Equality : Journal of Law and Justice
Vol. 3, No. 1, May, 2026, P. 26-49
e-ISSN: 3048-1252 (online)
https://jurnal.sinesia.id/index.php/Equality-JLJ

Tanggung Jawab Direksi–Komisaris Pasca Serangan Siber: *Fiduciary Duty* dan *Business Judgment Rule*

Responsibilities of Boards of Directors and Commissioners After a Cyberattack: Fiduciary Duty and the Business Judgment Rule

Sigit Ugra Nugraha[1], Muhammad Arafat[2]
E-mail Korespondensi: 24912059@students.uii.ac.id
Universitas Islam Indonesia, Yogyakarta, Indonesia

Info Article
|Submitted: 23 October 2025**|Revised**: 21 December 2025**|Accepted**: 3 January 2026
|Published: 9 January 2026

How to cite: Sigit Ugra Nugraha, "Tanggung Jawab Direksi–Komisaris Pasca Serangan Siber: *Fiduciary Duty* dan *Business Judgment Rule*", *Equality : Journal of Law and Justice*, Vol. 3, No. 1, May, 2026, p. 26-49.

ABSTRACT

Digital transformation positions cyberattacks as a critical business risk, raising accountability questions at the board level. This article aims to (i) map the synergy between the legal frameworks of the Limited Liability Company Law (UU PT), the Personal Data Protection Law (UU PDP), and the Electronic Information and Transactions Law (UU ITE) and sectoral regulations in dividing the obligations for preventing, monitoring, and reporting cyber incidents; (ii) formulate operational parameters for when negligence in cybersecurity governance can be qualified as a breach of fiduciary duty (specifically the duty of care) to the point of implicating the personal liability of company organs and, in certain circumstances, the penetration of limited liability; and (iii) assess the limits of the applicability of the Business Judgment Rule (BJR) as a post-incident safe harbor through process-based evidence. This research uses a normative juridical method with three approaches: legislation (Law 40/2007 concerning Limited Liability Companies, Law 27/2022 concerning Personal Data Protection, the ITE Law and its amendments, and sectoral regulations), doctrinal (fiduciary duty and BJR), and limited comparative (GDPR and the Caremark doctrine regarding the duty of oversight). The research findings indicate that: (i) failure to establish and oversee an adequate cybersecurity system can be viewed as a breach of duty of care, and if accompanied by circumstances indicating abuse or bad faith can strengthen the basis for attribution of personal responsibility and open up the possibility of assessing the penetration of limited liability; (ii) BJR only protects decisions/supervision made in good faith, based on adequate information, free from conflicts of interest, and accompanied by proportional preventive measures; (iii) documented and deadline-sensitive compliance – including notification of data protection failures no later than 3x24 hours, reporting of financial services sector incidents, and disclosure of information to issuers regarding material facts – is a key evidentiary element for assessing the fairness of the process and the enforceability of BJR; and (iv) the NIST Cybersecurity Framework and ISO/IEC 27001 can be positioned as objective benchmarks for assessing compliance with prudential standards. These findings offer a simple supervisory adequacy test for courts and process documentation guidelines (process dossiers) for Directors and Boards of Commissioners to strengthen the defensibility of post-incident decisions and supervision.

Keyword: *fiduciary duty; Business Judgment Rule; PDP Law; cybersecurity; corporate governance.*

ABSTRAK

Transformasi digital menempatkan serangan siber sebagai risiko bisnis kritis yang memunculkan pertanyaan akuntabilitas pada tingkat dewan. Artikel ini bertujuan (i) memetakan sinergi kerangka hukum UUPT–UU PDP–UU ITE beserta regulasi sektoral dalam membagi kewajiban pencegahan, pengawasan, dan pelaporan insiden siber; (ii) merumuskan parameter operasional kapan kelalaian tata kelola keamanan siber dapat dikualifikasikan sebagai pelanggaran fiduciary duty (khususnya duty of care) hingga berimplikasi pada tanggung jawab pribadi organ perseroan dan, dalam keadaan tertentu, penembusan tanggung jawab terbatas; serta (iii) menilai batas berlakunya Business Judgment Rule (BJR) sebagai safe harbor pasca-insiden melalui pembuktian berbasis proses. Penelitian ini menggunakan metode yuridis normatif dengan tiga pendekatan: perundang-undangan (UU 40/2007 tentang Perseroan Terbatas, UU 27/2022 tentang

Pelindungan Data Pribadi, UU ITE beserta perubahannya, serta aturan sektoral), doktrinal (fiduciary duty dan BJR), dan komparatif terbatas (GDPR dan doktrin Caremark mengenai duty of oversight). Hasil penelitian menunjukkan: (i) kegagalan membangun dan mengawasi sistem keamanan siber yang memadai dapat dipandang sebagai pelanggaran duty of care, dan apabila disertai keadaan yang menunjukkan penyalahgunaan atau itikad buruk dapat memperkuat dasar atribusi tanggung jawab pribadi serta membuka ruang penilaian penembusan tanggung jawab terbatas; (ii) BJR hanya melindungi keputusan/pengawasan yang dilakukan beritikad baik, berbasis informasi yang memadai, bebas benturan kepentingan, dan disertai langkah pencegahan yang proporsional; (iii) kepatuhan yang terdokumentasi dan sensitif-tenggat—termasuk notifikasi kegagalan pelindungan data paling lambat 3×24 jam, pelaporan insiden sektor jasa keuangan, dan keterbukaan informasi bagi emiten atas fakta material—menjadi elemen pembuktian kunci untuk menilai kewajaran proses dan keberlakuan BJR; dan (iv) NIST Cybersecurity Framework dan ISO/IEC 27001 dapat diposisikan sebagai tolok ukur objektif untuk menilai pemenuhan standar kehati-hatian. Temuan ini menawarkan uji kecukupan pengawasan yang sederhana bagi pengadilan dan pedoman dokumentasi proses (dossier proses) bagi Direksi dan Dewan Komisaris guna memperkuat defensibilitas keputusan dan pengawasan pasca-insiden.
Kata Kunci: *fiduciary duty; Business Judgment Rule; UU PDP; keamanan siber; tata kelola korporasi.*

Pendahuluan

Era digital menggeser isu siber dari ranah teknis TI menjadi risiko strategis yang sistemik di tingkat dewan. Literatur mutakhir tentang tata kelola siber menunjukkan bahwa kualitas pengawasan direksi/komisaris atas risiko siber berkelindan dengan nilai perusahaan dan resiliensi operasional; dewan perlu melakukan sense-making strategis, bukan sekadar compliance checking. Temuan empiris terbaru juga menunjukkan kesenjangan keahlian siber di dewan sehingga proses pengawasan sering "*inexpert*", memperkuat urgensi desain tata kelola yang berfokus pada proses.[1]

Dalam konteks Indonesia, dua insiden besar dalam beberapa tahun terakhir menunjukkan bahwa serangan siber tidak lagi bersifat sporadis, melainkan dapat berdampak sistemik. Pada Mei 2023, Bank Syariah Indonesia (BSI) dilaporkan terdampak serangan ransomware yang memicu gangguan layanan serta isu dugaan kebocoran data; sejumlah kajian domestik juga mengangkat peristiwa ini sebagai contoh dalam pembahasan notifikasi pelanggaran data.[2] Selanjutnya, pada Juni 2024, Pusat Data Nasional Sementara (PDNS) mengalami serangan ransomware (dilaporkan terkait varian LockBit 3.0) yang mengakibatkan terganggunya berbagai

[1] Yaniv Harel dan Abraham Carmeli, "A strategic cybersecurity oversight framework: a board's imperative," *Journal of Cybersecurity* 11, no. 1 (17 Januari 2025), https://doi.org/10.1093/cybsec/tyaf021.

[2] Jayant Chakravarti, "LockBit Leaks 1.5 TB of Data Stolen From Indonesia's BSI Bank," BankInfoSecurity (Information Security Media Group), 2023, https://www.bankinfosecurity.com/lockbit-leaks-15tb-data-stolen-from-indonesias-bsi-bank-a-22110%0A.

layanan publik—termasuk keimigrasian—selama beberapa hari.[3] Rangkaian peristiwa tersebut menegaskan bahwa kegagalan pada infrastruktur kritis dapat menimbulkan efek lintas-sektor dan memperkuat urgensi pengelolaan risiko siber pada level tata kelola.

Secara normatif, UU No. 40 Tahun 2007 tentang Perseroan Terbatas (UUPT) menetapkan Direksi sebagai organ pengurusan dan Dewan Komisaris sebagai organ pengawasan, dengan standar itikad baik dan kehati-hatian (Pasal 97 dan 114), serta membuka kemungkinan penembusan tanggung jawab terbatas (*piercing the corporate veil*) dalam keadaan tertentu (Pasal 3 ayat (2)).[4] Rezim digital modern menambahkan kewajiban spesifik melalui UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mana di dalamnya termasuk kewajiban notifikasi insiden kepada subjek data/lembaga dalam 3×24 jam[5] dan UU ITE yang telah diperbarui dengan UU No. 1 Tahun 2024, yang mempertegas koridor kepatuhan elektronik dan sanksinya[6].

Dari sisi doktrin, *fiduciary duty* (khususnya *duty of care* dan *duty of loyalty*) dan *Business Judgment Rule* (BJR) berfungsi sebagai kerangka evaluasi akuntabilitas dewan. Tradisi hukum korporasi memosisikan BJR sebagai doktrin abstensi yakni pengadilan menahan diri menilai substansi keputusan bisnis selama proses pengambilannya beritikad baik, berbasis informasi memadai, dan bebas konflik kepentingan—rangka yang sejalan dengan konstruksi Pasal 97 ayat (5) dan 114 ayat (5) UUPT.[7]

Artikel ini memandang insiden siber bukan sekadar kegagalan teknis, melainkan sinyal kegagalan tata kelola di level dewan ketika pengawasan risiko, kesiapsiagaan, dan pelaporan tidak berjalan; urgensinya makin nyata di Indonesia setelah insiden besar seperti gangguan layanan Bank Syariah Indonesia (BSI) akibat *ransomware* pada Mei 2023 dan lumpuhnya berbagai layanan publik pasca serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024 yang menunjukkan dampak lintas-sektor dari rapuhnya infrastruktur kritis. Dalam

---

[3] Georgia Butler, "Ransomware Incident Shuts Down Indonesian Gov't Data Center," Data Center Dynamics, 2024, https://www.datacenterdynamics.com/en/news/ransomware-incident-shuts-down-indonesian-govt-data-center/%0A.

[4] Indonesia. *Undang-Undang Republik Indonesia Nomor 40 Tahun 2007 tentang Perseroan Terbatas*. Lembaran Negara Republik Indonesia Tahun 2007 Nomor 106. https://peraturan.bpk.go.id/Details/39965

[5] Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. https://peraturan.bpk.go.id/Details/229798

[6] Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. https://peraturan.bpk.go.id/Details/274494

[7] Michelle R. Lowry, Anthony Vance, dan Marshall D. Vance, "Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity," *Management Science*, 23 Mei 2025, https://doi.org/10.1287/mnsc.2023.04147.

perkembangan *state of the art*, literatur tata kelola siber menekankan bahwa peran direksi/komisaris seharusnya bersifat strategis dan berorientasi proses (*oversight*, arus informasi, dan ketahanan), bukan semata kepatuhan administratif; namun, dalam konteks Indonesia masih tampak kesenjangan karena banyak pembahasan berhenti pada pemetaan norma atau checklist, belum cukup mengaitkan secara operasional sinergi UUPT–UU PDP–UU ITE (beserta aturan sektoral), batas perlindungan Business Judgment Rule (BJR), serta kondisi yang dapat mendorong tanggung jawab pribadi hingga *piercing the corporate veil*, padahal sengketa pasca-insiden biasanya ditentukan oleh bukti proses yang "sensitif tenggat" dan terdokumentasi (apa yang diputuskan, kapan, berdasar informasi apa, dan langkah pencegahan apa yang benar-benar dijalankan). Berangkat dari situ, penelitian ini merumuskan tiga pertanyaan: (i) bagaimana sinergi kerangka hukum UUPT–UU PDP–UU ITE membagi dan menautkan tanggung jawab Direksi/Komisaris dalam mitigasi risiko siber; (ii) dalam kondisi apa kelalaian tata kelola keamanan siber dapat dikualifikasikan sebagai pelanggaran fiduciary duty yang membenarkan piercing the corporate veil serta menimbulkan tanggung jawab pribadi; dan (iii) sejauh mana BJR dapat berfungsi sebagai safe harbor pasca-insiden. Kebaruannya terletak pada upaya "mendaratkan" norma ke alat uji praktis: menyusun parameter operasional pelanggaran fiduciary duty di konteks siber, memperjelas bahwa BJR hidup-matinya ditentukan kualitas proses dan dokumentasi (bukan sekadar ada kerugian atau tidak), serta menawarkan uji kecukupan pengawasan yang sederhana bagi pengadilan dan pedoman ringkas penyusunan dossier proses bagi dewan agar keputusan dan pengawasan lebih defensible ketika diuji setelah insiden.

Metode Penelitian

Penelitian ini merupakan yuridis normatif (*doctrinal legal research*) yang secara deskriptif menganalisis norma, asas, doktrin, dan peraturan perundang-undangan terkait tata kelola risiko siber di tingkat organ perseroan[8]; pendekatan yang digunakan meliputi: (i) pendekatan perundang-undangan untuk menafsirkan dan mensistematisasi ketentuan UUPT (UU No. 40/2007, khususnya Pasal 3 ayat (2), 97, dan 114), UU PDP (UU No. 27/2022), UU ITE beserta perubahannya (UU No. 11/2008 jo. UU No. 1/2024), serta regulasi sektoral seperti PP 71/2019, POJK 11/POJK.03/2022, SEOJK 29/SEOJK.03/2022, dan POJK 31/POJK.04/2015; (ii) pendekatan doktrinal untuk menelaah *fiduciary duty* (khususnya *duty of care* dan *duty of loyalty*) serta *Business Judgment Rule* (BJR) dalam literatur korporasi; dan (iii)

[8] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Prenada Media, 2005), h. 35–37. ; lihat juga Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2012), h. 13-15.

pendekatan komparatif terbatas terhadap kerangka GDPR (Regulation (EU) 2016/679) dan yurisprudensi Delaware tentang *duty of oversight* (In re Caremark dan Marchand v. Barnhill) sebagai tolok ukur perkembangan hukum. Sumber data mencakup bahan hukum primer (undang-undang, peraturan pelaksana, Putusan MA No. 121 K/Pid.Sus/2020), bahan hukum sekunder (buku/artikel ilmiah tentang metode penelitian hukum, fiduciary duty, dan BJR), serta bahan tersier (kamus hukum/ensiklopedia) untuk penegasan istilah. Metode analisis memadukan interpretasi gramatikal, sistematis, teleologis, dan historis, dilengkapi konstruksi normatif dan perbandingan yurisprudensial untuk menyusun parameter operasional pelanggaran fiduciary duty dan batas perlindungan BJR dalam konteks insiden siber.

Hasil dan pembahasan

Bagian berikut menyajikan hasil penelitian berupa pemetaan arsitektur hukum yang mengatur tanggung jawab Direksi dan Dewan Komisaris di Indonesia, mulai dari kewajiban fundamental dalam UUPT hingga transformasinya oleh regulasi siber (UU PDP, UU ITE, dan rezim sektoral) sebagai landasan bagi analisis kritis pada bagian pembahasan.

1. Kewajiban Fundamental Berdasarkan UU No. 40 Tahun 2007

Arsitektur tanggung jawab organ perseroan dalam UU PT membagi secara tegas fungsi pengurusan pada Direksi dan fungsi pengawasan pada Dewan Komisaris. Direksi menyelenggarakan pengurusan untuk kepentingan serta tujuan perseroan sekaligus mewakili perseroan di dalam dan di luar pengadilan, sedangkan Dewan Komisaris mengawasi kebijakan pengurusan dan jalannya perseroan serta memberi nasihat kepada Direksi. Rumusan ini menempatkan dua organ pada rel peran yang berbeda namun saling melengkapi: Direksi berorientasi eksekusi dan keputusan operasional-strategis; Dewan Komisaris berorientasi supervisi, penilaian independen, dan penjaga kepatuhan proses.[9]

Pada sisi Direksi, Pasal 97 UU PT menegaskan standar "itikad baik dan penuh tanggung jawab" sebagai landasan pengurusan. Secara doktrinal, standar ini dipahami sebagai penerimaan fiduciary duty dalam dua pilar: *duty of care* yaitu kewajiban bertindak hati-hati, cermat, dan berbasis informasi yang memadai sebagaimana diharapkan dari direktur pada posisi serupa serta *duty of loyalty* yaitu kewajiban mendahulukan kepentingan terbaik perseroan di atas kepentingan

[9] Doni Sagitarian Warganegara, Norhayati Mohamed, dan Imbarine Bujang, "Regulatory Settings And Corporate Governance Of Indonesia's Two-Tier Board System," 2023, 823–36, https://doi.org/10.15405/epsbs.2023.11.68; lihat juga Dabella Yunia dan Siti Mutmainah, "Does Corporate Governance Matter?," *KnE Social Sciences* 2024 (2024): 337–57, https://doi.org/10.18502/kss.v9i21.16727.

pribadi maupun pihak terkait. Dengan kacamata tata kelola risiko modern, pilar-pilar ini menuntut Direksi mampu memahami profil risiko usaha (termasuk risiko siber), mengalokasikan sumber daya yang proporsional, memastikan adanya sistem manajemen risiko yang berjalan efektif dan terdokumentasi, serta menjaga disiplin proses pengambilan keputusan.[10]

Pada sisi Dewan Komisaris, Pasal 108 dan Pasal 114 UU PT menuntut pengawasan aktif atas kebijakan pengurusan dan jalannya perseroan. Pengawasan yang dimaksud bukanlah penerimaan pasif atas laporan manajemen, melainkan keterlibatan substantif: meminta klarifikasi, menilai kecukupan kontrol internal, menantang asumsi manajemen, dan memastikan adanya jalur informasi yang memadai untuk menilai risiko material (termasuk siber). Praktik tata kelola internasional juga menekankan peran dewan dalam oversight atas manajemen risiko dan integritas pengungkapan, sehingga standar "itikad baik dan kehati-hatian" pada level komisaris beresonansi dengan prinsip-prinsip OECD (*Organisation for Economic Co-operation and Development*) mengenai tanggung jawab dewan.[11]

Mekanisme pertanggungjawaban UU PT memberikan sanksi personal ketika standar-standar tersebut dilanggar. Pasal 3 ayat (2) membuka kemungkinan penembusan tanggung jawab terbatas (*piercing the corporate veil*) pada keadaan tertentu; Pasal 97 ayat (3)–(4) menegaskan anggota Direksi bertanggung jawab pribadi atas kerugian perseroan apabila bersalah atau lalai (dan tanggung renteng bila kolegial), sedangkan Pasal 114 ayat (3)–(4) mengatur paralel untuk Dewan Komisaris. Di saat yang sama, Pasal 97 ayat (5) dan Pasal 114 ayat (5) mengenalkan safe harbor ala *Business Judgment Rule* (BJR), yakni organ dapat bebas dari tanggung jawab jika membuktikan telah bertindak dengan itikad baik, kehati-hatian, tanpa benturan kepentingan, dan telah mengambil langkah pencegahan yang wajar.[12]

Fokus tanggung jawab Direksi terletak pada akibat dari kesalahan/kelalaian dalam manajemen dan pengambilan keputusan (*process-based decision making*), sementara fokus tanggung jawab Dewan Komisaris terletak pada kegagalan pengawasan atas kebijakan Direksi (*process-based oversight*). Keduanya dipagari oleh asas itikad baik dan kehati-hatian yang harus dibuktikan melalui rekam proses

---

[10] Frederic de Mariz, Laura Aristizábal, dan Daniela Andrade Álvarez, "Fiduciary duty for directors and managers in the light of anti-ESG sentiment: an analysis of Delaware Law," *Applied Economics* 57, no. 30 (27 Juni 2025): 4309–20, https://doi.org/10.1080/00036846.2024.2356898.

[11] Athalia De Valerie dan Moody Rizqy Syailendra Putra, "Penerapan Asas Fiduciary Duty Dalam Tanggung Jawab Direksi pada Perseroan Terbatas," *JLEB: Journal of Law, Education and Business* 2, no. 1 (2024): 373–79, https://doi.org/10.57235/jleb.v2i1.1670.

[12] Indonesia. *Undang-Undang Republik Indonesia Nomor 40 Tahun 2007 tentang Perseroan Terbatas*. Lembaran Negara Republik Indonesia Tahun 2007 Nomor 106. https://peraturan.bpk.go.id/Details/39965

yang dimulai dari kualitas informasi yang dipertimbangkan, keberadaan sistem dan kontrol, hingga dokumentasi diskusi serta alasan pemilihan opsi, sehingga pada akhirnya, dalam sengketa korporasi modern, proses adalah bukti utama yang memisahkan risiko usaha yang sah dari kelalaian yang dapat dipertanggungjawabkan.

2. Transformasi Kewajiban di Era Digital

Transformasi digital telah mengubah kewajiban umum tata kelola dalam UUPT menjadi kewajiban yang lebih spesifik, terukur, dan dapat diaudit, yang secara langsung menyoroti proses, pengendalian, serta pencatatan dalam pengelolaan data dan operasi sistem elektronik. Di atas dasar tanggung jawab kepercayaan antara Direksi dan Komisaris, kini hadir lapisan regulasi siber yang menuntut perusahaan melakukan pencegahan, deteksi, penanganan, dan pelaporan insiden secara ketat. Dengan demikian, standar kehati-hatian yang sebelumnya hanya menuntut sikap hati-hati kini berkembang menjadi "terbukti berhati-hati," yakni dapat dibuktikan melalui keberadaan kebijakan, prosedur, catatan pengujian, dan laporan yang disusun serta disampaikan secara tepat waktu sesuai ketentuan.[13]

Menjawab tuntutan pembuktian proses tersebut, lapis norma yang paling konkret hadir melalui UU PDP yang secara langsung menaikkan standar kehati-hatian bagi Pengendali Data Pribadi. UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menaikkan tingkat standar kehati-hatian (*standard of care*) bagi setiap Pengendali Data Pribadi. Norma kunci mencakup kewajiban menyusun dan menerapkan langkah teknis–organisasi pengamanan (Pasal 35), melakukan pengawasan atas pihak yang terlibat dalam pemrosesan (Pasal 37), mencegah akses tidak sah (Pasal 39), serta memberitahukan kegagalan pelindungan data kepada subjek data dan lembaga berwenang paling lambat 3×24 jam sejak diketahui (Pasal 46). Kegagalan patuh, khususnya pada kewajiban notifikasi, memperkuat inferensi kelalaian[14]; UU PDP juga menyiapkan sanksi administratif (termasuk denda hingga 2% pendapatan/penerimaan tahunan) dan rejim pidana untuk pelanggaran tertentu.

[13] Hidayat Chusnul Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10, no. 2 (25 November 2019): 113–28, https://doi.org/10.22212/jp.v10i2.1447.

[14] Muhammad Arafat dan Alexander Tito Enggar Wirasto, "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia," *Equality : Journal of Law and Justice* 1, no. 2 (30 November 2024): 220–41, https://doi.org/10.69836/equality-jlj.v1i2.170.

Namun, kepatuhan terhadap UU PDP tidak berhenti pada "*checklist*" teknis (daftar pemeriksaan atau daftar hal-hal yang harus dipenuhi secara administratif) semata, karena tanggung jawab akhirnya tidak dapat didelegasikan dan berlabuh pada organ perseroan. Kewajiban UU PDP tersebut tidak dapat "didelegasikan" secara absolut sehingga tanggung jawab akhirnya tetap berada pada organ perseroan. Bagi Direksi, kewajiban ini berkelindan dengan *duty of care*, antara lain memastikan ada Sistem Manajemen Keamanan Informasi (SMKI) yang berjalan, audit berkala, dan panduan tanggap insiden, adapun bagi Dewan Komisaris, kewajiban pengawasan menuntut akses informasi yang memadai, siklus penilaian risiko, serta kemampuan menantang strategi keamanan siber manajemen. Dokumentasi pemenuhan Pasal 35–39–46 (Misalnya berupa bukti penilaian risiko, pengujian pengendalian, dan surat pemberitahuan dalam waktu 3×24 jam) menjadi bukti proses yang relevan dalam pembuktian pemenuhan *fiduciary duty*.[15]

Di luar rezim PDP, standar minimum keandalan dan keamanan bagi seluruh PSE ditegaskan oleh UU ITE bersama PP 71/2019 sebagai "*baseline*" teknis-yuridis. UU ITE (UU 11/2008 jo. UU 1/2024) mempertegas standar minimum keandalan dan keamanan sistem. Pasal 15 mewajibkan setiap Penyelenggara Sistem Elektronik (PSE) untuk menyelenggarakan sistem yang andal, aman, dan bertanggung jawab—norma "pagar atas" yang menuntut desain kontrol, monitoring, dan pemulihan yang wajar. Norma ini beroperasi bersama PP 71/2019 (PSTE) yang mensyaratkan ketersediaan, keutuhan, kerahasiaan, audit trail, dan business continuity/ disaster recovery sebagai elemen kepatuhan PSE. Bagi organ perseroan, kombinasi UU ITE–PP 71/2019 menjadi "*baseline* teknis yuridis" yang harus diinternalisasi dalam kebijakan dan penganggaran.[16]

Khusus pada sektor jasa keuangan, *baseline* tersebut dipertajam oleh ketentuan OJK yang menetapkan tenggat pelaporan insiden dan eskalasi hingga level Direksi–Komisaris. Sektor jasa keuangan menghadapi kewajiban tambahan yang lebih granular. Untuk bank, POJK 11/POJK.03/2022 mengatur tata kelola TI, sementara SEOJK 29/SEOJK.03/2022 mengharuskan notifikasi awal insiden siber ke OJK ≤ 24 jam dan laporan lengkap ≤ 5 hari kerja, disertai eskalasi hingga Direksi/Komisaris.[17] Untuk Lembaga Jasa Keuangan Nonbank (LJKNB), POJK

---

[15] A.R.Y. Toronata Tambun, Gatot Yudoko, dan Leo Aldianto, "Strategy and Innovation in AI Oversight: Fiduciary Duties of Banking Boards," *SSRN Electronic Journal*, 2025, https://doi.org/10.2139/ssrn.5403675.

[16] Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. https://peraturan.bpk.go.id/Details/274494

[17] Indonesia. *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 5/OJK. https://peraturan.bpk.go.id/Details/227376; lihat juga Indonesia. *Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum*. Ditetapkan

4/POJK.05/2021 mewajibkan penerapan manajemen risiko TI dan pengawasan aktif organ, termasuk evaluasi rencana TI dan pertanggungjawaban Direksi atas implementasi kontrol. Rejim sektoral ini secara efektif menaikkan heightened duty of care, membuat dalih "tidak tahu" atau "keliru teknis" semakin sulit diterima.[18]

Mengakumulasi seluruh kewajiban lintas rezim tersebut, tata kelola bergeser menuju kepatuhan berbasis bukti waktu yang menjadi fondasi pembuktian itikad baik dan kehati-hatian di bawah *Business Judgment Rule* (Prinsip Pertimbangan Bisnis). Bagi emiten/perusahaan publik, POJK 31/POJK.04/2015 mewajibkan keterbukaan informasi/fakta material. Insiden siber yang material terhadap nilai atau keputusan investasi harus diungkap tanpa penundaan melalui kanal yang ditentukan. Kewajiban ini berdiri berdampingan dengan UU PDP/UU ITE: perusahaan dapat serentak berkewajiban mengirim notifikasi 3×24 jam (UU PDP), notifikasi/ laporan ke OJK (bila bank), dan pengungkapan fakta material (POJK 31)—serangkaian kewajiban yang, jika tidak dipenuhi, dapat menjadi dasar tanggung jawab Direksi/Komisaris dan menihilkan klaim perlindungan proses[19].

Secara keseluruhan, arsitektur regulasi siber (UU PDP, UU ITE–PP 71/2019, dan POJK/SEOJK) mengubah tata kelola dari sekadar kepatuhan kebijakan menjadi kepatuhan berbasis bukti waktu (time-bound evidence of compliance). Tenggat 3×24 jam untuk pemberitahuan pelanggaran data, 24 jam/5 hari kerja untuk pelaporan insiden perbankan, Hingga kewajiban keterbukaan informasi (disclosure) bagi emiten memaksa organ perseroan untuk membangun mekanisme deteksi, eskalasi, dan pelaporan yang terdokumentasi dengan baik. Dalam perspektif tanggung jawab pribadi dan *Business Judgment Rule*, dokumentasi ini menjadi benteng pembuktian bahwa keputusan/ pengawasan telah diambil beritikad baik, berbasis informasi memadai, bebas konflik, dan disertai langkah pencegahan—syarat kunci untuk menghindari atribusi kelalaian pasca-insiden.

3. Doktrin Hukum sebagai Pedang & Perisai

Dalam kerangka hukum perseroan Indonesia, dua doktrin inti—*fiduciary duty* dan *Business Judgment Rule* (BJR)—bekerja sebagai logika ganda yang saling menyeimbangkan: yang pertama berfungsi sebagai "pedang" untuk menilai dan

27 Desember 2022. https://ojk.go.id/id/regulasi/Pages/Ketahanan-dan-Keamanan-Siber-Bagi-Bank-Umum.aspx

[18] Indonesia. *Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank*. Lembaran Negara Republik Indonesia Tahun 2021 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 6668. https://peraturan.bpk.go.id/Details/227125

[19] Indonesia. *Peraturan Otoritas Jasa Keuangan Nomor 31/POJK.04/2015 tentang Keterbukaan Atas Informasi atau Fakta Material oleh Emiten atau Perusahaan Publik*. Lembaran Negara Republik Indonesia Tahun 2015 Nomor 306, Tambahan Lembaran Negara Republik Indonesia Nomor 5780. https://peraturan.bpk.go.id/Details/128835

menegakkan pertanggungjawaban direksi/komisaris atas proses pengurusan dan pengawasan; yang kedua sebagai "perisai" yang membatasi atribusi kesalahan ketika keputusan telah diambil melalui proses yang wajar, beritikad baik, dan bebas benturan kepentingan. Konstruksi ini berakar pada norma UUPT tentang pengurusan dan pengawasan dengan itikad baik dan kehati-hatian, serta diperjelas oleh literatur korporasi modern yang menekankan keutamaan process over outcome: hukum memeriksa bagaimana keputusan dibuat, bukan sekadar apa hasilnya.[20]

Sebagai "pedang", *fiduciary duty* memancangkan pilar *duty of care dan duty of loyalty* yang menuntut direksi bertindak cermat, terinformasi, dan mendahulukan kepentingan perseroan, serta menuntut komisaris melakukan pengawasan aktif. Dalam konteks siber, pelanggaran tidak hanya berupa tindakan yang salah (misfeasance), tetapi juga kelalaian (nonfeasance/omission): tidak menganggarkan keamanan siber secara memadai, mengabaikan temuan audit kritis, tidak membangun sistem manajemen risiko informasi, atau tidak menyiapkan incident response dan jalur eskalasi. Norma khusus UU PDP memperkuat standar ini dengan kewajiban langkah teknis–organisasi (Pasal 35), pengawasan pihak pemroses (Pasal 37), pencegahan akses tidak sah (Pasal 39), dan notifikasi kegagalan pelindungan data ≤3×24 jam (Pasal 46); kegagalan patuh—khususnya pada tenggat—dapat menjadi indikator kuat kelalaian proses yang menggerakkan tanggung jawab pribadi organ.[21]

Dimensi *duty of oversight* sebagai cabang dari *duty of care* memberi kedalaman pada analisis kelalaian pasif. Yurisprudensi Delaware (AS) melalui *In re Caremark*, Stone v. Ritter, dan dipertegas dalam Marchand v. Barnhill menetapkan bahwa dewan dapat dimintai pertanggungjawaban bila terjadi "*utter failure*" membangun dan memantau sistem informasi/pelaporan yang wajar atas risiko yang misi-kritis bagi perusahaan. Meskipun bukan preseden mengikat di Indonesia, doktrin ini menawarkan tolok ukur konseptual yang kompatibel dengan UUPT: pengawasan yang bermakna menuntut adanya sistem, saluran informasi, dan siklus evaluasi

[20] Marika Turava, "The Scope of the Business Judgment Rule and its Relation to the Fiduciary Duties of Company Directors," *Journal of Law*, no. 1 (30 Juni 2023): 234–51, https://doi.org/10.60131/jlaw.1.2023.7073.

[21] Matthew Perri and Sara Catherine Thompson, "Overseeing Cybersecurity Risk: Confirmation of Officer Oversight Duties Could Mean Increased Personal Risk for Data Privacy and Cybersecurity Breaches," *Business Law Today*, March 9, 2023, https://www.americanbar.org/groups/business_law/resources/business-law-today/2023-march/overseeing-cybersecurity-risk-confirmation/.

risiko yang terdokumentasi termasuk untuk risiko siber yang kini bersifat strategis.[22]

Sebagai "perisai", BJR hadir dalam Pasal 97 ayat (5) dan Pasal 114 ayat (5) UUPT yang pada praktiknya membentuk safe harbor: anggota direksi/komisaris tidak bertanggung jawab atas kerugian apabila dapat membuktikan bahwa kerugian bukan karena kesalahan/kelalaiannya, ia bertindak dengan itikad baik dan kehati-hatian untuk kepentingan perseroan, bebas benturan kepentingan, serta telah mengambil langkah pencegahan.[23] Di Indonesia, arah penalaran ini mendapatkan resonansi melalui Putusan MA No. 121 K/Pid.Sus/2020, yang membedakan kerugian akibat risiko bisnis dari kerugian karena proses yang cacat (fraud, konflik kepentingan, atau pelanggaran hukum). Dengan demikian, BJR tidak melindungi ketidakpedulian (inattention) atau keputusan yang diambil tanpa basis informasi yang wajar.[24]

Sintesisnya, hubungan antara "pedang dan perisai" menggambarkan keseimbangan antara tanggung jawab dan perlindungan hukum bagi direksi dan komisaris. Dalam tata kelola modern, keduanya didorong untuk menerapkan tata kelola berbasis pembuktian proses, artinya setiap langkah harus dapat dibuktikan melalui catatan dan dokumentasi yang jelas. Direksi atau komisaris perlu memperkuat bukti melalui daftar risiko (*risk register*), pemetaan ancaman (*threat modeling*), kebijakan pengendalian, uji berkala (*table-top exercise*, yaitu simulasi penanganan insiden di atas meja), catatan ruang krisis (*war-room log*), notulensi yang mencatat opsi serta alasan keputusan, pemberitahuan dalam 3×24 jam sesuai UU PDP, dan—khusus sektor perbankan—pemberitahuan maksimal 24 jam serta laporan dalam 5 hari kerja kepada OJK.

Standar teknis seperti NIST *Cybersecurity Framework* (kerangka kerja keamanan siber NIST) dan ISO/IEC 27001 (standar sistem manajemen keamanan informasi) dapat digunakan sebagai tolok ukur objektif untuk menunjukkan bahwa keputusan dan pengawasan telah dilakukan secara berdasarkan informasi yang memadai (*reasonably informed*) dan sepadan dengan tingkat risikonya (*proportionate*). Jika bukti-bukti proses ini tersedia, Prinsip Pertimbangan Bisnis (*Business Judgment Rule*) menjadi perisai hukum yang efektif; namun bila tidak ada, tanggung jawab

[22] *Stone v. Ritter*, 911 A.2d 362 (Del. 2006), https://law.justia.com/cases/delaware/supreme-court/2006/84060.html. Justia Law; lihat juga *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019), https://law.justia.com/cases/delaware/supreme-court/2019/533-2018.html.

[23] Indonesia. *Undang-Undang Republik Indonesia Nomor 40 Tahun 2007 tentang Perseroan Terbatas*. Lembaran Negara Republik Indonesia Tahun 2007 Nomor 106. https://peraturan.bpk.go.id/Details/39965

[24] Indonesia. *Putusan Mahkamah Agung Nomor 121 K/Pid.Sus/2020*. Putusan kasasi tanggal 9 Maret 2020. Direktori Putusan Mahkamah Agung, https://putusan3.mahkamahagung.go.id/direktori/putusan/zaeb354ecfec9b009f5c313730333337.htm

kepercayaan (*fiduciary duty*) kembali berfungsi sebagai "pedang" yang menembus alasan bahwa kegagalan tersebut hanyalah "risiko bisnis biasa.".

1.1 Kerangka Penilaian Kelalaian & Bukti Proses

Standar *reasonable care* menilai kewajaran proses, bukan kemustahilan hasil. Hukum tidak menuntut keamanan absolut—yang secara teknis mustahil—melainkan tata kelola risiko yang rasional, terdokumentasi, dan proporsional dengan profil ancaman serta model bisnis perusahaan. Ukuran "rasional" mencakup keterdugaan (*foreseeability*) ancaman, kelayakan tindakan pencegahan, dan kesepadanan biaya–manfaat; ukuran "proporsional" menimbang nilai aset/data, ketergantungan operasional, dan dampak hukum–reputasi. Karena itu, pembuktian kelalaian berfokus pada jejak proses: apa yang diketahui manajemen/dewan, opsi yang dipertimbangkan, alasan pemilihan/penolakan opsi, serta konsistensi pengawasan dari waktu ke waktu.

Fondasi proses yang wajar dimulai dari arsitektur tata kelola, yaitu kebijakan keamanan informasi, penetapan risk appetite di tingkat dewan, penunjukan peran (RACI) termasuk CISO/komite risiko, inventaris aset & klasifikasi data, serta risk register yang hidup (terkini) lengkap dengan penanggung jawab, tingkat risiko residu, dan rencana penanganan. Di tahap desain, threat modeling (misal STRIDE/kill chain) memastikan skenario serangan kritikal telah diidentifikasi dan dikaitkan ke kontrol pengaman (*prevent–detect–respond–recover*). Semua ini mesti terdokumentasi dan ditinjau berkala—tanpa dokumentasi, klaim kepatuhan mudah runtuh karena tak ada bukti proses.[25]

Sebagai tolok ukur yang objektif, perusahaan sebaiknya menggunakan dan dapat membuktikan kepatuhan terhadap kerangka kerja keamanan siber NIST (NIST *Cybersecurity Framework*) dan/atau standar ISO/IEC 27001. Kerangka NIST menjelaskan lima tahap penting dalam keamanan siber, yaitu identifikasi (Identify), perlindungan (*Protect*), deteksi (*Detect*), tanggapan (*Respond*), dan pemulihan (Recover). Setiap tahap memiliki kategori dan subkategori yang bisa diaudit, seperti pengelolaan aset, pengendalian akses, pemantauan keamanan, mitigasi insiden, dan peningkatan berkelanjutan. Sementara itu, ISO/IEC 27001 mewajibkan penerapan Sistem Manajemen Keamanan Informasi (*Information Security Management System*/ISMS) yang mencakup penentuan ruang lingkup, metode penilaian risiko, rencana penanganan risiko, Pernyataan Penerapan (Statement *of Applicability*/SoA), serta penerapan kontrol dari Lampiran A (Annex A) yang meliputi aspek seperti kontrol akses, kriptografi, operasi keamanan, dan ketahanan

[25] Jeffrey G. Proudfoot et al., "The Importance of Board Member Actions for Cybersecurity Governance and Risk Management," *MIS Quarterly Executive* 22, no. 4 (2023): 235–50, https://doi.org/10.17705/2msqe.00084.

sistem.[26] Kepatuhan bukan sekadar "menyebut" kerangka, tetapi menunjukkan jejak: kebijakan, prosedur, bukti pelaksanaan, dan hasil evaluasi.

Dimensi assurance (jaminan kepatuhan dan keandalan sistem) dibangun melalui serangkaian uji dan pemantauan yang dilakukan secara disiplin. *Table-top exercise* (TTX) adalah simulasi untuk menguji kesiapan dan koordinasi tim saat terjadi krisis. Rencana tanggap insiden (*incident response plan*/IRP) dan rencana pemulihan bencana (*disaster recovery plan*/DRP) diuji secara berkala untuk memastikan sistem dapat pulih dalam waktu yang telah ditetapkan (RTO/RPO, yaitu waktu pemulihan dan batas kehilangan data yang dapat diterima). Manajemen kerentanan (*vulnerability management*) dilakukan secara berulang mulai dari pemindaian, penentuan prioritas risiko menggunakan skor seperti CVSS (*Common Vulnerability Scoring System*), hingga penerapan perbaikan sesuai dengan SLA (service level agreement). Uji penetrasi (*penetration test*) atau simulasi serangan oleh tim merah menilai ketahanan kontrol keamanan, sementara sistem pemantauan keamanan (SIEM/SOC) memantau anomali untuk menekan waktu deteksi dan pemulihan (MTTD/MTTR). Semua kegiatan ini menghasilkan bukti nyata (artefak) seperti laporan uji, daftar temuan dan perbaikan, perubahan kebijakan, serta persetujuan anggaran — yang menjadi bahasa pembuktian bahwa tanggung jawab kehati-hatian (*duty of care*) benar-benar dijalankan, bukan sekadar diklaim di atas kertas.[27]

Saat insiden terjadi, fokus pembuktian bergeser ke ketertiban respons. Perusahaan perlu klasifikasi tingkat keparahan, aktivasi war-room, dan decision log yang merekam fakta, opsi, external advice (forensik/penasihat hukum), alasan keputusan (mis. menahan operasi, isolasi, komunikasi publik), serta chain of custody untuk bukti digital. Jalur eskalasi ke manajemen puncak/dewan, dokumentasi notifikasi pelanggaran data ≤ 3×24 jam kepada subjek data & otoritas (serta tenggat sektoral seperti OJK untuk bank), dan catatan komunikasi pemangku kepentingan menjadi indikator kunci reasonably informed basis. Tanpa log dan dokumentasi waktu nyata, sulit membuktikan proses yang wajar.[28]

Kebalikannya, pola kelalaian nyata mudah dikenali: tidak adanya risk register dan threat modeling; IRP/DRP yang usang atau belum pernah diuji; patch management yang lalai terhadap kerentanan kritis; absennya MFA pada aset vital;

---

[26]National Institute of Standards & Technology. *"The CSF 1.1 Five Functions | NIST"*. U.S. Department of Commerce. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions. NIST; lihat juga "ISO 27001:2022 Annex A Controls – A Complete Guide." *IT Governance Blog*, 2024. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained. IT Governance

[27] Harel dan Carmeli, "A strategic cybersecurity oversight framework: a board's imperative."

[28] Rheva Anindya Wijayanti dan Monica Christy Natalia, "Analisis Kemampuan Security Incident Response PT XXX dalam Mengelola Insiden Siber," *Info Kripto* 18, no. 1 (2024): 31–38, https://doi.org/10.56706/ik.v18i1.98.

SOC tanpa use case deteksi yang relevan; penganggaran yang tak sepadan dengan eksposur; serta respons yang lambat dan tak terdokumentasi. Kegagalan memenuhi tenggat pelaporan (mis. 3×24 jam ke subjek data/otoritas;[29] 24 jam/5 hari kerja ke OJK untuk bank[30]) memperkuat inferensi proses cacat, sehingga klaim bahwa kerugian semata-mata akibat "risiko bisnis" cenderung ditolak[31].

Semua elemen di atas berkaitan langsung dengan *Business Judgment Rule* (BJR). BJR melindungi keputusan yang beritikad baik, berbasis informasi memadai, bebas konflik, dan disertai langkah pencegahan. Artinya, rekam proses—bukan hasil akhir—menjadi tameng utama. Paket bukti yang lazim mendukung BJR defense antara lain: board minutes yang menunjukkan diskusi risiko siber & opsi mitigasi; laporan periodik CISO ke komite risiko/dewan; SoA ISO 27001 & hasil audit internal/eksternal; metrik KRI/KPI (MTTD, MTTR, patch SLA); bukti TTX & uji pemulihan; kontrak dan due diligence vendor kritikal; serta berkas notifikasi sesuai tenggat. Tanpa "dossier proses" ini, kedudukan manajemen/dewan menjadi rapuh dalam pembuktian.[32]

Oleh sebab itu standar *reasonable care* yang operasional dapat diringkas sebagai siklus hidup bukti: (i) rancang kontrol berbasis risiko dan dokumentasikan (kebijakan, RACI, *risk register*, *threat model*); (ii) jalankan dan pantau (SOC, *logging*, *metrik*); (iii) uji dan perbaiki (TTX, *pentest*, audit, *lessons learned*); (iv) laporkan dan escalate tepat waktu (regulator, subjek data, pasar modal bila material); (v) catat seluruh keputusan, termasuk pertimbangan yang ditolak. Siklus ini tidak hanya menurunkan peluang dan dampak insiden, tetapi juga membangun benteng pembuktian bahwa Direksi dan Dewan Komisaris telah memenuhi duty of care secara profesional dan dapat dipertanggungjawabkan.

1.2 Studi Kasus Indonesia & Alokasi Tanggung Jawab Direksi–Komisaris

Kalau kita jadikan PDN dan BSI sebagai lensa, pola yang muncul bukan sekadar "mesin sempat ngadat," melainkan kegagalan pengelolaan risiko yang sistemik. Pada PDN, indikasi infrastruktur yang usang, ketidakselarasan dengan ISO/IEC 27001, kemampuan deteksi dini yang lemah, plus faktor human error, menunjukkan bahwa kontrol teknis, prosedur, dan ownership risikonya tidak

[29] Indonesia, *Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi*, Pasal 46.

[30] Indonesia, *Surat Edaran OJK No. 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum* (27 Desember 2022).

[31] National Institute of Standards and Technology (NIST), *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf; and NIST, *SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, April 3, 2025, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

[32] Harel dan Carmeli, "A strategic cybersecurity oversight framework: a board's imperative."

benar-benar menyatu. Di BSI, dampak langsungnya terasa ke layanan inti dan kepercayaan publik; langkah korektif membentuk CISO dan SOC pasca-insiden memang positif, tetapi dari kacamata tata kelola, ini seharusnya komponen arsitektur sejak awal, bukan respons setelah kebakaran. Intinya: gejala teknis yang kita lihat adalah ekspresi dari arsitektur tata kelola yang belum matang.[33]

Di PDN, jika kita terjemahkan ke bahasa *duty of care*, dewan (pada entitas pengelola) semestinya menuntut bukti bahwa *risk register* hidup, *threat modeling* dilakukan, k kritikal dipetakan, dan siklus uji, yaitu perbaiki dan uji ulang berjalan. Ketika logging dan monitoring tidak mumpuni, alarm yang harusnya berbunyi dini jadi senyap; itu berarti bukan hanya tooling yang kurang, tapi mekanisme pengawasan yang tidak bekerja. Pada level ini, pertanyaan kuncinya sederhana tapi tajam: "Apa risiko misi-kritis kita? Bagaimana kami (dewan) mendapat sinyal kalau kontrol gagal? Di mana bukti uji terakhir?" Jika jawaban tidak ada atau tidak terdokumentasi, maka itu sudah lampu merah dari sisi *oversight*.

Kasus BSI menyorot sisi lain, yaitu dampak operasional dan reputasi. Setelah serangan, pembentukan CISO/SOC adalah perbaikan penting, namun tata kelola yang sehat mengharuskan struktur ini terpasang sebelum insiden, seperti garis komando jelas, kebijakan akses ketat (mis. MFA di aset kritikal), playbook respons, dan latihan TTX rutin.[34] Dewan seharusnya menerima dashboard risiko yang bermakna: patching SLA, MTTD/MTTR, temuan pentest, hasil audit internal/eksternal, serta status rencana remediasi. Tanpa matriks seperti itu, dewan pada dasarnya "mengemudi dalam kabut." Di sinilah terlihat bedanya organisasi yang compliance-driven (dokumen ada tapi tidak hidup) dengan yang *resilience-driven* (dokumen hidup, bukti uji nyata).

Soal *responsibility gap*, sering terjadi Direksi merasa sudah "serah terima" ke tim TI/CISO, sementara Komisaris merasa sudah "menerima laporan." Padahal, delegasi tidak menghapus tanggung jawab. Direksi tetap wajib menilai kompetensi penerima delegasi dan efektivitas sistemnya; Dewan wajib aktif bertanya, menantang asumsi, dan bila perlu meminta assurance independen (mis. audit pihak ketiga, red-team). Ukuran keaktifan itu tampak dari notulensi: adakah permintaan scenario testing, permintaan external advice, atau keputusan untuk menggeser anggaran ke kontrol yang lebih material? Tanpa jejak itu, sulit membuktikan itikad baik dan kehati-hatian bila kelak diuji.

Agar celah dalam pengawasan bisa tertutup, langkah-langkah praktisnya harus jelas dan dapat dijalankan. Pertama, tetapkan pembagian peran dan

[33] Indah Nurjanah dan Didik Hariyanto, "Framing analysis of the hacking of Bank Syariah Indonesia by LockBit Ransomware on Republika.co.id and Idntimes.com," *COMMICAST* 5, no. 3 (28 Desember 2024): 1–20, https://doi.org/10.12928/commicast.v5i3.11663.

[34] Nicky Maulana et al., "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah," *INNOVATIVE: Journal Of Social Science Research* 4 (2024): 8244–58.

tanggung jawab yang tegas (siapa pemilik risiko, siapa yang melaksanakan, siapa yang menyetujui, dan siapa yang harus diberi tahu). Kedua, pastikan agenda rapat dewan secara rutin membahas risiko siber, bukan hanya ketika terjadi insiden. Ketiga, buat ukuran kinerja pengendalian seperti tingkat kepatuhan terhadap pembaruan sistem, waktu yang dibutuhkan untuk mendeteksi dan memulihkan gangguan, serta jumlah kontrol penting yang lolos pengujian. Keempat, disiplinkan dokumentasi, misalnya notulen rapat harus memuat pilihan dan alasan keputusan, alur eskalasi masalah, keputusan pelaporan insiden dalam waktu 3×24 jam sesuai UU PDP, pelaporan ke OJK bila relevan, dan keterbukaan informasi publik bila berdampak material. Dengan bukti proses yang lengkap seperti ini, direksi dan komisaris tidak hanya memperkecil kemungkinan terulangnya insiden, tetapi juga memiliki dasar pembelaan hukum yang kuat bahwa keputusan dan pengawasan telah dilakukan secara wajar, tanpa konflik kepentingan, dan dengan dokumentasi yang memadai.

1.3 Perspektif Komparatif & Arah Yurisprudensi Indonesia

Di Uni Eropa, Peraturan Perlindungan Data Umum (*General Data Protection Regulation*/GDPR) menjadikan tata kelola data sebagai tanggung jawab dewan perusahaan, bukan sekadar urusan teknis, karena ancaman denda yang dapat mencapai 4% dari omzet global memaksa perusahaan membangun sistem akuntabilitas yang nyata, yaitu perlindungan data yang dirancang sejak awal (data protection by design), catatan kegiatan pemrosesan data (*records of processing*), mekanisme penanganan pelanggaran data yang teruji (*data breach response*), serta keterbukaan informasi yang tepat waktu (*timely disclosure*). Efeknya bersifat manajerial, yaitu dewan diminta memastikan ada arsitektur risiko yang terukur dan bisa diaudit serta juga yuridis, karena setiap kegagalan bukan dinilai dari "apakah serangan terjadi," melainkan "apakah sistem pencegahan–deteksi–respons telah dibangun dan dijalankan secara wajar."[35] Lensa ini relevan bagi Indonesia: kewajiban UU PDP (termasuk notifikasi 3×24 jam) dapat dibaca sebagai penanda bahwa *duty of care* atas data pribadi kini bermakna organisasional, terdokumentasi, dan sensitif pada tenggat.

Di Amerika Serikat, khususnya Delaware, rangkaian perkara Caremark (dipertegas Stone v. Ritter dan Marchand v. Barnhill) membentuk *standar duty of oversight*: dewan baru dapat dimintai tanggung jawab jika ada "*utter failure*" untuk membangun dan memantau sistem informasi/pelaporan yang wajar atas risiko

[35] Prof. Dr. Paolo Balboni dan Kate Elizabeth Francis, "Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future," *Journal of Responsible Technology* 22 (Juni 2025): 100099, https://doi.org/10.1016/j.jrt.2024.100099.

misi-kritis.[36] Ambang ini tinggi dan jarang dikabulkan, namun ia memberi kompas: pengadilan fokus pada keberadaan (atau ketiadaan) sistem, arus informasi, dan pemantauan yang bermakna. Dengan kata lain, bukan hasil bisnis yang diuji, melainkan proses pengawasan yang dapat ditelusuri. Kerangka ini kompatibel dengan konstruksi Business Judgment Rule (BJR): hasil yang merugi tidak otomatis melahirkan tanggung jawab bila prosesnya baik, tetapi proses yang kosong menyingkirkan perisai BJR.

Ditarik ke Indonesia, frasa "melakukan pengawasan" pada Pasal 114 UUPT berpeluang dimaknai substantif seperti logika Caremark: bukan menghukum substansi keputusan siber (misalnya, memilih A ketimbang B), melainkan ketiadaan sistem pengawasan atas risiko yang krusial (mis. siber dan pelindungan data).[37] Agar tanggung jawab direksi dan komisaris bisa dinilai secara adil, pengadilan dapat menggunakan beberapa ukuran yang sederhana tetapi tegas. Pertama, apakah perusahaan memiliki sistem dan kebijakan pengelolaan risiko siber yang memadai. Kedua, apakah dewan menerima laporan rutin dan memiliki tampilan informasi yang cukup untuk memantau risiko. Ketiga, apakah evaluasi dilakukan secara berkala, misalnya melalui audit, uji penetrasi, atau simulasi krisis. Keempat, apakah langkah penanganan dan pemulihan dilakukan secara seimbang serta dicatat dengan baik. Kelima, apakah kewajiban pelaporan dilaksanakan tepat waktu, seperti pelaporan insiden data dalam 3×24 jam sesuai UU PDP, pelaporan ke OJK dalam 24 jam atau lima hari kerja, dan keterbukaan informasi publik bagi emiten jika peristiwa tersebut berdampak material. Jika semua unsur ini terpenuhi, direksi dan komisaris dapat menggunakan prinsip pertimbangan bisnis sebagai dasar pembelaan; tetapi jika tidak, maka ada potensi kelalaian yang dapat dimintakan pertanggungjawaban hukum.

Implikasinya praktis: bagi perusahaan, siapkan "dossier proses" (kebijakan, risk register, threat model, metrik KRI/KPI, notulensi yang memuat opsi & external advice, bukti uji TTX/DRP, dan arsip notifikasi sesuai tenggat); bagi regulator, harmonisasi pengawasan (UU PDP–OJK–pasar modal) mendorong budaya kepatuhan berbasis bukti waktu; bagi pengadilan, fokus pemeriksaan bergeser ke audit proses—apakah dewan benar-benar mengawasi, menerima sinyal, lalu bertindak, alih-alih sekadar "mendengar laporan." Dengan arah ini, ekosistem Indonesia dapat menyeimbangkan pedang (*fiduciary duty* yang menuntut proses) dan perisai (BJR yang melindungi proses yang wajar), sekaligus mengangkat standar tata kelola siber ke level yang layak secara global.

---

[36] Katherine M King, "Marchand v. Barnhill's Impact on the Duty of Oversight: New Factors to Assess Directors' Liability for Breaching the Duty of Oversight," *Boston College Law Review*, 2021.

[37] lili Wulandari, Utary Maharany Barus, Dan Mahmul Siregar, "Pt. Media Akademik Publisher Tanggung Jawab Direksi Dan Komisaris Yang Tidak Melaksanakan Rups Tahunan," *Jurnal Media Akademik (Jma)* 2, no. 2 (2024): 3031–5220.

Penutup

Pertama, penelitian ini menunjukkan bahwa kerangka hukum Indonesia membentuk rantai kewajiban yang sinergis: UUPT menetapkan standar umum pengurusan (Direksi) dan pengawasan (Dewan Komisaris) berbasis itikad baik dan kehati-hatian serta membuka safe harbor melalui Business Judgment Rule (BJR); UU PDP menerjemahkan standar itu menjadi kewajiban spesifik dan terukur (langkah teknis–organisasi, pengawasan pemroses, pencegahan akses tidak sah, dan notifikasi ≤ 3×24 jam); UU ITE dan PP 71/2019 memasang baseline keandalan & keamanan PSE, sementara rezim OJK/SEOJK/POJK 31 menambah tenggat pelaporan dan keterbukaan informasi pada sektor keuangan dan pasar modal. Secara operasional, sinergi ini menggeser tata kelola dari "patuh kebijakan" menjadi patuh berbasis bukti waktu, yang menuntut desain kontrol, pelaksanaan, pengujian, dan dokumentasi yang dapat diaudit.

Kedua, kelalaian tata kelola keamanan siber dapat dikualifikasikan sebagai pelanggaran fiduciary duty—dan dalam keadaan tertentu membuka tanggung jawab pribadi serta penembusan tanggung jawab terbatas—apabila terbukti adanya kegagalan proses yang material: tidak adanya/ tidak berfungsinya sistem pengelolaan risiko (mis. risk register, threat modeling, IRP/DRP yang diuji), penganggaran yang tidak proporsional, pengabaian temuan audit kritis, konflik kepentingan dalam keputusan vendor, ketidakpatuhan tenggat pelaporan (UU PDP 3×24 jam; OJK 24 jam/5 hari), atau penghilangan fakta material (emiten). Dalam konfigurasi ini, kerugian tidak lagi dipandang sebagai konsekuensi "risiko bisnis" belaka, melainkan sebagai akibat kelalaian pengurusan/pengawasan yang dapat dibuktikan dari absennya rekam proses yang wajar.

Ketiga, BJR berfungsi sebagai perisai sejauh keputusan/ pengawasan diambil beritikad baik, berbasis informasi memadai, bebas benturan kepentingan, dan disertai langkah pencegahan yang proporsional—yang semuanya tercermin dalam dokumen (notulensi rapat dewan, board pack risiko, laporan CISO, hasil uji TTX/DRP, controls testing, serta arsip notifikasi/regulatory disclosure sesuai tenggat). BJR tidak melindungi ketidakpedulian (inattention) atau proses yang kosong; pelanggaran kewajiban yang bersifat mandatory (terutama notifikasi/ pelaporan) merupakan indikator kuat runtuhnya BJR karena menunjukkan proses yang tidak wajar.

Secara keseluruhan, kontribusi praktis penelitian ini adalah mengajukan uji kecukupan pengawasan yang sederhana namun tegas—apakah sistem & kebijakan ada dan relevan; arus informasi ke dewan memadai dan rutin; evaluasi & stress test dilakukan; respons & pemulihan proporsional dan terdokumentasi; serta tenggat pelaporan dipenuhi. Penerapan uji ini tidak hanya membantu menjawab

identifikasi masalah yang diajukan (sinergi kerangka hukum, kriteria pelanggaran fiduciary duty, dan batas perlindungan BJR), tetapi juga memberi peta jalan bagi Direksi dan Dewan Komisaris untuk membangun dossier proses sebagai benteng pembuktian—meningkatkan ketahanan siber sekaligus memperkuat posisi hukum korporasi pasca-insiden.

Saran

1. **Untuk Direksi**: tetapkan cyber risk appetite dan tautkan langsung ke anggaran kontrol prioritas (MFA, EDR, patch kritikal, backup imutabel, SOC). Resmikan mandat CISO dan RACI lintas unit. Wajibkan dashboard risiko triwulanan dan uji IRP/DRP/BCP minimal 2×/tahun agar "rekam proses" siap untuk BJR defense.
2. **Untuk Dewan Komisaris**: masukkan pengawasan risiko siber ke Board/Committee Charter dan jadikan agenda tetap. Lakukan assurance independen (audit ISO 27001, red-team/TTX) dan program literasi siber berkala. Pastikan notulensi mencatat pertanyaan, arahan, tenggat, serta keputusan terkait notifikasi/disclosure.
3. **Untuk Manajemen Eksekutif**: operasionalkan ISMS (ISO/IEC 27001) atau peta NIST CSF lengkap dengan risk register, threat modeling, dan SoA yang hidup. Jalankan SOC berbasis use-case, tetapkan SLA patch CVE kritikal, perluas MFA/EDR, serta bangun TPRM dengan klausul breach notice ≤24 jam.
4. **Untuk Emiten/Sekretaris Perusahaan & Auditor/Asuransi Siber**: siapkan prosedur uji materialitas insiden dan sinkronisasi tenggat (UU PDP 3×24 jam; OJK 24 jam/5 hari; POJK 31 untuk disclosure). Latih spokesperson dan siapkan holding statement. Minta auditor menautkan temuan ke board action plan; dorong premi asuransi berbasis kematangan kontrol.
5. **Untuk Regulator**: terbitkan panduan terpadu format & tenggat pelaporan (PDP–OJK–pasar modal) serta ekspektasi minimal oversight dewan. Dorong sandbox/insentif bagi yang menunjukkan kematangan ISMS dan timely disclosure. Ukur dengan KPI/KRI sederhana: MTTD/MTTR, % MFA/EDR, kepatuhan SLA patch, % vendor dinilai, dan kepatuhan tenggat notifikasi.

Daftar Pustaka

Anindya Wijayanti, Rheva, dan Monica Christy Natalia. "Analisis Kemampuan Security Incident Response PT XXX dalam Mengelola Insiden Siber." *Info Kripto* 18, no. 1 (2024): 31–38. https://doi.org/10.56706/ik.v18i1.98.

Arafat, Muhammad, dan Alexander Tito Enggar Wirasto. "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia." *Equality : Journal of Law and Justice* 1, no. 2 (30 November 2024): 220–41.

https://doi.org/10.69836/equality-jlj.v1i2.170.
Balboni, Prof. Dr. Paolo, dan Kate Elizabeth Francis. "Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future." *Journal of Responsible Technology* 22 (Juni 2025): 100099. https://doi.org/10.1016/j.jrt.2024.100099.
Butler, Georgia. "Ransomware Incident Shuts Down Indonesian Gov't Data Center." Data Center Dynamics, 2024. https://www.datacenterdynamics.com/en/news/ransomware-incident-shuts-down-indonesian-govt-data-center/%0A.
Chakravarti, Jayant. "LockBit Leaks 1.5 TB of Data Stolen From Indonesia's BSI Bank." BankInfoSecurity (Information Security Media Group), 2023. https://www.bankinfosecurity.com/lockbit-leaks-15tb-data-stolen-from-indonesias-bsi-bank-a-22110%0A.
Chotimah, Hidayat Chusnul. "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10, no. 2 (25 November 2019): 113–28. https://doi.org/10.22212/jp.v10i2.1447.
Harel, Yaniv, dan Abraham Carmeli. "A strategic cybersecurity oversight framework: a board's imperative." *Journal of Cybersecurity* 11, no. 1 (17 Januari 2025). https://doi.org/10.1093/cybsec/tyaf021.
Indonesia. *Undang-Undang Republik Indonesia Nomor 40 Tahun 2007 tentang Perseroan Terbatas.* Lembaran Negara Republik Indonesia Tahun 2007 Nomor 106. https://peraturan.bpk.go.id/Details/39965
Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.* Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. https://peraturan.bpk.go.id/Details/229798
Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. https://peraturan.bpk.go.id/Details/274494
Indonesia. *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.* Lembaran Negara Republik Indonesia Tahun 2022 Nomor 5/OJK. https://peraturan.bpk.go.id/Details/227376
Indonesia. *Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum.* Ditetapkan 27 Desember 2022. https://ojk.go.id/id/regulasi/Pages/Ketahanan-dan-Keamanan-Siber-Bagi-

Bank-Umum.aspx

Indonesia. *Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank*. Lembaran Negara Republik Indonesia Tahun 2021 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 6668. https://peraturan.bpk.go.id/Details/227125

Indonesia. *Peraturan Otoritas Jasa Keuangan Nomor 31/POJK.04/2015 tentang Keterbukaan atas Informasi atau Fakta Material oleh Emiten atau Perusahaan Publik*. Lembaran Negara Republik Indonesia Tahun 2015 Nomor 306, Tambahan Lembaran Negara Republik Indonesia Nomor 5780. https://peraturan.bpk.go.id/Details/128835

Indonesia. *Putusan Mahkamah Agung Nomor 121 K/Pid.Sus/2020*. Putusan Kasasi tanggal 9 Maret 2020. Direktori Putusan Mahkamah Agung. https://putusan3.mahkamahagung.go.id/direktori/putusan/zaeb354ecfec9b009f5c313730333337.html

King, Katherine M. "Marchand v. Barnhill's Impact on the Duty of Oversight: New Factors to Assess Directors' Liability for Breaching the Duty of Oversight." *Boston College Law Review*, 2021.

Lowry, Michelle R., Anthony Vance, dan Marshall D. Vance. "Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity." *Management Science*, 23 Mei 2025. https://doi.org/10.1287/mnsc.2023.04147.

Marchand v. Barnhill, 212 A.3d 805 (Del. 2019). https://law.justia.com/cases/delaware/supreme-court/2019/533-2018.html

Mariz, Frederic de, Laura Aristizábal, dan Daniela Andrade Álvarez. "Fiduciary duty for directors and managers in the light of anti-ESG sentiment: an analysis of Delaware Law." *Applied Economics* 57, no. 30 (27 Juni 2025): 4309–20. https://doi.org/10.1080/00036846.2024.2356898.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Prenada Media, 2005.

Matthew Perri and Sara Catherine Thompson. "Overseeing Cybersecurity Risk: Confirmation of Officer Oversight Duties Could Mean Increased Personal Risk for Data Privacy and Cybersecurity Breaches." *Business Law Today*, March 9, 2023. https://www.americanbar.org/groups/business_law/resources/business-law-today/2023-march/overseeing-cybersecurity-risk-confirmation/

Maulana, Nicky, Tito Laurens, Hadrian Afzal Faiz, dan Tria Patrianti. "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah." *INNOVATIVE: Journal Of Social Science Research* 4 (2024): 8244–58.

Nurjanah, Indah, dan Didik Hariyanto. "Framing analysis of the hacking of Bank Syariah Indonesia by LockBit Ransomware on Republika.co.id and

Idntimes.com." *COMMICAST* 5, no. 3 (28 Desember 2024): 1–20. https://doi.org/10.12928/commicast.v5i3.11663.

Proudfoot, Jeffrey G., W. Alec Cram, Stuart Madnick, dan Michael Coden. "The Importance of Board Member Actions for Cybersecurity Governance and Risk Management." *MIS Quarterly Executive* 22, no. 4 (2023): 235–50. https://doi.org/10.17705/2msqe.00084.

Soekanto, Soerjono, dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2012.

Stone v. Ritter, 911 A.2d 362 (Del. 2006). https://law.justia.com/cases/delaware/supreme-court/2006/84060.html

Tambun, A.R.Y. Toronata, Gatot Yudoko, dan Leo Aldianto. "Strategy and Innovation in AI Oversight: Fiduciary Duties of Banking Boards." *SSRN Electronic Journal*, 2025. https://doi.org/10.2139/ssrn.5403675.

Turava, Marika. "The Scope of the Business Judgment Rule and its Relation to the Fiduciary Duties of Company Directors." *Journal of Law*, no. 1 (30 Juni 2023): 234–51. https://doi.org/10.60131/jlaw.1.2023.7073.

Valerie, Athalia De, dan Moody Rizqy Syailendra Putra. "Penerapan Asas Fiduciary Duty Dalam Tanggung Jawab Direksi pada Perseroan Terbatas." *JLEB: Journal of Law, Education and Business* 2, no. 1 (2024): 373–79. https://doi.org/10.57235/jleb.v2i1.1670.

Warganegara, Doni Sagitarian, Norhayati Mohamed, dan Imbarine Bujang. "Regulatory Settings And Corporate Governance Of Indonesia's Two-Tier Board System," 823–36, 2023. https://doi.org/10.15405/epsbs.2023.11.68.

Wulandari, Lili, Utary Maharany Barus, dan Mahmul Siregar. "PT. Media Akademik Publisher Tanggung Jawab Direksi Dan Komisaris Yang Tidak Melaksanakan Rups Tahunan." *Jurnal Media Akademik (Jma)* 2, no. 2 (2024): 3031–5220.

Yunia, Dabella, dan Siti Mutmainah. "Does Corporate Governance Matter?" *KnE Social Sciences* 2024 (2024): 337–57. https://doi.org/10.18502/kss.v9i21.16727.

Biografi Singkat Penulis

	**Sigit Ugra Nugraha, S.H**. adalah mahasiswa Program Magister Hukum Bisnis berusia 24 tahun dengan fokus pada hukum korporasi, penyelesaian sengketa bisnis, dan hukum perjanjian komersial modern. Ia memiliki ketertarikan mendalam terhadap isu-isu kontemporer seperti restrukturisasi utang, kepailitan, arbitrase komersial, dan tata kelola perusahaan yang berkeadilan. Selain menempuh pendidikan pascasarjana, Sigit aktif sebagai Junior Associate di RB Law Office, terlibat dalam penyusunan kontrak bisnis, pendampingan klien dalam perkara perdata dan komersial, serta analisis yuridis terhadap kebijakan korporasi. Kombinasi antara studi akademik dan pengalaman praktik menjadikan Sigit memiliki pemahaman yang komprehensif antara teori dan praktik hukum. Ia berkomitmen mengembangkan karier sebagai ahli hukum bisnis yang profesional, berintegritas, dan berorientasi pada penyelesaian masalah secara adil serta efisien guna memperkuat sistem hukum bisnis di Indonesia.

	**Muhammad Arafat, S.H., M.H., C.Me., CLA., CIRP**. 27 tahun, adalah mahasiswa doktoral di bidang Hukum Islam di Universitas Islam Indonesia. Saat ini, saya berprofesi sebagai advokat dengan pengalaman kurang lebih satu tahun. Dalam peran saya sebagai advokat, saya tidak hanya menangani berbagai kasus hukum, tetapi juga aktif memberikan penyuluhan hukum kepada masyarakat. Kegiatan penyuluhan ini bertujuan untuk meningkatkan pemahaman masyarakat mengenai hak-hak hukum mereka dan bagaimana hukum Islam dapat diterapkan dalam konteks modern. Saya berkomitmen untuk terus mengembangkan wawasan dan keahliannya dalam hukum Islam agar dapat memberikan kontribusi yang bermanfaat bagi masyarakat luas, serta membantu menciptakan kesadaran hukum yang lebih baik di Indonesia