700 miliar, dengan sektor perbankan sebagai sasaran utama. Fakta-fakta ini diperkuat oleh dokumen *KPMG 2025 CEO Outlook* yang menegaskan bahwa *data & information governance, AI technology*, serta *cybersecurity* kini menempati tiga fokus investasi teratas bagi dewan direksi global. Kerentanan tata kelola ini semakin kompleks akibat tantangan rantai pasok digital (*digital supply chain*) pihak ketiga yang diidentifikasi oleh 78% organisasi, keterbatasan alokasi dana (63%), dan kelangkaan talenta siber yang kompeten (56%).

Pelajaran berharga dari berbagai kegagalan teknologi berskala besar dunia, mulai dari kasus *SolarWinds (2020), Colonial Pipeline (2021), Uber (2022), MOVEit (2023), Change Healthcare (2024)*, hingga gangguan sistem global *CrowdStrike (2024)* membuktikan secara nyata tingginya risiko konsentrasi teknologi saat ini. Salah satu fenomena paling mengkhawatirkan di era digital-first ini adalah kemunculan *emerging cyber risks*. Merujuk pada standar *ISO/TS 31050*, *emerging risk* diidentifikasi sebagai risiko yang belum pernah dikenali sebelumnya atau berkembang sangat cepat dengan tingkat ketidakpastian dan dampak yang sangat tinggi (*high uncertainty, high impact*). Terdapat enam pendorong utama *emerging risk* saat ini: serangan siber berbasis AI, *deepfake social engineering, shadow AI* (penggunaan alat AI di luar tata kelola resmi), ancaman komputasi *post-quantum* terhadap metode enkripsi

konvensional, volatilitas regulasi perlindungan data lintas negara, serta kerentanan inheren pada ekosistem pihak ketiga.

Ancaman spekulatif berbasis *deepfake* dan rekayasa sosial ini bukan lagi sekadar teori, melainkan bahaya nyata yang telah melumpuhkan sistem kontrol internal korporasi. Sebagai contoh, kasus penipuan siber yang menimpa perusahaan global Arup di Hong Kong mengakibatkan kerugian sebesar US$25 juta. Melalui skenario *video conference* palsu yang memanfaatkan manipulasi wajah dan suara digital (rekayasa sosial berbasis AI) yang menyerupai CFO dan rekan kerja, korban diinstruksikan untuk melakukan 15 kali transfer dana. Kasus luar biasa ini membuktikan bahwa kontrol internal konvensional dapat lumpuh total tanpa adanya peretasan infrastruktur siber secara langsung, melainkan melalui manipulasi faktor psikologis dan kepercayaan manusia. Tidak heran jika *Gartner* menempatkan *cybersecurity vulnerabilities, data governance*, dan *regulatory compliance* sebagai tiga area risiko teratas dalam rencana *assurance* tahun 2026.

Kesenjangan Audit (*Assurance gap*) dan Penguatan Komponen Manusia (Human Firewall)

Meskipun infrastruktur teknologi terus diperkuat dengan biaya besar, faktor manusia tetap disepakati sebagai titik lemah utama sekaligus benteng pertahanan terdepan melalui konsep *human firewall*. Data menunjukkan bahwa sekitar 62% pelanggaran keamanan siber melibatkan unsur kelalaian manusia, di mana tingkat keberhasilan serangan *phishing* yang dirancang oleh AI mencapai 54%, jauh mengungguli *phishing* konvensional yang hanya mencatat tingkat keberhasilan 12%. Realitas ini menunjukkan adanya kesenjangan yang lebar (*assurance gap*) di dalam organisasi: meskipun *cybersecurity* diakui sebagai lima risiko teratas oleh 86% *Chief Audit Executive (CAE)*, alokasi rencana audit operasional khusus untuk keamanan siber secara umum baru menyerap 9% kapasitas audit, tertinggal jauh di bawah porsi audit operasional (17%) dan laporan keuangan (16%).

Untuk menjembatani kesenjangan kepastian (*assurance gap*), kesenjangan keyakinan (*confidence gap*), dan kesenjangan kompetensi (*capability gap*) tersebut, auditor internal tidak boleh lagi bertindak sekadar sebagai pemeriksa kepatuhan administratif dasar (*compliance checker*). Fungsi audit internal harus bertransformasi secara radikal menjadi penasihat risiko strategis (*strategic risk advisor* atau *trusted advisor*). Auditor internal wajib menguasai tujuh kapabilitas kunci yang diselaraskan dengan standar global seperti *NIST Cybersecurity Framework (CSF) 2.0*, yang mencakup fungsi *Govern, Identify, Protect, Detect, Respond*, dan *Recover*. Fokus kapabilitas baru ini meliputi pelaksanaan *cybersecurity risk assessment*, audit vendor pihak ketiga, pengelolaan insiden, hingga pemanfaatan *data analytics*. Dengan demikian, pemahaman mendalam dikembangkan bahwa sistem keamanan terkuat bukanlah

sistem yang terpasang di *data center*, melainkan yang tertanam dalam pola pikir dan kesadaran siber setiap pegawai.

Restrukturisasi Tata Kelola AI, Peran Kerja Lintas Fungsi, dan Continuous Assurance

Menghadapi lansekap ancaman yang dinamis ini, tata kelola siber organisasi wajib diatur secara ketat dengan mengacu pada kerangka kerja *The IIA Three Lines Model*. Dalam model ini, lini pertama (manajemen operasi dan IT) bertindak sebagai pemilik risiko (*risk owner*); lini kedua (manajemen risiko dan kepatuhan) berfungsi melakukan pemantauan, penyusunan kebijakan, dan pengawasan; sedangkan lini ketiga (audit internal) memberikan kepastian independen (*independent assurance*) secara objektif langsung kepada dewan komisaris dan komite audit. Restrukturisasi pengawasan dewan (*board oversight*) yang kokoh menjadi mutlak agar risiko-risiko kritikal seperti *ransomware-as-a-service*, penipuan berbasis *deepfake*, dan ancaman rantai pasok masuk secara eksplisit dalam rencana audit formal organisasi.

Dalam konteks tata kelola teknologi baru, AI diposisikan sebagai pedang bermata dua; di satu sisi AI memperkuat sistem deteksi pertahanan, namun di sisi lain menjadi pengganda kekuatan (*force multiplier*) bagi penyerang untuk menciptakan *automated social engineering* yang masif. Oleh karena itu, auditor internal didorong untuk menggunakan standar seperti *NIST AI Risk Management Framework 1.0* (meliputi pilar *Govern, Map, Measure, Manage*) guna menilai independensi model AI, perlindungan data privasi, serta aspek akuntabilitas dan penjelasan kecerdasan buatan (*explainability*).

Lebih lanjut, fungsi audit internal wajib menerapkan lima langkah penilaian risiko siber yang terintegrasi penuh dengan *Enterprise risk Management (ERM)*:

1. Identifikasi aset kritikal dan layanan bisnis utama organisasi.
2. Penilaian skenario ancaman siber secara dinamis.
3. Evaluasi efektivitas kontrol preventif dan detektif yang ada.
4. Pengujian ketahanan operasional pemulihan (*incident response & recovery*).
5. Pemantauan indikator risiko siber secara berkelanjutan.

Transformasi metodologi audit akhirnya diarahkan untuk bergerak meninggalkan pendekatan audit periodik tradisional (tahunan) menuju ke arah *continuous cyber assurance*. Dengan memanfaatkan pengawasan *real-time*, teknik *continuous auditing*, dan dasbor risiko terintegrasi, profesi audit internal dapat melahirkan profil *T-shaped auditor,* yaitu para profesional yang tidak hanya memahami aspek bisnis organisasi secara mendalam, tetapi juga menguasai tata kelola teknologi dan ketahanan siber secara komprehensif demi mengawal keberlanjutan korporasi di era *Governance 5.0*.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Bimantara dari PT Sarana Multi Infrastruktur):

Ketika organisasi telah melakukan *strategic foresight* sesuai SOP yang dimiliki, namun output yang dihasilkan berbeda-beda, bagaimana posisi seorang auditor dalam menyikapi kondisi tersebut?

Jawaban:

Perbedaan output tersebut merupakan salah satu konsekuensi dari lingkungan VUCA (*Volatility, Uncertainty, Complexity, Ambiguity*) yang dapat menimbulkan efek berantai (*contingent effect*) ke berbagai lini organisasi. Sebagai ilustrasi, sektor keuangan secara rutin melakukan *stress test* untuk mengantisipasi berbagai skenario *contingent effect*, mengingat sumber ketidakpastian bukan hanya berasal dari satu faktor, melainkan juga dari dinamika perubahan teknologi yang semakin cepat serta munculnya modus kejahatan (*fraud*) baru. Ketika *strategic plan* yang telah disusun berhadapan dengan perubahan yang berlangsung sangat cepat, organisasi perlu melakukan penyesuaian (revisi) *strategic plan* secara berkala, di mana manajemen puncak (CEO) harus secara kritis mengevaluasi kembali berbagai asumsi yang mendasari perencanaan tersebut. Dalam hal ini, auditor internal berperan memastikan bahwa proses *foresight* dan perencanaan strategis telah memanfaatkan *data analytics* dan AI dalam *modeling analysis* secara memadai, didukung oleh teknologi dan *key capability* yang dimiliki organisasi. Auditor juga perlu mendorong penerapan *budgeting*, *planning*, dan *foresight* yang berbasis data (*data-driven*) secara konsisten, agar output perencanaan strategis tidak menyesatkan (*misleading*) dan tetap dapat diandalkan sebagai dasar pengambilan keputusan di tengah ketidakpastian.

Pertanyaan 2 (Bapak Rustam dari PT BRI):

Bagaimana insight penerapan *Artificial Intelligence* (AI) di fungsi Internal Audit PT Pertamina (Persero) saat ini, dan apa contoh rekomendasi prediktif yang dihasilkan dari proses AI tersebut dalam mendukung pekerjaan Internal Audit?

Jawaban:

Penerapan AI di PT Pertamina (Persero) saat ini masih berjalan dalam konteks *enterprise* secara luas, namun pemanfaatannya terbuka untuk digunakan oleh fungsi Internal Audit maupun unit-unit lain di dalam organisasi. Kunci keberhasilan pemanfaatan AI tersebut terletak pada kesiapan data (*data readiness*): bagaimana Internal Audit memastikan data yang akan diolah bersih (*clean*), terstruktur, dan valid, sehingga mampu mendukung proses *continuous auditing & analytics* dalam menghasilkan dokumentasi kerja audit maupun output

analitis lainnya secara akurat. Tanpa kualitas data yang memadai, hasil prediktif atau *insight* yang dihasilkan AI berisiko menyesatkan pengambilan keputusan. Hal ini sejalan dengan salah satu *capability gap* yang menjadi tantangan utama Internal Audit, yaitu kebutuhan akan kapabilitas *data analytics* dan *AI expertise* yang terus meningkat sebagai fondasi bagi Internal Audit untuk bertransformasi dari sekadar *risk-based assurance* menjadi *insight & foresight provider* yang mampu menghasilkan rekomendasi prediktif dan nilai tambah strategis bagi manajemen.

GENERAL SESSION 3

Governance 5.0 and the Future of Public Sector Leadership: Governing Complexity in a Digital and Data-Driven Era

Dr. Nyoman Adhi Suryadnyana, S.E., M.E., M.Ak., QIA

Anggota I Badan Pemeriksa Keuangan Republik Indonesia

ABSTRAK

Transformasi digital telah mengubah kompleksitas tata kelola sektor publik secara fundamental. Pengambilan keputusan tidak lagi hanya bergantung pada struktur birokrasi dan prosedur administratif, tetapi juga pada kualitas data, keandalan sistem digital, keamanan informasi, serta tingkat kepercayaan masyarakat terhadap institusi publik. Kondisi tersebut mendorong lahirnya paradigma *Governance 5.0* sebagai pendekatan tata kelola yang adaptif, terintegrasi, transparan, berbasis data, dan berorientasi pada penciptaan nilai publik yang berkelanjutan. Materi ini membahas urgensi transformasi kepemimpinan sektor publik dalam menghadapi kompleksitas era digital, penguatan tata kelola berbasis data, pemanfaatan *artificial intelligence* (AI) dan *data analytics* untuk mendukung pengambilan keputusan, pentingnya *cyber security* sebagai fondasi keandalan sistem pemerintahan, pembangunan *digital trust* dan akuntabilitas algoritmik, serta karakter kepemimpinan yang inovatif, resilien, dan responsif. Keseluruhan konsep tersebut menegaskan bahwa keberhasilan *Governance 5.0* tidak ditentukan oleh teknologi semata, melainkan oleh kemampuan pemimpin sektor publik dalam mengintegrasikan tata kelola yang baik, pemanfaatan teknologi secara bertanggung jawab, dan orientasi pada kepentingan masyarakat.

Kata Kunci: *Governance 5.0,* Kepemimpinan Sektor Publik, *Data Analytics*

PEMBAHASAN

Perkembangan teknologi digital telah mengubah lanskap tata kelola sektor publik secara signifikan. Kompleksitas pemerintahan saat ini tidak lagi hanya dipengaruhi oleh struktur organisasi maupun regulasi, tetapi juga oleh kualitas data, keandalan sistem digital, risiko lintas sektor, serta tingkat kepercayaan masyarakat terhadap institusi publik. Model tata kelola tradisional yang bersifat hierarkis, linier, dan berorientasi pada kepatuhan administratif semakin menghadapi keterbatasan dalam merespons tantangan yang berkembang dengan cepat. Oleh karena itu, *Governance 5.0* hadir sebagai paradigma baru yang menekankan tata kelola yang antisipatif, terintegrasi, terpercaya, dan berkelanjutan dengan mengedepankan

prinsip integritas, transparansi, akuntabilitas, partisipasi, inovasi, kolaborasi, dan orientasi hasil.

Perubahan tersebut menuntut transformasi kepemimpinan sektor publik. Kepemimpinan tidak lagi semata-mata bertumpu pada kewenangan formal, tetapi harus mampu membangun kepercayaan, mengelola risiko, serta mengambil keputusan berdasarkan bukti dan data yang akurat. Orientasi kepemimpinan bergeser dari pendekatan administratif menuju pendekatan berbasis risiko, dari pengambilan keputusan yang mengandalkan intuisi menuju keputusan berbasis data, serta dari kepemimpinan sektoral menuju kepemimpinan kolaboratif yang mampu menyatukan berbagai pemangku kepentingan. Selain itu, pemimpin sektor publik juga dituntut menjadi pembelajar yang terus mengembangkan kompetensinya agar mampu mengikuti dinamika teknologi dan perubahan lingkungan strategis. Transformasi kepemimpinan tersebut menjadi fondasi bagi terwujudnya tata kelola yang kuat, didukung teknologi yang andal, sumber daya manusia yang kompeten, keputusan yang berkualitas, risiko yang terkendali, dan pelayanan publik yang semakin baik.

Implementasi *Governance 5.0* dibangun di atas tiga pilar utama, yaitu adaptif, transparan, dan berbasis data. Pilar adaptif menekankan kemampuan organisasi dalam membaca perubahan lingkungan, mengantisipasi risiko, serta melakukan perbaikan kebijakan secara berkelanjutan berdasarkan hasil analisis data. Pilar transparansi menegaskan bahwa proses dan dasar pengambilan keputusan harus dapat dijelaskan kepada publik sehingga tidak menciptakan *black box* dalam pelayanan pemerintah. Sementara itu, pilar berbasis data mengharuskan seluruh keputusan didasarkan pada data yang akurat, mutakhir, aman, dan dapat ditelusuri, sehingga kebijakan publik memiliki dasar yang objektif dan dapat dipertanggungjawabkan. Teknologi dalam konteks ini bukan merupakan tujuan akhir, melainkan instrumen untuk meningkatkan kualitas pelayanan dan memperkuat akuntabilitas pemerintahan.

Keputusan publik yang berkualitas hanya dapat dihasilkan apabila organisasi mampu mengelola data secara baik sepanjang siklus hidupnya. Data tidak lagi dipandang sekadar sebagai bahan penyusunan laporan, melainkan sebagai dasar dalam mengevaluasi kebijakan, mengidentifikasi risiko, mempercepat respons terhadap kebutuhan masyarakat, serta meningkatkan efektivitas program pemerintah. Pemanfaatan *data analytics* memungkinkan pemerintah mendeteksi belanja yang tidak wajar, memetakan risiko penerimaan, mengidentifikasi pola *fraud*, mengevaluasi efektivitas program, dan mempercepat penyelesaian berbagai permasalahan publik. Di sisi lain, AI dapat dimanfaatkan untuk mengelompokkan dokumen, membaca pola pengaduan masyarakat, memprediksi kebutuhan layanan, serta mendeteksi anomali yang memerlukan tindak lanjut lebih lanjut.

Namun demikian, kualitas keputusan tetap sangat bergantung pada kualitas data yang digunakan sebagai dasar analisis.

Pemanfaatan AI dan *data analytics* juga membawa implikasi terhadap tata kelola dan proses audit sektor publik. Auditor tidak lagi cukup berfokus pada hasil akhir berupa laporan keuangan atau laporan kinerja, tetapi perlu menelusuri keseluruhan *data lifecycle*, mulai dari proses data dihasilkan, diproses, disimpan, diubah, direkonsiliasi, hingga dilaporkan. Kelemahan pada salah satu tahapan tersebut dapat mengakibatkan kesalahan analisis, meningkatnya risiko salah saji, *fraud*, maupun menurunnya akuntabilitas organisasi. Oleh karena itu, AI harus diposisikan sebagai alat bantu dalam mendukung proses analisis, sedangkan tanggung jawab akhir atas keputusan tetap berada pada manusia dan institusi publik yang memiliki mandat.

Selain kualitas data, keamanan informasi menjadi prasyarat utama dalam menghasilkan keputusan publik yang tepat. Sistem digital yang tampak berjalan dengan baik belum tentu menghasilkan informasi yang andal apabila integritas data tidak terjaga. Serangan siber berpotensi menyebabkan data dicuri, diubah, dihapus, atau tidak tersedia ketika dibutuhkan sehingga mengganggu kualitas analisis dan menghasilkan keputusan yang keliru. Oleh sebab itu, *cyber security* tidak hanya dipandang sebagai isu teknologi, tetapi merupakan bagian integral dari tata kelola publik. Penguatan keamanan informasi dilakukan melalui perlindungan integritas data, peningkatan keandalan sistem, pengendalian akses, *audit trail*, *backup* dan *disaster recovery*, pengelolaan perubahan sistem, serta respons insiden yang efektif. Seluruh pengendalian tersebut menjadi fondasi dalam menjaga akuntabilitas dan keberlangsungan pelayanan publik.

Kepercayaan masyarakat terhadap layanan digital pemerintah dibangun melalui empat elemen utama, yaitu keamanan, reliabilitas, transparansi, dan akuntabilitas. Keempat elemen tersebut membentuk *digital trust* yang menjadi modal utama keberhasilan transformasi digital sektor publik. Dalam konteks pemanfaatan AI, muncul kebutuhan untuk memperkuat akuntabilitas algoritmik agar setiap keputusan yang dihasilkan sistem tetap dapat dijelaskan, diawasi, dikoreksi, dan dipertanggungjawabkan. Walaupun sistem mampu memberikan analisis dan rekomendasi secara otomatis, pihak yang memperoleh mandat untuk mengambil keputusan tetaplah manusia dan institusi publik. Dengan demikian, penggunaan AI tidak mengurangi tanggung jawab pejabat publik dalam memastikan bahwa setiap keputusan tetap sesuai dengan prinsip tata kelola yang baik dan kepentingan masyarakat.

Pada akhirnya, kepemimpinan sektor publik pada era *Governance 5.0* dituntut mampu membangun institusi yang inovatif, resilien, dan responsif. Institusi yang inovatif berani memperbaiki cara kerja melalui pemanfaatan teknologi tanpa mengabaikan pengendalian

internal dan akuntabilitas. Institusi yang resilien mampu bertahan serta pulih dari tekanan digital, fiskal, sosial, maupun lingkungan melalui pengelolaan risiko yang baik dan perbaikan berkelanjutan. Sementara itu, institusi yang responsif mampu membaca kebutuhan masyarakat secara cepat dengan memanfaatkan data sebagai sumber pembelajaran dan dasar penyusunan kebijakan. Seorang pemimpin harus mampu menjaga keseimbangan antara inovasi dan kehati-hatian, kecepatan dan akuntabilitas, keterbukaan dan keamanan, pemanfaatan data dan perlindungan hak warga negara, serta efisiensi birokrasi dan nilai-nilai publik. Keseimbangan tersebut menjadi esensi kepemimpinan sektor publik dalam mewujudkan tata kelola yang terpercaya, berkelanjutan, dan memberikan dampak nyata bagi masyarakat.

ONE ON ONE DISCUSSION

Implementation of the Business Judgment Rule in SOEs in Indonesia: Challenges & Opportunities

Dr. Ir. Ira Puspadewi, MDM

CEO PT ASDP Indonesia Ferry (Persero) 2017–2024

ABSTRAK

Doktrin *Business Judgment Rule* (BJR) merupakan pilar perlindungan hukum esensial bagi direksi Badan Usaha Milik Negara (BUMN) dalam mengambil keputusan bisnis strategis di tengah volatilitas pasar, namun implementasinya di Indonesia menghadapi tantangan unik akibat irisan antara hukum korporasi dan hukum pidana korupsi terkait keuangan negara. Paparan diawali dengan ilustrasi transformasi kinerja ASDP yang mencatatkan rekor pendapatan dan laba tertinggi sepanjang sejarah perusahaan pada 2023, untuk menautkan pentingnya keberanian mengambil keputusan bisnis strategis termasuk aksi korporasi seperti merger dan akuisisi dengan kemakmuran suatu bangsa maupun perusahaan, merujuk pada literatur pembangunan ekonomi serta data korelasi positif antara Global Innovation Index dan PDB per kapita. Inti pembahasan kemudian diarahkan pada prinsip BJR sebagai instrumen perlindungan hukum bagi direksi BUMN, dengan mengangkat studi kasus proses hukum atas akuisisi PT Jembatan Nusantara serta pertimbangan majelis hakim yang merekomendasikan pelepasan terdakwa dari segala tuntutan hukum. Narasumber juga menyampaikan analisis perbandingan UU BUMN No. 19 Tahun 2003 dan UU BUMN No. 16 Tahun 2025 yang secara eksplisit mengadopsi BJR, implikasi UNCAC bagi Indonesia, dokumentasi praktis yang perlu disiapkan direksi agar memperoleh perlindungan BJR, serta ajakan bagi Satuan Pengawasan Intern (audit internal) untuk melakukan redefinisi peran dari sekadar fungsi kepatuhan administratif (post-factum compliance) menjadi mitra strategis (*trusted advisor*) yang memvalidasi kecukupan proses pengambilan keputusan bisnis sejak tahap perencanaan. Pesan kunci yang disampaikan adalah bahwa kriminalisasi terhadap keputusan bisnis yang diambil dengan itikad baik akan menghambat inovasi, investasi, dan tata kelola BUMN.

Kata Kunci: *Business Judgment Rule*, Tata Kelola BUMN, Kriminalisasi Kebijakan Bisnis

PEMBAHASAN

Sebagai operator penyeberangan dengan penugasan pelayanan publik, ASDP mengelola 307 lintasan sekitar 70% di antaranya berstatus perintis dan secara komersial belum menghasilkan keuntungan didukung 27 kantor cabang, 226 kapal, dan 36 pelabuhan. Dalam kondisi tersebut, ASDP berhasil mencatatkan pertumbuhan pendapatan dan laba bersih yang konsisten dari tahun ke tahun, dari pendapatan Rp1,16 triliun dan laba bersih Rp127 miliar

pada 2011 menjadi rekor tertinggi sepanjang sejarah perusahaan pada 2023 sebesar Rp4,93 triliun pendapatan dan Rp630 miliar laba bersih termasuk melewati tekanan pandemi Covid-19 pada 2020 serta melakukan aksi akuisisi korporasi pada 2021. Capaian ini disampaikan sebagai ilustrasi bahwa pertumbuhan signifikan suatu BUMN kerap kali lahir dari keberanian mengambil keputusan bisnis strategis yang terukur, bukan semata bisnis yang berjalan aman tanpa risiko.

Narasumber mengangkat pertanyaan klasik dalam ekonomi pembangunan: mengapa sejumlah negara kaya dan sebagian lain tetap miskin? Perspektif geografis menekankan bahwa iklim, beban penyakit, sumber daya alam, jarak dari pasar, akses ke sungai dan pelabuhan, biaya transportasi wilayah, serta produktivitas pertanian membentuk peluang ekonomi suatu negara (merujuk Diamond, 1997; Sachs, 2001). Perspektif institusional menegaskan bahwa kualitas institusi *rule of law*, hak kepemilikan, efektivitas pemerintahan, rendahnya korupsi, stabilitas politik, pasar yang kompetitif, kebijakan pendidikan dan inovasi, serta institusi politik-ekonomi yang inklusif pada akhirnya menentukan bagaimana peluang geografis tersebut dimanfaatkan (merujuk Acemoglu & Robinson, 2012). Perbandingan Korea Utara dan Korea Selatan dijadikan contoh bagaimana kualitas institusi, bukan geografi, yang membedakan tingkat kemakmuran dua negara dengan kondisi geografis serupa, sejalan dengan fenomena *resource curse*.

Data Global Innovation Index (GII) turut dipaparkan: dari sepuluh negara peringkat teratas GII, hanya satu perubahan komposisi terjadi antara 2021 dan 2025, yaitu masuknya Tiongkok ke posisi 10 pada 2025 menggantikan Jerman. Pada level ASEAN, Singapura menempati peringkat inovasi tertinggi (peringkat 5 dunia, PDB per kapita sekitar USD93.000), diikuti Malaysia, Vietnam, Thailand, Filipina, dan Indonesia (peringkat 55 dunia, PDB per kapita sekitar USD4.900). Analisis korelasi terhadap 133 perekonomian pada 2025 menunjukkan hubungan positif dan signifikan secara statistik antara skor GII dan PDB per kapita ($r = +0,74$, signifikan pada level 1%), melalui lima jalur: peningkatan produktivitas, penciptaan industri dan lapangan kerja baru, penguatan daya saing global, kenaikan upah dan standar hidup, serta ketahanan ekonomi jangka panjang. Sebagai ilustrasi, kesenjangan PDB per kapita Indonesia dan Vietnam yang pada 2010 mencapai USD1.824 per orang (PDB per kapita Indonesia 2,4 kali Vietnam), pada 2024 menyusut tajam menjadi hanya USD208 per orang, karena Vietnam mengejar melalui investasi dan inovasi yang lebih agresif menegaskan bahwa inovasi merupakan pendorong utama pertumbuhan ekonomi.

Untuk mewujudkan inovasi dan pertumbuhan di level korporasi, perusahaan termasuk BUMN lazim menempuh berbagai *corporate actions*, yaitu aktivitas yang secara material memengaruhi para pemangku kepentingannya. Delapan bentuk utama *corporate actions* diuraikan: dividen, *stock split*, saham bonus, *rights issue*, merger dan akuisisi (M&A), *delisting*,

spin-off, serta *share buyback*. Merger dan akuisisi menjadi sorotan khusus karena merupakan instrumen ekspansi dan transformasi bisnis yang kerap ditempuh BUMN, namun sekaligus salah satu *corporate action* dengan kompleksitas hukum dan risiko terbesar apabila keputusannya kelak dipersoalkan.

Sebagai gambaran tata kelola atas transaksi akuisisi di lingkungan BUMN, disampaikan pihak-pihak kompeten yang lazim dilibatkan: penyedia jasa *due diligence* dan valuasi aset (seperti PWC dan Hiswara Numajin & Tanjung untuk *legal due diligence*, BKI untuk *engineering due diligence*, serta penilai aset/KJPP), financial advisor (seperti PT Sarana Multi Infrastruktur/SMI), pendampingan instansi negara (BPKP, Kementerian Perhubungan, Jaksa Pengacara Negara/Jamdatun, dan Kementerian BUMN), hingga audit pasca akuisisi oleh KPPU dan Badan Pemeriksa Keuangan (BPK). Proses persetujuan aksi akuisisi BUMN mengikuti hierarki berjenjang: RJPP dan RKAP, proposal manajemen oleh Direksi, *due diligence independen*, valuasi independen oleh KJPP, review dan persetujuan Dewan Komisaris, persetujuan pemegang saham oleh Menteri BUMN, koordinasi regulasi dengan kementerian teknis, penandatanganan *Share Purchase Agreement* (SPA), hingga closing dan integrasi transaksi rangkaian tahapan berlapis yang menjadi bukti bahwa suatu keputusan akuisisi BUMN telah melalui proses bisnis yang lazim dan penuh kehati-hatian.

Doktrin BJR secara yuridis melindungi direksi dari tanggung jawab pribadi atas kerugian finansial yang timbul dari keputusan bisnis, dengan catatan keputusan tersebut diambil dengan iktikad baik (*good faith*), penuh kehati-hatian (*due care*), serta didasarkan pada informasi yang memadai dan independen tanpa benturan kepentingan (*conflict of interest*). Kerugian komersial murni merupakan bagian dari risiko bisnis inheren yang tidak sepatutnya dikategorikan sebagai tindak pidana. Tantangan utama di Indonesia muncul ketika kerugian korporasi pada BUMN diinterpretasikan sebagai kerugian keuangan negara berdasarkan Undang-Undang Tindak Pidana Korupsi, sehingga batasan yang kabur antara salah urus komersial (*commercial mismanagement*) dan tindakan *fraud* kriminal menciptakan fenomena ketakutan mengambil keputusan (*fear of decision-making*) di kalangan eksekutif BUMN.

Bagian inti paparan mengangkat studi kasus proses hukum atas akuisisi PT Jembatan Nusantara oleh PT ASDP Indonesia Ferry, di mana Ketua Majelis Hakim menilai bahwa para terdakwa seharusnya dilepaskan dari segala tuntutan hukum (*ontslag van alle rechtsvervolging*), dengan lima pertimbangan utama: (1) akuisisi PT Jembatan Nusantara dinilai sebagai kebijakan korporasi (*corporate policy*) yang masuk ranah risiko bisnis dan telah melalui proses bisnis lazim, sehingga sepatutnya dinilai dengan doktrin BJR; (2) tidak ditemukan bukti niat jahat (*mens rea*) maupun keuntungan pribadi, benturan kepentingan, atau motif ekonomi pribadi dari para pengambil keputusan; (3) proses pengambilan keputusan dilakukan dengan itikad baik dan kehati-hatian, dibuktikan melalui *due diligence* yang

komprehensif, keterlibatan sejumlah konsultan profesional, serta persetujuan berlapis dari komisaris, RUPS, dan Kementerian BUMN; (4) terdapat keraguan serius mengenai perhitungan kerugian negara akibat perbedaan pendapat ahli yang tajam, persoalan kompetensi pihak penghitung, serta metode perhitungan yang dianggap mengandung kelemahan mendasar; dan (5) berlakunya asas in dubio pro reo ketika bukti dapat menghasilkan dua kesimpulan yang sama kuat, hukum pidana mengharuskan hakim memilih kesimpulan yang menguntungkan terdakwa.

Pertimbangan majelis hakim menekankan agar penyelesaian non-pidana diutamakan terlebih dahulu, dengan prinsip bahwa hukum pidana merupakan upaya terakhir (*ultimum remedium*). Kekhawatiran yang lebih luas turut disampaikan: apabila setiap keputusan bisnis BUMN yang kemudian dinilai tidak optimal secara hasil langsung dipidana sebagai korupsi, direksi BUMN akan takut mengambil risiko bisnis, para profesional terbaik akan enggan menjadi pengurus BUMN, serta inovasi dan ekspansi perusahaan negara dapat terhambat sementara jika memang ditemukan kesalahan manajerial, mekanisme perdata, administratif, atau perbaikan tata kelola dinilai lebih tepat digunakan dibanding hukum pidana.

Perbandingan UU No. 19 Tahun 2003 tentang BUMN dengan UU No. 16 Tahun 2025 menunjukkan pergeseran arah kebijakan yang signifikan. Dari sisi fokus tujuan, UU lama menekankan keseimbangan antara mengejar keuntungan dan pelayanan publik (*public service obligation*), sementara UU baru berorientasi mengoptimalkan nilai investasi, profesionalisme internasional, dan fokus pada keuntungan (*profit orientation*). Dari sisi kelembagaan, UU lama mengatur BUMN dikelola secara birokratis langsung di bawah Kementerian BUMN, sedangkan UU baru memisahkan operasional investasi ke Badan Pengelola Investasi (Danantara), dengan Kementerian BUMN bertransformasi menjadi BP BUMN sebagai regulator. Yang paling relevan dengan tema pembahasan, dari sisi perlindungan hukum organ, UU lama belum mengatur secara eksplisit pada level undang-undang untuk kerugian bisnis murni, sementara UU No. 16 Tahun 2025 memperkuat kerangka perlindungan hukum bagi pengambil keputusan dalam pengelolaan BUMN dan investasi negara melalui prinsip itikad baik, kehati-hatian, tidak adanya benturan kepentingan, serta tidak diperolehnya keuntungan pribadi secara tidak sah. Dalam konteks Direksi Perseroan, prinsip Business Judgment Rule perlu dibaca bersama ketentuan peraturan perundang-undangan mengenai Perseroan Terbatas dan prinsip tata kelola perusahaan yang baik.

Dasar hukum perlindungan pengambil keputusan bisnis diuraikan melalui dua rujukan utama: UU Perseroan Terbatas No. 40 Tahun 2007 Pasal 97 ayat (5), yang menyatakan anggota Direksi maupun Komisaris tidak dapat dimintai pertanggungJawaban: atas kerugian perseroan apabila dapat membuktikan telah menjalankan tugas atau pengawasan dengan itikad baik, kehati-hatian, dan tanpa benturan kepentingan; serta UU BUMN No. 16 Tahun

2025 Pasal 3Y, yang memperluas perlindungan tersebut bagi Kepala BP BUMN serta organ dan pegawai Badan, sepanjang dapat membuktikan telah bertindak dengan itikad baik, kehati-hatian, tanpa benturan kepentingan, dan tanpa memperoleh keuntungan pribadi secara tidak sah.

Untuk memperjelas batasan antara keputusan bisnis yang dilindungi BJR dan tindak pidana korupsi, dipaparkan pula perbedaan mendasar antara Pasal 2 dan Pasal 3 UU Tindak Pidana Korupsi. Pasal 2 mensyaratkan unsur perbuatan melawan hukum yang memperkaya diri sendiri, orang lain, atau korporasi, dan menimbulkan kerugian negara, berlaku untuk setiap orang tanpa harus memiliki jabatan tertentu, dengan ancaman pidana minimum 4 tahun hingga maksimum 20 tahun atau seumur hidup serta denda Rp200 juta–Rp1 miliar. Pasal 3 mensyaratkan unsur penyalahgunaan wewenang karena jabatan yang bertujuan menguntungkan diri sendiri, orang lain, atau korporasi, dan menimbulkan kerugian negara, umumnya dikenakan pada pihak yang memiliki jabatan atau kewenangan, dengan ancaman pidana minimum 1 tahun hingga maksimum 20 tahun atau seumur hidup serta denda Rp50 juta–Rp1 miliar.

Definisi korupsi menurut sejumlah lembaga dunia Transparency International, UNDP, dan WHO secara konsisten merujuk pada "*the abuse of entrusted power for private gain*", dengan unsur private gain sebagai inti definisi. United Nations Convention against Corruption (UNCAC) tidak mendefinisikan korupsi berdasarkan timbulnya kerugian negara semata, melainkan menggunakan pendekatan offence-based yang mengidentifikasi berbagai perbuatan koruptif seperti *bribery, embezzlement, abuse of functions*, dan *trading in influence*, yang umumnya mensyaratkan adanya *intentional conduct* atau penyalahgunaan kewenangan yang disengaja. Indonesia telah meratifikasi UNCAC melalui UU No. 7 Tahun 2006, dengan empat implikasi utama bagi tata kelola BUMN: (1) penegakan hukum berfokus pada pembuktian unsur pidana penyalahgunaan kewenangan, konflik kepentingan, suap atau gratifikasi, penggelapan aset negara, keuntungan pribadi tidak sah, dan *mens rea* bukan hanya membuktikan adanya kerugian negara; (2) perlindungan bagi keputusan bisnis yang beritikad baik melalui BJR; (3) pencegahan kriminalisasi risiko bisnis, mengingat kerugian investasi tidak selalu berarti korupsi; serta (4) dorongan bagi iklim investasi dan tata kelola yang lebih sehat.

Dalam ekosistem *Governance* 5.0, Satuan Pengawasan Intern (SPI) atau audit internal dinilai memegang peran sentral dalam menegakkan doktrin BJR. Audit internal didorong untuk bertransformasi melampaui batas pengujian kepatuhan dokumen administratif di masa lalu (post-factum compliance), menjadi mitra strategis (*trusted advisor*) sejak tahap perencanaan aksi korporasi. Tugas krusial audit internal adalah menguji dan memvalidasi kecukupan formalitas pengambilan keputusan oleh direksi sebelum keputusan tersebut dieksekusi,

mencakup verifikasi independensi sumber data, pengujian objektivitas asumsi finansial, pengawasan program pencegahan benturan kepentingan, serta pemantauan berkelanjutan terhadap realisasi parameter bisnis utama.

Sesi ditutup dengan panduan praktis bagi direksi BUMN agar dapat memperoleh perlindungan BJR, yaitu perlunya menyiapkan dan mendokumentasikan secara memadai: notulen rapat direksi, studi kelayakan (*feasibility study*), *legal due diligence*, pendapat konsultan independen, analisis risiko, serta pendampingan atau audit oleh instansi terkait sejak tahap pengambilan keputusan. Dokumen-dokumen tersebut menjadi bukti bahwa keputusan diambil secara hati-hati dan profesional, dengan fokus pembuktian pada “apakah prosesnya benar?”, bukan semata “apakah hasilnya untung?” sebuah pergeseran cara pandang yang relevan pula bagi auditor internal dalam menilai keputusan bisnis korporasi, yaitu menilai kualitas proses pengambilan keputusan (*governance* dan *risk management*), bukan menghakimi keputusan bisnis semata dari hasil akhirnya. Narasumber menutup paparan dengan mengutip pandangan Michael Porter bahwa inovasi adalah inti dari kemakmuran ekonomi, serta pandangan Jack Ma bahwa inovasi mengarah pada kemakmuran dan kemakmuran mengarah pada perdamaian menegaskan bahwa perlindungan hukum yang memadai bagi keputusan bisnis yang beritikad baik merupakan prasyarat bagi BUMN Indonesia untuk berani berinovasi, bertransformasi, dan bersaing di tingkat global.

SESI TANYA JAWAB

Pertanyaan 1 (Bapak Vifan Bramantyo dari PT Penjaminan Infrastruktur Indonesia):

Apa rekomendasi bagi seorang direksi (CEO) atau komisaris BUMN agar dapat menjalankan tugasnya secara amanah dan memberikan hasil terbaik bagi organisasi maupun bangsa Indonesia, tanpa meninggalkan preseden buruk di kemudian hari?

Jawaban:

Amanah dalam kepemimpinan BUMN tercermin dari keberanian untuk terus melakukan transformasi dan digitalisasi organisasi, bahkan di tengah situasi yang sulit sekalipun, karena keterbatasan sumber daya justru mendorong efisiensi dan inovasi dalam bekerja ("*if you can make it in a hard situation, you can make it anywhere*"). Berdasarkan pengalaman memimpin transformasi di PT ASDP Indonesia Ferry (Persero), keberhasilan tersebut tidak selalu memerlukan intervensi besar, melainkan dapat dimulai dari intervensi sederhana yang didukung oleh *change management* yang kuat dan konsisten, sehingga mampu mengubah budaya kerja organisasi secara menyeluruh. Kunci utamanya adalah niat dan komitmen direksi maupun komisaris untuk senantiasa memberikan yang terbaik (*do the best*) bagi

perusahaan dan menjaga amanah yang telah diberikan, sembari tetap berpegang pada prinsip itikad baik, kehati-hatian, dan bebas dari benturan kepentingan sebagaimana disyaratkan dalam prinsip *Business Judgment Rule* (BJR) sehingga keputusan bisnis yang diambil, sekalipun mengandung risiko, tetap berada dalam koridor tata kelola yang baik dan terlindungi secara hukum.

Pertanyaan 2 (Bapak Bimantara dari PT Sarana Multi Infrastruktur):

Berdasarkan pengalaman kasus akuisisi PT Jembatan Nusantara di ASDP, bagaimana peran (fungsi) Auditor Internal yang ideal diharapkan dapat berjalan? Apakah *Three Lines Model* benar-benar diterapkan dan efektif dalam kasus tersebut?

Jawaban:

Three Lines Model pada dasarnya telah berjalan dengan baik dalam proses akuisisi tersebut. Seluruh tahapan keputusan bisnis telah melalui proses yang lazim, termasuk konsultasi dengan Badan Pemeriksa Keuangan (BPK) sebagaimana telah menjadi isu publik, di mana BPK dapat melakukan audit khusus atas kepatuhan investasi yang dilakukan. Manajemen turut melakukan langkah-langkah koreksi yang diperlukan, dan proses tersebut pada akhirnya dinyatakan lulus audit. Hal ini menunjukkan bahwa lini pertama (manajemen sebagai *risk owner*), lini kedua (fungsi pengawasan, manajemen risiko, dan kepatuhan), maupun lini ketiga (Internal Audit sebagai pemberi *independent assurance*) telah menjalankan perannya sesuai dengan koridor tata kelola yang berlaku. *External assurance providers*, termasuk BPK sesuai kewenangannya, memberikan *assurance* independen di luar struktur Three Lines Model organisasi. Namun demikian, perlu diakui bahwa terdapat faktor-faktor lain di luar aspek governance dan kepatuhan formal yang turut memengaruhi jalannya proses hukum atas keputusan bisnis tersebut.


Konferensi
Audit
Internal
www.ypia.id