

gaskita
Juaranya Gas Ngalir Terus

by **PGN**



PLN

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



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

Empowering Internal Auditors to Navigate Emerging Cyber Risks

Ishfihana Hafny Noer

VP Portfolio & Emerging Risk Management
PT Pertamina (Persero)

Yogyakarta, 9 Juli 2026

Why Should Internal Auditors Care?



US\$25 Million Lost
in One Deepfake Video Call

A

Seorang pegawai keuangan Arup Hong Kong **menerima pesan** terkait transaksi rahasia yang seolah-olah **berasal dari CFO perusahaan**.

B

Meskipun sempat **mencurigai pesan** tersebut, pegawai kemudian **mengikuti video conference** bersama CFO dan beberapa kolega.

C

Seluruh peserta dalam video conference, selain korban, ternyata merupakan **rekayasa deepfake**.

Alur Kejadian

1

Initial Contact

Pegawai menerima pesan yang mengatasnamakan CFO dan meminta pelaksanaan transaksi rahasia.

2

Synthetic Trust Building

Pelaku mengadakan *video conference* dengan wajah dan suara digital yang menyerupai CFO serta sejumlah kolega.

3

Transaction Execution

Korban melakukan 15 transfer ke lima rekening bank, dengan total sekitar HK\$200 juta (~US\$25 juta).

4

Fraud Discovery

Penipuan baru diketahui setelah pegawai melakukan konfirmasi lanjutan kepada kantor pusat perusahaan.

Business Impact



Direct Financial Loss

Kerugian mencapai sekitar US\$25 juta akibat transaksi yang telah diotorisasi dan dieksekusi.



Control & Governance Exposure

Kontrol pembayaran dan proses verifikasi identitas dapat gagal meskipun sistem teknologi organisasi tidak diretas.



Trust Becomes the Attack Surface

Pelaku mengeksploitasi kepercayaan, hierarki organisasi, tekanan kerahasiaan, dan *visual confirmation*.



Cyber Resilience Beyond IT

Arup menyatakan sistem internal tidak terdampak; kasus ini lebih tepat dikategorikan sebagai *technology-enhanced social engineering*.



Di mana seharusnya Internal Audit bisa memberikan
Early Warning?



Cyber Risk is Now a Boardroom & Strategic Risk

Cybersecurity is no longer just a technical issue, but a critical enabler of economic resilience and trust.



Transformasi digital & konektivitas global menciptakan interconnected & systemic risk, di mana satu gangguan dapat berdampak luas lintas sektor



Cyber risk tidak lagi terbatas pada fungsi IT, melainkan berdampak langsung pada operasi, keuangan, reputasi, dan business continuity organisasi



Perkembangan AI, geopolitik, dan fragmentasi regulasi meningkatkan kompleksitas, ketidakpastian, dan *attack surface* ancaman siber

Top Risk Areas in 2026 Assurance Plan

Gartner



Cybersecurity Vulnerabilities



Data Governance



Regulatory Compliances

“

Risk & Assurance Function must evolve from a compliance checker into a **strategic risk advisor** to effectively navigate emerging cyber risks.

”

What Makes Cyber Risk “Emerging”?

What is Emerging Risk?

Source: ISO/TS 31050

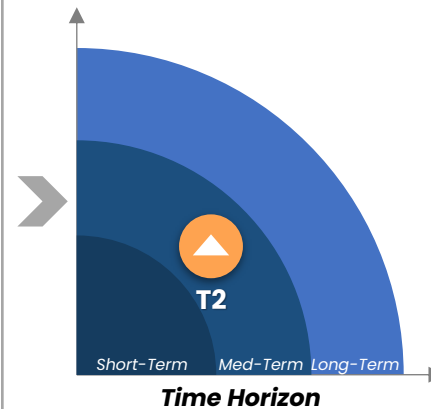


Risiko yang muncul biasanya diwakili oleh serangkaian keadaan atau kondisi baru, yang sebelumnya tidak dikenali, atau perubahan dalam karakteristik risiko yang telah diidentifikasi.

Nature of Emerging Risk

- 1 Risiko yang **belum pernah diidentifikasi** atau dialami sebelumnya oleh organisasi;
- 2 Konteks baru di mana **pengetahuan** yang ada **tidak dapat diterapkan**;
- 3 Risiko yang **berkembang** secara signifikan, risiko **sistemik**, dan **kombinasi** baru dari risiko-risiko.

Time Horizon Emerging Risk



Risiko “Meningkatnya penggunaan AI yang dapat memicu ketergantungan pada teknologi, konflik hubungan industrial, kebocoran informasi, serta tambahan kebutuhan energi” masuk dalam *time horizon Medium Term* (3-8 Tahun).

Key Drivers of Emerging Cyber Risk

1 AI-driven attacks & autonomous cybercrime

Pemanfaatan AI untuk mengotomatisasi serangan siber sehingga lebih cepat, masif, dan sulit dideteksi

2 Deepfake & advanced social engineering

Teknologi deepfake meningkatkan efektivitas penipuan berbasis manipulasi identitas dan komunikasi

3 Shadow AI & uncontrolled digital tools

Penggunaan tools AI tanpa governance meningkatkan risiko kebocoran data dan pelanggaran kepatuhan

4 Post-quantum risk & future data exposure

Ancaman bahwa teknologi quantum computing di masa depan dapat membobol enkripsi data saat ini

5 Regulatory volatility & cross-border compliance

Perubahan regulasi lintas negara meningkatkan kompleksitas kepatuhan dan risiko hukum organisasi

6 Supply chain & third-party vulnerabilities

Ketergantungan pada vendor, cloud, dan ekosistem digital meningkatkan risiko gangguan berantai lintas organisasi.

Why it Matters?

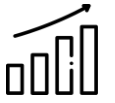
- Cyber risk meningkat karena karakteristiknya:



High
Uncertainty



High
Impact



Rapidly
Evolving

- Banyak organisasi di Indonesia belum siap menghadapi kompleksitas ancaman siber yang semakin dinamis.
- Emerging cyber risks* memerlukan pemantauan berkelanjutan karena profil risiko dapat berubah lebih cepat dibandingkan siklus *risk assessment* tradisional.

Internal Audit Must Evolve with Cyber Risk

Global Risk Landscape is Changing

Accelerating Technology & AI Risk

Perkembangan AI, cloud, dan digitalisasi mempercepat munculnya risiko baru yang sulit diprediksi serta meningkatkan *cyber attack surface* organisasi.

Geopolitical & Regulatory Fragmentation

Ketegangan geopolitik dan dinamika regulasi menciptakan ketidakpastian baru dalam pengelolaan risiko, kepatuhan, dan keamanan data lintas negara.

Interconnected & Systemic Risk

Risiko semakin saling terhubung sehingga gangguan pada teknologi, vendor, atau rantai pasok dapat berdampak luas terhadap operasional dan bisnis.

Tantangan Utama



Assurance Gap

Keterbatasan *assurance internal audit* terhadap *emerging cyber risks* yang berkembang cepat.



Confidence Gap

Muted confidence dalam memberikan *assurance* atas *cybersecurity* dan *data governance*.



Capability Gap

Kebutuhan *data analytics*, *artificial intelligence (AI)*, dan *cyber expertise* terus meningkat.

From Assurance to Strategic Insight

Peran internal audit perlu berkembang dari sekadar *compliance checker*.



Translate Cyber Risk into Business Impact

Menerjemahkan hasil *assurance* menjadi *insight* mengenai *emerging cyber risks*, dampak bisnis, dan area perbaikan pasca insiden (*post-mortem*).



Insight & Foresight Provider

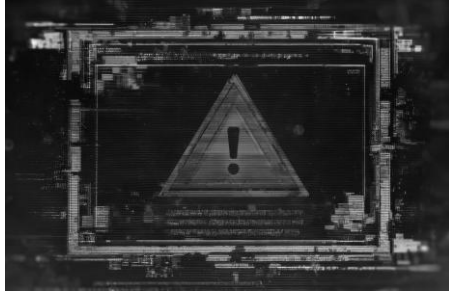
Memberikan pandangan independen untuk mendukung pengambilan keputusan.



Risk-Based Assurance

Audit difokuskan pada risiko yang paling berdampak terhadap tujuan organisasi.

How Risk & Assurance Function Should Assess Cyber Risk



1 Identify Critical Assets & Business Services

Petakan aset, sistem, dan layanan utama yang paling berdampak pada operasional bisnis

2 Assess Vulnerabilities & Threat Scenarios

Identifikasi celah keamanan dan skenario ancaman yang dapat mengganggu proses bisnis

3 Evaluate Control Effectiveness (Preventive + Detective)

Uji apakah kontrol pencegahan dan deteksi sudah berjalan efektif dalam mengurangi risiko

4 Test Resilience (Incident Response, Recovery)

Nilai kesiapan organisasi dalam merespons, memulihkan, dan menjaga kelangsungan layanan

5 Continuous Monitoring (Continuous Auditing & Analytics)

Pantau indikator risiko, anomali, dan efektivitas kontrol secara berkelanjutan

Note :



Fokus ke **business impact** (not just control failure) **and managing leading risk signal**



Integrasi assurance dengan ERM & enterprise risk profile

Cyber Risk Governance Requires Clear Roles and Strong Oversight

The Three Lines Model

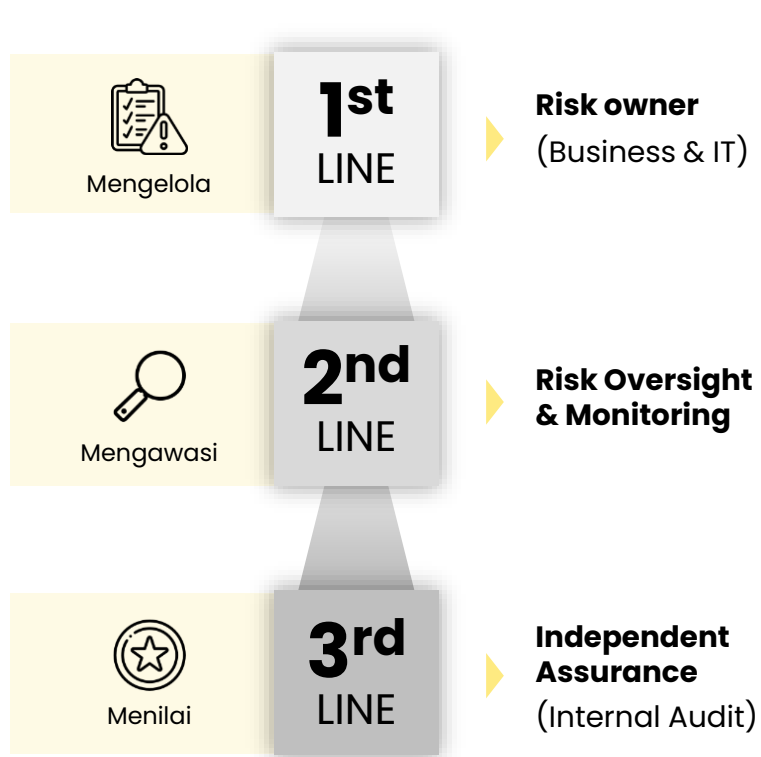
Membantu memastikan pengelolaan *Cyber Risk* dilakukan secara terstruktur melalui pembagian peran yang jelas.

Key Requirement

Tata kelola risiko siber perlu didukung peran yang jelas, koordinasi kuat, dan selaras dengan *risk appetite*.

Common Governance Gaps

Gap tata kelola dapat membuat pengelolaan risiko siber tidak efektif.



Clear Role Segregation

Mencegah Tumpang Tindih Peran.

Strong Coordination

Agar *cyber risk* ditangani terpadu.

Alignment With Risk Appetite

Perlu sejalan dengan batas risiko organisasi.

A

Fragmented governance structure

Peran dan eskalasi belum terintegrasi.

B

Lack of clear cybersecurity strategy

Strategi belum selaras dengan bisnis.

C

Delays in cybersecurity initiatives

Inisiatif siber berjalan lambat.

D

Budget constraints

Anggaran membatasi penguatan kontrol.

E

Weak accountability

Penanggung jawab risiko belum jelas.

What Strong Cyber Governance Looks Like

Elemen Utama Cyber Governance yang Kuat

Cyber governance yang kuat menuntut kejelasan peran, strategi yang selaras, kolaborasi lintas fungsi, dan assurance berkelanjutan.

FIRST LINE (1st Line)



Peran dan akuntabilitas yang jelas di seluruh *three lines*.



Cybersecurity strategy yang jelas dan selaras dengan *risk appetite*.



Awareness dan *capability* yang kuat di seluruh organisasi.



Monitoring, incident response, dan *remediation* yang berkelanjutan.



Kolaborasi terintegrasi antara fungsi *business*, *risk*, dan *IT*.

Penguatan Oversight Emerging Risk

Emerging Risk Management mendukung identifikasi, *assessment*, *monitoring*, dan mitigasi emerging cyber risks secara berkala.

SECOND LINE (2nd Line)

Emerging Risk Management:

1

Menyusun *risk concern* atas *emerging cyber risks*.

2

Melakukan kajian dan *assessment* atas eksposur serta dampak risiko.

3

Melakukan *risk monitoring* dalam periode tertentu.

4

Mengawal risiko hingga mitigasi memadai oleh *risk owner*.

Memastikan Efektivitas Governance

Internal audit berperan memberikan *assurance* independen untuk memastikan efektivitas *governance*, *risk management*.

THIRD LINE (3rd Line)



Memastikan keselarasan dengan *enterprise risk appetite*

Contoh: akses data kritikal dibatasi sesuai tingkat sensitivitas.



Menilai efektivitas *governance* dan *control*

Contoh: kebijakan akses, *incident response*, dan backup diuji berkala.



Memberikan *assurance* berkelanjutan atas *emerging cyber risks*

Contoh: risiko AI, *ransomware*, dan *third-party system* masuk *audit plan*.

Cyber governance yang kuat tercapai ketika peran sudah:

1

Jelas

2

Risiko Dipahami

3

Assurance Diberikan Secara Berkelanjutan

Empowering Internal Audit in the Cyber Era

Cyber Risk

Akan Terus Berkembang



Tidak Bisa Dihindari

Internal Audit

Enabler of Resilience

Membantu organisasi mengantisipasi, merespons, dan pulih dari *Cyber Risk*.

Fokus: kesiapan, respons, dan pemulihan.

Trusted Advisor to Management

Memberikan *insight* independen untuk mendukung keputusan manajemen.

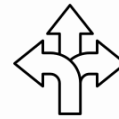
Fokus: *insight*, prioritas risiko, dan rekomendasi.

Key Success



Proactive Approach

Mengantisipasi risiko sebelum menjadi insiden.



Risk-based Mindset

Memprioritaskan area dengan dampak tertinggi.



Cross-functional Collaboration

Menghubungkan audit, *risk*, *business*, dan IT.

“

In a world of evolving cyber threats, assurance alone is not enough—

Risk & Assurance Functions must drive insight and resilience.

”

Thank You

The only limit to our realization of tomorrow will be our doubts of today." – Franklin D. Roosevelt

