



WHEN VENDORS HOLD THE EVIDENCE: OUTSOURCED AI OVERSIGHT AND CORPORATE INFORMATION DUTIES IN NEPAL, GERMANY AND DELAWARE

Prajwal Bhattarai

Nepal

Legal & Regulatory Consultant | Public Policy Analyst | Corporate Governance & Strategic Management Advisor

ORCID iD: <https://orcid.org/0009-0004-3313-7772>

Google Scholar Profile: <https://scholar.google.com/citations?user=Bdrgc5QAAAAJ>

Abstract

Outsourced artificial intelligence (AI) can separate the company making consequential decisions from the organization possessing material vendor warnings. This doctrinal and functional study asks how a Nepal-incorporated deployer could obtain, assess and act on those warnings without presupposing a Nepalese AI-specific board duty. The historical English rendering of Nepal's Companies Act supplies a provisional legal starting point; current German stock-corporation provisions illustrate differentiated reporting and risk-control obligations; and Delaware decisions supply a distinct bad-faith oversight comparator. The amended 2026 EU AI Act and international due-diligence frameworks are examined only within their territorial, temporal and nonbinding limits. Three expressly hypothetical organizational configurations test contractual privity, escalation authority and practical remedies. The comparison finds that effective escalation depends on three separable capacities: legal access to vendor evidence, authority to decide on continued use and a record linking the warning to the decision. It proposes a risk-proportionate architecture without presenting the comparators as Nepalese positive law. Authentic current Nepali statutory consolidation, actual board or vendor records and any causal effects of the proposal have not been independently established. The contribution is a competence-first decision rule identifying the minimum lawful correction needed to turn a supplier warning into proportional, reviewable action; it is not evidence of reduced AI harm.

Keywords: Nepal; corporate oversight; outsourced artificial intelligence; subsidiary governance; Delaware Caremark; Germany; vendor incident evidence; comparative law

1. Introduction: the missing warning

An enterprise can make a consequential decision using an artificial-intelligence system without having designed, trained or even directly contracted for that system. A multinational parent negotiates a procurement agreement, a third-party provider hosts and updates the model and a Nepal-incorporated operating company uses its output to screen customers, prioritize claims or assess business risk. A warning about data drift, discriminatory errors, an insecure interface or a change in the provider's testing assumptions may arrive first at the purchasing parent or an offshore technical team. The local directors, whose company is making the consequential decision, may receive a quarterly assurance summary but no incident record. The resulting accountability problem is not simply whether the algorithm was inaccurate. It is whether legally competent people received sufficiently intelligible information to decide whether continued use was justified.

This article examines a narrow question: when an AI provider warns of a material compliance risk affecting a Nepal-incorporated subsidiary, what legal and organizational arrangements can ensure that the warning reaches the subsidiary's authorized decision-makers and results in a proportionate, reviewable response? The comparison is deliberately asymmetric. Nepal is the domestic decision setting; German stock-corporation law supplies a structured institutional contrast on management reporting and risk controls; and Delaware corporate oversight doctrine supplies a jurisprudential contrast on the consequences of defective board-level compliance systems. The European Union's AI Act enters only insofar as it



establishes a distinct provider-and-deployer regulatory model relevant to some German or cross-border transactions. None of those external rules is presumed to govern an ordinary Nepalese company merely because its parent or supplier is abroad.

The analysis yields a practical distinction: a warning creates potential accountability only if a competent decision-maker can receive it, interpret its significance and exercise a proportionate corrective power. Where AI-related harms are material to a business, governance is more defensible when the operating entity maintains a documented route from vendor warnings to a named management owner, from that owner to the board when escalation criteria are met and from the board to corrective powers that can actually be exercised. This proposed managerial design is not a judicially established Nepalese standard: neither strict liability whenever an AI output is wrong nor universal board examination of model architecture follows from the cited company-law text. It is an information-and-decision process proportional to severity, control, expected harm and organizational means. Whether failure to establish such a process constitutes a legal breach in Nepal depends on the authentic statute, governing organizational documents, relevant sectoral law, factual knowledge and remedy. The article does not assert that any Nepalese court has already imposed an AI-specific duty.

The transnational problem is a division of legal powers: a parent procures a system and holds vendor rights, a provider retains incident logs, while a Nepal-incorporated company makes consequential operational decisions. Accountability requires identifying who can compel disclosure, who can suspend use and which actor can document the reasons for doing so. This paper therefore follows authority and evidence across legal persons rather than ranking countries by digital sophistication. The scenarios are constructed doctrinal tests, not reports of corporate practice.

The investigation is a comparative doctrinal and design-oriented study, not an empirical effectiveness evaluation. It closely examines Nepal's Companies Act, 2063, German Aktiengesetz provisions, Delaware's published Marchand opinion and associated oversight doctrine, the EU AI Act's differentiated obligations and current commencement provisions and international soft-law risk-management guidance. It then applies those sources to explicitly hypothetical incident sequences. No actual Nepalese board minutes, private outsourcing agreement, breach event, customer outcome or interview is represented as having been obtained. This scope supports a legal-institutional argument and an auditable management proposal; it cannot establish that adopting the proposal would statistically reduce harms.

2. Prior scholarship, research gap and analytical contribution

The relevant literature spans several conversations that should not be collapsed. Corporate oversight scholarship asks what information directors should seek and what omissions generate legal liability. Work on AI accountability addresses explainability, contestability, supply-chain power and the distribution of responsibility across the AI lifecycle. Management scholarship examines how outsourcing creates monitoring problems when a firm delegates technical production while retaining business exposure. Regulatory literature studies the relationship between binding risk duties and voluntary frameworks. These literatures converge on accountability yet do not assign identical meanings to that term. Legal liability concerns enforceable consequences under a particular jurisdiction; managerial accountability concerns designated authority and internal records; public accountability asks whether affected people can obtain reasons and remedies.

Zhao's 2024 study of accountable AI in the boardroom considers how AI can assist, support or reproduce directors' decisions and argues for smart regulation connecting corporate oversight with technical accountability. This article studies a different legal-person chain: a Nepal-incorporated deployer relies on an externally developed system, while procurement rights and technical warnings may be held by a parent company or provider. The doctrinal question is not whether AI itself informs



Cover Page



the board but which actor can obtain vendor evidence and exercise an enforceable corrective power. This is a specifically framed distinction from Zhao's inquiry, not proof of scholarly priority against the entire AI-governance literature (Zhao 2024).

Passador's 2025 analysis of insourcing and outsourcing strategies identifies tensions in proceduralized corporate decision-making and the purchase of specialist expertise (Passador 2025). That scholarship is particularly relevant to the inference that obtaining an external expert does not eliminate a board's need to make a reasoned organizational decision. Yet contracting itself cannot be treated as proof of adequate oversight. The contract might contain a right to demand audit records but the operating subsidiary might not be a party, the right might never have been exercised or important information might be protected by technical or commercial restrictions. The key doctrinal and management question becomes who can activate the right when a time-sensitive warning arises.

Ishkhanyan's cross-border AI governance study focuses on corporate power, sovereign regulation and international coordination (Ishkhanyan 2026). Its macro-level framing helps explain why jurisdictions cannot rely solely on firms' voluntary cross-border harmonization. A Nepalese company may face contractual standards set abroad while being answerable to local corporate and sectoral requirements. But macro-regulatory conflict is not enough to identify the domestic director who must act on a particular report. The missing analytical scale is the level of the subsidiary meeting, compliance escalation and corrective authorization. The present inquiry proposes that those interfaces, rather than abstract claims of convergent AI principles, are the appropriate starting points for an operational comparison.

Dana's 2025 critique argues that performative gestures can satisfy appearances without producing substantive oversight and proposes changes to Delaware's bad-faith liability threshold (Dana 2025). Shiman's 2025 study of Caremark decisions from 1996 to 2024 supplies a complementary empirical counterpoint: pleading outcomes vary with the character of alleged harm, yet cannot be reduced to a single universal predictor of liability (Shiman 2025). These studies challenge a simple inference from policies or minutes to responsible conduct. This article therefore distinguishes records documenting actual choices, escalation and follow-through from formal reporting rituals; it also avoids treating scholarship proposing doctrinal reform as current binding Delaware law. The operative test is not the number of meetings but whether lawfully available evidence was evaluated by a person empowered to do something meaningful about it.

The article's intellectual contribution is not that oversight requires information, a proposition already familiar to agency theory and corporate governance. It is the claim that three institutional capacities are independently variable: lawful access to a risk signal, legal or delegated competence to decide and an observable capacity to implement and revisit the decision. An organization with access and competence but no follow-through has paper oversight; one with access and follow-through but no delegated authority risks unauthorized intervention; one with competence and follow-through but no risk evidence may make an energetic but uninformed decision. This capacity-combination test distinguishes the legal identity that receives a warning from the one that can change the deployment. It is offered as a new functional synthesis, not an assertion that prior scholarship has never considered its elements.

3. Framework and method: comparison by function, not resemblance

The article uses a structured functional comparison with three linked questions applied to each jurisdiction: who owes the legally relevant duty, what information must or reasonably should reach that actor and what action can that actor authorize? These questions are deliberately more discriminating than simply asking whether the legal system values transparency or



Cover Page



responsible AI. A broad commitment to transparency does not tell a board whether it may suspend use of an outsourced service. A requirement for risk management does not necessarily create standing for customers to sue directors. A vendor's promise to notify a parent does not make the parent's directors fiduciaries of its Nepalese subsidiary.

The governing theoretical relationship is agency under informational asymmetry, constrained by corporate-law competence. The principal-agent vocabulary is useful but insufficient on its own. The vendor may possess detailed model information while the deploying company bears much of the business loss; the parent may act as centralized purchaser while the subsidiary owns the deployment decision; directors delegate daily operations to managers yet retain legally defined governance functions. Each interface creates an opportunity for a warning to be filtered or delayed. But agency theory cannot create a statutory duty. It helps identify incentives and information gaps only after the legal identity and power of every actor are established.

For Nepal, the relevant unit is a Nepal-incorporated private or public company using a high-consequence third-party AI service. For Germany, the statutory model is principally the Aktiengesellschaft under the Stock Corporation Act, not every German GmbH or unincorporated organization. For Delaware, the doctrinal reference is a corporation whose directors are subject to Delaware fiduciary law. These are not matched samples of similar firms. The comparison is deliberately functional and contrastive: Nepal offers the operative local governance problem, Germany a differentiated management/supervisory reporting architecture and Delaware a judicially developed duty-of-loyalty oversight framework. A German company is not treated as a development peer merely because the comparison is convenient.

The Nepal Law Commission supplies published Nepali text of the Companies Act 2063 and the earlier amendment sequence. More recent evidence changes the version inquiry: the Office of the Company Registrar separately lists an official compilation including amendments through 2081/12/17, published in 2083. Its complete provisions could not be retrieved and compared in this research pass. Consequently, the quoted §§95, 96 and 99 are established only for the published text inspected, not certified as the unchanged October 2026 consolidated wording. The 2075 proposal on the Law Commission website is not itself enacted law. Each comparative inference remains contingent on an actual law-in-force check (Nepal Law Commission, Companies Act §§95, 96, 99; Office of Company Registrar, Companies Act including 2081/12/17 amendment).

The case method is a transparently constructed doctrinal stress test. Three configurations are considered: a wholly owned Nepalese subsidiary with parent-level procurement; an independent Nepalese company purchasing directly; and a franchise-like independent firm using technology specified by a foreign commercial counterparty. In each, an identical hypothetical vendor alert is tested against ownership, reporting, budget and remediation variables. This is not process tracing from real company records, not a survey and not a causal comparison of observed incidents. Those stronger methods would require dated contracts, board minutes, regulator actions, actual incident logs and informed consent or other lawful data-access bases.

Five observations could falsify or materially weaken the proposed governance model. Authentic Nepalese law may allocate a relevant task to a regulator or manager rather than the board; a contract may leave the deployer without meaningful vendor access; direct sectoral supervision may outperform board escalation; disproportionate monitoring costs may outweigh benefits for low-impact systems; or recorded decisions may fail to generate operational follow-through. The proposed test therefore asks not whether information was produced but whether the relevant person could lawfully obtain it, exercise an



actual corrective power and preserve a decision record. Those are research variables, not demonstrated correlates of lower AI harm.

Operationalization requires three separate document tests. Evidence access is assessed by the executed procurement agreement, notice and audit clauses, actual recipient of incident messages and any lawfully available disclosure exception; a parent-held contractual right is not automatically enforceable by its subsidiary. Decision authority is assessed through articles, delegation schedules, incident escalation instructions and evidence of who may suspend, restrict or resume deployment. Decision traceability is assessed through timestamps, the risk assessment communicated, documented reasons, a responsible decision-maker and verified follow-up. Failure of one capacity should be recorded independently of the others and a contractual clause should not be scored as operationally effective merely because it exists.

4. Nepal: company duties, board competence and legal caution

The Nepal Law Commission's published Nepali text of the Companies Act 2063 supplies concrete corporate-organ rules, while a completed consolidation of all changes effective in October 2026 remains outstanding. Section 95(1) describes collective board administration and §96(1) addresses appointment of a managing director. More importantly, the published original wording of §99(4) expressly refers to each director and officer (sanchalak tatha padadhikari) and sets out honesty, good faith, care and diligence in performing official duties. This verifies the published wording's inclusion of both categories; it does not by itself settle current amendments, the definition of an officer, enforcement standing or the conditions of §99(5). A draft amendment remains a proposal, not enacted law. None of these provisions is an AI-specific strict-liability rule (Nepal Law Commission, Companies Act 2063, §§95(1), 96(1), 99(4)).

The domestic legal question has three levels which cannot be substituted for one another: who has competence to manage deployment which persons must exercise legally specified standards of care and which claimant can obtain what remedy upon breach. The published §95(1) describes collective board management subject to the Act, articles and general-meeting decisions; §96(1) concerns selection of a managing director; and §99(4) expressly names directors and officers in its published Nepali wording. The duties' amended scope, legal remedy and application to a particular AI warning require a separate current-law and fact-specific analysis. A subsidiary's practical right to receive vendor evidence must moreover be grounded in a contract, valid delegation or another enforceable instrument, not assumed from corporate competence (Nepal Law Commission, Companies Act 2063, §§95(1), 96(1), 99(4)).

Corporate separation limits the analysis. A Nepal-incorporated subsidiary and its overseas parent remain distinct legal persons, even if group procurement or technical policy is centralized. The parent may own the vendor contract while the subsidiary controls use; the board's operational competence does not create a direct claim against a vendor merely by inference. An enforceable notification or information route could arise from the subsidiary's own contract, a valid contractual mandate exercised by the parent or another demonstrated legal basis. Whether a Nepalese contract may grant third-party enforcement, how delegation operates and which remedies attach must be tested under the actual instrument and applicable law. The proposal therefore identifies a contractual problem to solve, rather than presupposing that cross-group information sharing is already legally compulsory.

The published Nepali text and the historical English rendering must be kept separate from any unverified later amendment. Four issues remain distinct: collective board competence under §95; standards relevant to the director or officer under the published §99(4); evidence of knowledge and response in the particular company; and an enforceable remedy with its own



Cover Page



statutory predicates. The original-language §99(4) expressly mentions directors and officers but this fact does not itself establish a customer cause of action. The conditions and beneficiary of any recovery under §99(5) still require full current-law verification. This structure prevents a parent procurement contract from being mistaken for a direct fiduciary undertaking toward a Nepalese subsidiary's customers (Companies Act 2063, §§95, 99(4)–(5)).

The published original-language text draws a substantive liability distinction. Section 99(4) expressly directs every director and officer to act honestly, in good faith and with care in discharging official responsibilities. Section 99(5), however, provides that the company may recover loss from a director who, contrary to subsection (4), acts in bad faith so as to cause company loss (the published Nepali text uses “सञ्चालकबाट” in subsection (5)); it is not textually an automatic damages action against every officer or a claim in favor of an injured customer. The separate Companies Act §159(1) identifies persons whose complaints may initiate proceedings, while §159(2) allocates defined dispute and compensation matters to the court; neither erases the elements of the particular cause of action. The later amended text must still be compared before a present-law recovery claim is certified. In practice, incident notice, internal escalation and suspension authority should be established by governing company documents and contracts rather than falsely derived from this damages provision (Companies Act 2063, published §§99(4)–(5), 159(1)–(2)).

The crucial doctrinal separation is between identifying an organizational duty and establishing its judicial enforcement. In the published Nepalese text, §99(4) addresses conduct by directors and officers, whereas §99(5) sets out distinct predicates for recovering company loss from directors. Neither provision alone resolves standing, proof of causation, contractual access to vendor evidence or the status of a particular parent-company director. The proposed warning architecture accordingly supplements, rather than purports to enlarge, statutory causes of action.

Publication and legal-currentness are different checks. The published Nepal Companies Act §§99(4)–(5) differentiate the broadly framed conduct standard for directors and officers from a specified company-loss recovery claim against bad-faith directors. Section 159 provides an additional procedural framework, not an AI-specific civil cause of action. An Office of Company Registrar compilation marked amended through 2081/12/17 has been located but not fully compared with those provisions. The doctrinal proposal accordingly rests on authenticated historical wording, while any claim about the exact law-in-force in an October 2026 dispute remains conditional. Neither German nor Delaware law supplies that missing domestic cause of action.

Nepal's public-policy context makes the distinction between corporate duty and regulatory program important. Authorities may wish to protect customers and encourage trustworthy digital services but supervisory jurisdiction differs across financial institutions, telecommunications, education, health and ordinary commercial companies. No unified AI incident filing requirement is assumed here. The policy proposal is accordingly modular: company-law governance principles supply responsible decision-making; existing sector regulators may impose their own concrete rules where legally empowered; and voluntary or contractual standards can fill operational gaps without being mislabeled as law. Its feasibility depends on mapping each regulator's statutory competence and avoiding conflicting obligations.

5. Germany: differentiated corporate organs and risk reporting

The current German statutory text offers a comparatively precise distinction. Aktiengesetz §90(1) obliges the Vorstand of an AG to report specified planning, profitability, business and material-transaction matters to the Aufsichtsrat; where the reporting company is a parent, the provision expressly encompasses relevant subsidiary and joint-venture matters. Section



Cover Page



90(3) enables the supervisory board to request reports. Section 91(2) requires suitable measures, notably a monitoring system for developments endangering the company's continued existence, whereas the additional effective internal-control and risk-management duty in §91(3) is addressed specifically to a listed company. Section 93(1) makes adequate information relevant to protected entrepreneurial decision-making. None of these provisions automatically imposes an identical obligation on every German company and none itself creates a Nepalese statutory duty (German Federal Ministry of Justice, AktG §§90, 91, 93; original text inspected October 2026).

The German architecture is relevant because it articulates legal channels between organizational functions and corporate organs. It separates management and supervisory responsibilities in a way not identical to a Delaware board or an ordinary Nepalese subsidiary. The comparator therefore helps ask what information a board or supervisory organ needs to exercise a defined function rather than who should possess omniscient technical expertise. A vendor model-performance report that materially affects the company's continued viability would present a different concern from a minor routine software defect. The statute itself distinguishes company-threatening developments, business-significant matters and the scope of specialized risk management. A corporate policy that mechanically treats all three as legally equivalent would overstate the law and undermine prioritization.

Germany's §90 also shows why corporate separation does not invariably make group-relevant facts irrelevant to an organ's reporting remit. In its specified parent-company context, relevant subsidiary and joint-venture matters are included in reporting; §90(3) further allows supervisory-board inquiries into corporate relationships and material affiliated-company developments (AktG). These provisions do not impose a general duty on all German parents to answer for a Nepal-incorporated subsidiary, nor make German law governing law for a Nepalese company's board. The transferable analytical point is narrower: the legislator can define a reporting interface for materially connected operations without merging corporate persons. For Nepalese governance design, the question is whether an equivalent interface can be secured by enforceable agreements and valid delegations, rather than imported by analogy as an existing statute.

The difference between German stock corporations and other German organizational forms must not be hidden. A multinational group's German parent may be an AG, a GmbH or a different entity, with corresponding changes to governance requirements. This article's principal legal comparison is restricted to the Aktiengesetz model. Similarly, the cross-border operational structure matters: a German parent may make the global procurement choice while the Nepalese subsidiary makes the local decision to process data. The parent might have valid security reasons to centralize access, while the local board may need only a carefully summarized alert with an avenue for independent verification. An indiscriminate demand for disclosure of all source code or commercially sensitive data is not the necessary implication of sound risk reporting.

A final difficulty concerns proof. The law's requirement for an appropriate management system does not prove that a particular company used one effectively and a supervisory report does not establish that those who received it understood the risk. A successful research extension would compare internal audit charters, escalation timetables and redacted board materials from actual firms rather than infer practice from statutory design. Without such documents, Germany serves as a structured legal contrast, not evidence that German AI oversight is empirically superior to Nepal's. Its apparent sophistication must not be used as a proxy for measurable risk outcomes.



6. Delaware: oversight liability is not strict liability for failure

In *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019), pleaded facts about food safety, a central business risk, supported an inference of inadequate board-level reporting, leading the Delaware Supreme Court to reverse dismissal rather than adjudicate ultimate liability. In *re The Boeing Company Derivative Litigation*, C.A. No. 2019-0907-MTZ (Del. Ch. 7 September 2021), provides a further pleading-stage illustration involving mission-critical airplane safety. The comparison is functional: decision-makers may need credible routes for learning of serious operational risks. The cases neither establish that every AI vendor warning is a legally decisive red flag nor prescribe a Nepalese standard of corporate liability.

The McDonald's litigation supplies a role-specific caution. The January 2023 Delaware Chancery opinion addressed oversight obligations of a corporate officer; a separate March 2023 opinion dismissed claims against director defendants in that litigation. Neither ruling means that officers are invariably liable or directors categorically insulated. Each turns on pleaded duty, knowledge, powers and procedural posture. For a Nepalese subsidiary, the analogy is limited to identifying which person could receive and act on a provider's warning; the opinions supply no Nepalese cause of action (In *re McDonald's Corp. Stockholder Derivative Litigation*, C.A. No. 2021-0324-JTL).

The useful question is therefore whether a material warning reached an actor with authority to respond, rather than whether the eventual corporate decision proved correct. Operational officers, directors and a parent contracting company may each have different information, rights and duties. A legal conclusion about any of them still requires the relevant domestic law and facts.

For this article, the case's value is analytical rather than jurisdictional. A corporation may have operating-level procedures yet lack a route that makes material compliance concerns available to those charged with oversight. In *Marchand*, the absence of a board-level food-safety reporting structure was legally salient because food safety was central to the company's business. In a Nepal-linked AI deployment, a similar information failure is imaginable when the software determines access to a highly consequential service and board reporting omits the provider's warnings. But analogy cannot substitute for the domestic legal threshold, nor does it establish that all commercial AI systems are 'mission critical.' Materiality must be proved by reference to the subsidiary's function, legal exposure, affected users and potential harm.

The significance of *Stone* is the difference between absence of a good-faith reporting effort and an imperfect system. Under the first pathway, the allegation is that directors failed to make any genuine effort to establish information or reporting controls. Under the second, directors consciously disregarded oversight responsibilities after creating them. Both turn on bad faith and the facts alleged, not on a retrospective preference for another monitoring arrangement (*Stone v. Ritter*, 911 A.2d at 370). An outsourced AI warning can therefore be a material red flag only if its substance, the company's operational exposure and the responsible decision-maker's knowledge make it legally relevant; a low-priority technical alert is not automatically such a warning.

The analogy is strongest at the level of design choice, not remedy. Delaware fiduciary litigation is shaped by a derivative action framework, standards for pleading, internal corporate law and case-specific procedural rules. A Nepalese claimant cannot simply cite *Marchand* as binding authority for a local director-damages action. Nor can a German supervisory body be assumed to have precisely the same function as a Delaware board committee. The comparison instead identifies several transferable questions: Was the risk central enough to justify periodic board information? Was there a specified pathway



Cover Page



from management to directors? Did the board make any good-faith effort to secure that information? When an alert came, was its response based on an intelligible evidentiary record?

A serious objection is that such questions may favor paperwork over responsible behavior. Dana's critique of performative oversight makes this objection precise: apparent procedural compliance can conceal a lack of genuine engagement (Dana 2025). Accordingly, this paper proposes an evidentiary hierarchy. An adopted policy alone is weak evidence. A dated incident record with acknowledged receipt is stronger. A minute recording alternative actions, responsible officials, stop-use authority and follow-up monitoring is stronger still. The most probative record may be evidence that a decision actually changed the system's deployment or remedied an affected person's harm. These distinctions should guide a Nepalese board seeking defensibility but they are not a restatement of a binding Nepalese evidentiary rule.

A second objection is that a court-led, after-the-fact liability regime may not be the best instrument for managing fast-moving operational incidents. The vendor warning could require action in hours, whereas a director-liability case can take years and depend on disputed procedural details. A forward-looking reporting architecture could therefore be valuable even where derivative litigation would be unavailable or inappropriate. The article resists making the court the universal governance actor. Its task is to clarify a corporate system capable of preserving options for company-level response, public oversight where authorized and proportionate remedies for affected people under applicable law.

7. EU AI rules, OECD due diligence and their jurisdictional boundaries

The EU AI Act offers a different level of analysis: obligations associated with types of AI systems and the roles of providers, deployers and other operators. In the text as amended, Article 26 sets out duties for deployers of high-risk systems, including appropriate organizational measures, human oversight and relevant notification and suspension steps. Article 25 addresses circumstances in which parties in the AI value chain may acquire provider responsibilities; Article 16 addresses providers (Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744). For a German participant, these provisions may become legally relevant where the regulation's subject-matter and territorial requirements are satisfied. For a Nepalese operating company, mere purchase from a European firm does not automatically establish that it is subject to every EU deployer rule. Territorial reach, system classification and the role performed must be examined separately.

Temporal accuracy is particularly important. Regulation (EU) 2026/1744, the Digital Omnibus on AI, was adopted on 8 July 2026 and entered into force on 27 July 2026. As amended, the high-risk provisions are scheduled to apply from 2 December 2027 for the Annex III pathway and 2 August 2028 for the Annex I product-related pathway (Regulation (EU) 2026/1744, amending Regulation (EU) 2024/1689). Other provisions have different commencement dates. It would be misleading to describe all high-risk obligations as uniformly enforceable on 18 October 2026 or to treat a proposed compliance practice as equivalent to a currently operative obligation. The AI Act's warning and deployment procedures can nevertheless inform prospective contract design; their value in the Nepalese setting is that they distinguish who created the system, who uses it, who controls inputs and who can suspend operation.

The OECD Due Diligence Guidance for Responsible AI, published on 19 February 2026, is presented as practical guidance to enterprises for implementing OECD responsible-business-conduct standards and the OECD AI Principles (OECD 2026). Its detailed treatment of business relationships should be read in the guidance itself; this article uses it only as a general operational vocabulary for the vendor-parent-subsidiary chain. Yet it is guidance, not a free-standing Nepalese liability statute. Similarly, the NIST AI Risk Management Framework, with its govern, map, measure and manage functions, is



designed as voluntary risk-management assistance (NIST 2023). Corporate boards may choose to adapt those functions but an author may not convert the act of choosing a voluntary standard into proof that a domestic regulator has mandated it.

A useful synthesis is therefore triangular. Corporate law identifies a competent organizational decision-maker; AI-specific regulation, where applicable, assigns operational responsibilities to the provider and deployer; voluntary due-diligence guidance helps design workable processes that may extend beyond the minimum binding rule. Conflating these levels causes two opposite errors. One is under-regulation by assuming that a procurement contract entirely substitutes for statutory responsibilities. The other is over-regulation by claiming that broad AI principles create identical enforceable duties in every jurisdiction. Accurate comparison demands an explicit status column for each rule: binding domestic law, binding cross-border instrument if applicable, persuasive foreign case, contractual duty or voluntary guidance.

8. A rights-and-information architecture for outsourced deployment

The proposed governance architecture begins with a responsibility map created before procurement. The first column names the deploying legal entity, the system's consequential use and the individual officer who owns the deployment decision. The second identifies the parent or group purchasing actor and the source of its contractual authority. The third names the vendor or integrator that generates testing reports, system change notices, security events and incident warnings. The fourth locates the people with power to pause, override, investigate and remedy the system. This map is meant to prevent the frequent confusion between an individual who receives reports and an entity that possesses legal authority to act on them.

Information disclosure should be proportionate to the problem and to legitimate vendor security and confidentiality interests. An initial triage tier should require a dated incident identifier, affected version or use, risk category, severity, relevant limitations, interim controls and a responsive contact. A validation tier can provide testing assumptions, error characteristics, remediation evidence and redacted audit results to authorized personnel under appropriate safeguards. Detailed model artefacts, sensitive personal information or trade-secret material should be accessible only where justified by contract or law, potentially through a controlled independent review. This is a proposed tiered contractual design, not an assertion that Nepalese company law currently compels any such disclosure.

Information rights must then be designed around credible alerts rather than unlimited access. For a material risk, an appropriate vendor notice might identify the affected system version, the date and scope of the event, the evidentiary basis for concern, likely consequences for the deploying use, known limitations, recommended mitigation and a secure channel for follow-up. The exact payload must be proportionate and consistent with privacy, trade-secret and cybersecurity concerns. Complete training datasets or source code will often be unnecessary for initial triage, whereas model version and exposure date can be indispensable. Rights of independent validation and escalation after a disputed report are more valuable than an unenforceable promise of absolute transparency.

The operating entity must have a usable route to receive a defined warning and act on it. If the parent signs the vendor agreement, options include direct vendor notice, a locally enforceable third-party benefit or a binding parent-to-subsidary reporting covenant. The alternatives are not interchangeable: privity may block enforcement, a group covenant may lack practical remedies and confidentiality or security law may restrict disclosure. The subsidiary's board should record who may compel evidence and who may suspend deployment. Where no corporate group relationship exists, the analysis must revert to an arm's-length contract, not presume a parent-level fiduciary channel.



Escalation thresholds should distinguish three categories. A routine performance observation may remain with the operational product owner subject to trend monitoring. A substantiated compliance warning affecting a consequential decision may require urgent management review, documented interim safeguards and notice to an appropriate board committee when materiality criteria are met. A credible threat of unlawful or serious irreparable harm may justify immediate suspension by a previously designated officer, with board notification and regulator reporting only where applicable law requires it. The categories are recommendations, not alleged statutory classifications. Each institution should document the severity assessment, affected population and practical authority before applying them.

8.1. A consequence-sensitive escalation rule

A workable allocation rule has five inputs: the gravity and reversibility of foreseeable harm (H), the reliability of the warning (R), the actor's practical control over use or suspension (C), the time available before further exposure (T) and the cost of an interim safeguard (K). These are decision variables, not statutory elements or numerical risk scores. When H and R are high, T is short and an authorized actor can impose a reversible safeguard at tolerable K, an immediate documented intervention is ordinarily preferable to awaiting a complete root-cause report. When R is weak, H modest and the safeguard itself threatens service continuity, verification with heightened monitoring may be preferable. A missing C changes the first required act: urgent escalation to the entity holding authority, not unilateral action beyond delegated powers.

This rule also explains which capacity is the binding constraint. If a parent possesses reliable testing data but the Nepalese operator cannot obtain it, expanding the operator's board committees will not cure the evidence-access failure. If the warning reaches the operator but no person can lawfully pause the system, buying a fuller vendor report will not solve the authority failure. If both conditions exist yet the next deployment continues unchanged, the defect is execution and auditability. The model therefore recommends a different remedy for each observed failure instead of treating all outsourcing hazards as calls for more meetings. A regulator's independent intervention remains a possible substitute when its powers, response speed and sectoral remit make that intervention more effective.

A complete decision record is not a ceremonial minute. It should identify the warning received, the information source and any reliability issue, decision options considered, the authority of the decision-maker, expected consequences of continuing or stopping use, alternative service arrangements, the chosen measure, deadline, follow-up owner and criteria for lifting restrictions. Recording uncertainty is part of accuracy. A board that has been told only that a vendor identified a 'possible model anomaly' cannot truthfully minute a conclusion that the model is safe without documenting what tests and explanations supported that finding. Equally, a board may reasonably decide not to suspend an essential service where a narrower manual review can manage uncertainty.

The proposed measure of success is not the number of vendor notifications. Useful process indicators include the proportion of consequential systems with designated legal owners, share of material warnings transmitted to those owners, time from verified warning to authorized decision, proportion of closure decisions independently reviewed and availability of a timely complaint route. Those are proposed metrics only: no observed Nepalese rates are supplied. A system that produces many alerts but no decisions could be less effective than a carefully calibrated channel producing fewer, higher-quality notices. Data collection should include false-positive and false-negative patterns and must not incentivize managers to suppress notifications simply to improve nominal timeliness.



Cover Page



This architecture connects law, management and policy without collapsing them. Law specifies which actor may demand information or be sued. Contract and organizational design determine whether that actor will learn of a material problem in time. Management systems determine whether an alert produces a proportionate decision. Public policy specifies when external oversight or user remedies are needed because private governance alone cannot protect affected interests. Economic reasoning constrains reporting to the value of information and the cost of delay. Developmental concerns require an implementation path that works for organizations without specialist AI departments.

8.2. A competence-first rule and the minimum sufficient correction

The capacity framework becomes decisional when legal competence is treated as a threshold rather than a score to be offset by other strengths. The first inquiry is whether the operating company, its manager, a parent or a sector regulator is lawfully entitled to obtain or act upon the particular information. No combination of technical confidence and managerial urgency authorizes a person to exercise a power it does not possess. Once the competent actor is identified, the decision moves through three stages: secure the least information sufficient to distinguish a credible material problem from background noise; authorize a reversible protective response proportionate to the likely harm and time available; and designate an accountable owner to test the response and decide whether the deployment can safely resume. This ordering distinguishes a legal constraint from a management preference. It does not convert the proposed stages into a statutory negligence test applicable in any comparator jurisdiction.

A warning therefore need not travel through every corporate tier to be actionable. If the Nepalese operator possesses a direct contractual right to a usable incident notice and a manager lawfully empowered to suspend the feature, a foreign parent's additional review may add assurance but is not a condition of timely intervention. If the parent alone holds the information right, local technical competence does not repair the notice bottleneck; the minimum correction is a legally supportable transmission mechanism rather than an enlarged board committee. Conversely, where a local regulator can impose an effective protective order on independently obtained information, public supervision may substitute for a missing private audit covenant. The principle is functional substitutability of *routes* to protection, not interchangeability of legal duties or defendant identities.

The escalation threshold must also contain an explicit stopping rule. For low-consequence reversible uses, routine logging, periodic review and a delegated operational owner may be proportionate even when the supplier's notice is uncertain. For a materially consequential use with credible evidence and an affordable reversible safeguard, authorized interim restriction is the presumptive managerial response pending examination; any decision to continue use should identify the countervailing harm of suspension and the alternative protections selected. For a severe but poorly evidenced allegation, the proper response may be accelerated evidence preservation and targeted precaution rather than automatic shutdown. These distinct outputs follow from the interaction of expected harm, warning reliability, reversibility, actual control and response time, not from the fashionable label attached to the AI system.

The hard counterexample is a vendor that delivers a flawless warning to the correct legal entity while the local board intentionally ignores reliable evidence of grave harm. Better clauses cannot correct that failure; the problem lies in decision and execution and any legal responsibility must be assessed under the forum's actual duty and remedial rules. The converse counterexample is a diligent board prevented by mandatory confidentiality restrictions from receiving model internals but able to suspend use based on externally observed outcomes. It may provide stronger protection without source-code access. A research design that records only the existence of vendor audit rights would misclassify both cases. Relevant observations



are the legally permissible signal, time to authorized intervention, effectiveness of the chosen safeguard and documented reason for resumption.

Worked decision outputs (hypothetical, not findings of statutory liability)

Configuration	Binding constraint and proportional decision	Test for a failure of the theory
Parent-held contract; credible severe warning	Secure a valid route to the Nepalese deployer; designate local interim authority; preserve implementation proof.	If a regulator or independent evidence reliably secures protection without a local vendor claim, private audit privacy is not indispensable.
Direct low-impact purchase; uncertain update notice	Delegate monitored response; no automatic director escalation or external audit.	If low-cost routine monitoring consistently misses serious defects, the threshold is too permissive.
Direct high-impact deployment; urgent credible warning	Authorized reversible restriction pending focused investigation, then independently tested resumption.	If restriction itself foreseeably causes greater irreversible harm, the decision must evaluate a safer alternative.

9. Three hypothetical configurations and disconfirming tests

Consider first a wholly owned Nepalese financial-services subsidiary, using a hypothetical screening model licensed under a foreign parent's master agreement. The external provider sends the parent a credible notice that a software update may have increased false rejections for a subgroup. The parent's technical team decides more investigation is necessary and does not notify the subsidiary. Several weeks later, the subsidiary's customer-service unit observes complaints but cannot identify the cause. This sequence is invented to test governance responsibility, not reported as a documented event. Its significance is the mismatch between contractual access and deployment control. Under the proposed model, the local operating entity should be a recipient of relevant material warnings and its manager should have authority to initiate manual review or temporary suspension pending evidence.

The legal conclusion from that scenario must remain limited. It does not establish a violation of Nepalese company law, financial regulation, consumer law or data law without knowing the actual entity, sector, legislation, board knowledge, damage and remedial route. It would be equally wrong to claim that Delaware directors of the parent necessarily breached their oversight duties merely because a message was delayed. However, the scenario exposes an avoidable structural vulnerability: the person responsible for local service outcomes may be unable to obtain the evidence needed to act. If authenticated group contracts and reports showed that the subsidiary already received the warning promptly and reasonably responded, the proposed premise of information failure would be falsified in that instance.



Institutional diagnostic matrix 1. Proposed document tests for the three hypothetical AI configurations (not observed outcomes).

Input / actor	Decision gate / test	Evidence and permissible output
Nepal subsidiary / parent / vendor	Who has legal privity and a right to the warning?	Executed agreements and permitted disclosure chain; classify as direct right, mediated right or unsupported expectation.
Incident affecting consequential AI	Does the warning identify a material deployment-specific risk?	Version, affected users, evidence quality and severity; log scope and urgent controls.
Named manager and board	Who can restrict, suspend, correct or resume use?	Articles, delegations and escalation threshold; record authorized decision and timestamp.
Follow-up and vendor response	Was correction implemented and independently checked?	Incident file, vendor reply, operator action and residual risk; do not equate minutes with effectiveness.

The matrix separates lawful access, decision competence and follow-through. Each output is a proposed documentary test, not evidence of actual Nepalese deployment.

In the second configuration, a Nepal-incorporated small enterprise contracts directly with a vendor to assist in routine inventory forecasting. The vendor issues a low-confidence model-update notice. No customer entitlement or legal compliance issue is identified and the enterprise maintains a simple monitoring spreadsheet with a manager who can revert to manual forecasts. Escalating every such notice to directors or commissioning external model audits would likely impose costs out of proportion to identifiable harm. The example shows why 'board oversight' must not become synonymous with maximum administrative activity. A proportionate arrangement could focus on periodic monitoring, simple contract terms and defined triggers for escalation if losses, legal exposure or safety concerns become material.

A future evaluation should test the architecture against adverse as well as favorable cases. It could purposively select Nepal-incorporated deployers with direct vendor contracts, parent-held contracts and franchise-like arrangements, while varying enterprise size and system consequence. For each legally accessible incident, researchers would code notification timing, contractual access right, decision-owner identity, escalation threshold, power to suspend, substantive decision, response latency and documented follow-up. Repeated incidents could be compared within the same organization to reduce variation in governance culture but the small, nonrandom design would not establish a population-level causal effect. Disconfirming cases include timely access without meaningful action, substantive action without a formal board route and excessive compliance cost for low-risk uses.

Across the three configurations, the same structured questions yield different answers. What harm is reasonably foreseeable? Who received the source warning? Which entity is the deployer? What contractual rights exist? Who can stop or correct the system? Who should hear from users and who is authorized to disclose personal information? Which action is feasible given



resources and the importance of continuing service? Comparing those answers is more analytically useful than counting the number of countries with AI-policy statements. It also yields disconfirming possibilities: a direct purchaser may already have adequate controls; a parent-subsidiary configuration may have extensive audit access; or a regulator may provide a more effective complaint mechanism than corporate internal review.

9.1. Fixed-warning comparison and an adverse case

Hold the technical alert constant: the vendor reports a credible, time-sensitive defect affecting a consequential customer classification. In the parent-procured subsidiary, the first corrective act is a contractually permissible transfer of the alert to the Nepalese deployer, followed by a local decision about interim manual review. In the direct-purchase company, no parent transmission link exists, so the chief concern is whether its own operational officer has sufficient delegated authority to suspend or mitigate. In the franchise-like arrangement, a foreign brand's model mandate may conflict with the local operator's risk duty; the operator must identify who can modify use without breaching the governing commercial instrument and pursue the lawful escalation route. These are three different binding constraints under identical assumed warning severity, not three claims of existing statutory liability.

Now vary one fact against the thesis. Suppose an independent and competent sectoral regulator promptly requires the same protective measure even though the vendor contract denies local audit access. A low-friction regulatory order could achieve better practical protection than the proposed private information right. The argument that every deployer requires the same contractual entitlement would then fail; what survives is the narrower claim that every consequential risk needs a lawful and timely route from credible information to a competent protective decision. The diagnostic test is thus also capable of recommending a noncorporate solution.

The empirical falsification strategy should compare failures as well as successes. A future documentary study could select cases in which a verified provider warning reached an operating manager, cases in which a parent received the warning but the subsidiary did not and negative cases in which a warning prompted timely suspension or justified continuation. For each, the researcher would preserve contemporaneous documents identifying notification timestamp, recipients, contract rights, responsible authority, any expert validation, decision timestamp, remedial action and subsequent adverse or non-adverse outcome. Without comparable exposure, sector, deployment scale and risk severity, incident rate differences cannot support a causal inference. Under that design, evidence that directors received complete warnings but still lacked corrective power would weaken an information-access-centered theory and favor the institutional-capacity rival; evidence of adequate control without additional paperwork would weaken any argument for a universal reporting architecture.

The scenarios reveal the limit of the current research. An illustration can uncover logical gaps but it cannot establish prevalence, cost effectiveness or actual doctrinal compliance. Before claiming a real case, a researcher must identify the company and contract, authenticate incident timing, inspect relevant notices and decision records, protect personal data, distinguish allegations from findings and seek contrary evidence. The article therefore makes no statement that a specific Nepal-based platform has operated a defective AI screening system. It proposes a replicable documentary investigation for a later empirical stage, including negative cases in which the reporting system worked.

10. Costs, rival explanations and development constraints

The strongest rival explanation to an information-chain thesis is that the central problem is not missing board information but poor substantive regulation or insufficient operational expertise. A company can perfectly transmit a wrong vendor



Cover Page



assurance. The local directors may lack the scientific capability to challenge it and the board's options may be limited by dependence on a single supplier. Reporting architecture is then necessary but insufficient. An effective design needs independent expertise where the consequences warrant it, contractually meaningful rights to commission tests and regulator access to relevant evidence when authorized. The recommendation is a layered governance response, not a claim that documentation alone makes AI trustworthy.

A second rival is that industry regulators, rather than company boards, should be the principal oversight institution. A finance or health authority may possess powers unavailable to a corporate board and may protect people whose interests are not represented by shareholders. This argument is compelling for publicly significant systems. Yet external regulators usually cannot decide every daily supplier configuration or procurement renewal. The potential complementarity is straightforward: a company should manage immediate risks within its control, while public institutions set minimum standards, investigate systemic harm and provide public-law remedies when legally mandated. This allocation also avoids pretending that board fiduciary duties necessarily create direct claims for every affected user.

A third challenge is economic. Effective incident reporting has fixed costs: contract negotiation, translation into locally usable notices, information-security controls, documentation, staffing and periodic testing. Its marginal costs rise with the number of systems and vendor updates. For a small Nepalese enterprise, the question is not whether perfect assurance would be valuable in principle but which evidence materially improves a consequential decision. The proposed risk-tier method is an attempt to limit unnecessary burdens. Nonetheless, this manuscript contains no Nepal-specific cost survey, willingness-to-pay estimate, incident-frequency dataset or causal cost-benefit calculation. It cannot quantify an optimal threshold. Future fieldwork would need to capture firm size, sector, language and connectivity constraints, vendor concentration and the costs of both system interruption and unremedied harm.

Cost-benefit analysis must distinguish obtaining an enforceable warning right, translating technical information for local decision-makers, preserving an auditable response and maintaining capacity to act. The relative expense of these functions depends on vendor concentration, contract negotiation power, sectoral risk and internal staff. No verified Nepalese cost series or vendor price comparison was available here. Accordingly the article does not claim that the proposed system is cost-effective. A proportionate pilot could record baseline warning frequency, delivery delay, human review time, contract costs and incidents requiring suspension. Those measurements would permit comparison against less elaborate incident-reporting and regulator-led alternatives without assuming the preferred architecture performs best.

The development implications run in both directions. Well-designed warning rights may protect consumers and small firms from risks hidden in global digital supply chains. Conversely, obligations that are too complex or expensive may consolidate large vendors' advantage, exclude local innovators and discourage use of potentially beneficial tools. Group parents may be willing to share incident summaries but reluctant to disclose valuable intellectual property or data that identify other customers. A proportional scheme must therefore protect confidentiality, permit third-party assurance under safeguards and prioritize records needed for decisions. Otherwise, a nominal accountability reform could make Nepal-linked enterprises more dependent on the same suppliers it seeks to discipline.

Transferability is bounded by legal form, evidence access and corporate role. German stock-corporation law allocates risk reporting among distinct organs and has listed-company-specific controls; Delaware oversight litigation depends on pleading, bad faith and particular facts. Neither creates a Nepalese fiduciary duty or guarantees vendor disclosure. Shiman



(2025) cautions that Caremark pleading patterns vary. The architecture advanced here is therefore a context-sensitive contractual and managerial hypothesis, not a universal liability checklist.

A discriminating rival-explanation test would compare cases with comparable vendor-risk severity but different contractual access and local delegation. If incidents are resolved equally quickly without direct evidence rights, technical skill or an effective sector regulator may explain performance better than the proposed architecture. Conversely, documented warnings that remain unaddressed despite technical capacity would support an authority-and-transmission explanation. This comparison cannot establish which account predominates without real organizational records.

11. Reform sequence, accountability test and conclusions

A feasible first stage is contractual and organizational. A Nepalese company purchasing consequential AI should identify the system's use and legal owner, seek contractually grounded, privacy-proportionate access for the local operating entity to receive material vendor warnings, assign a manager with authority to apply interim controls and adopt a board-escalation trigger based on materiality rather than technical novelty. Before committing to a contract, the company should confirm how model updates are identified, what records can be retained, whether warnings can be independently challenged and who can authorize an emergency workaround. Where the parent procures centrally, these rights should be reflected in an enforceable arrangement among the relevant parties, subject to local legal review.

11.1. Three-tier implementation sequence

Tier 1 (procurement and ownership): the parent, vendor and local deploying entity document the recipient of material notices and identify the person legally authorized to restrict use; the threshold is a consequential system entering operation or a material contract renewal. Tier 2 (operational assurance): the local risk owner maintains decision logs, measures alert-to-receipt and receipt-to-mitigation times, tests one simulated warning annually when feasible and escalates incidents that remain unresolved beyond a risk-calibrated interval. Where the chain fails, the relevant contract party funds the reporting interface rather than charging each small operator for duplicate full audits. Tier 3 (sectoral learning): a competent regulator may evaluate anonymized failures and consider proportionate notification or retention duties only where existing powers and documented harm warrant them. Success is a timely, lawful mitigation, not the number of forms completed; trade-secret and privacy limitations govern each tier.

A public-policy stage would allow relevant sector regulators, within statutory competence, to clarify recordkeeping and notifications for high-impact deployments while protecting trade secrets and privacy. New mandatory duties require an enacted authority, defined scope and remedies. Their costs and benefits remain untested.

The comparative result can therefore be stated as a minimum-correction principle: identify the first missing lawful link between signal, competent choice and implemented protection and repair that link before adding new reporting layers. Extra evidence is useless without usable authority; more authority is dangerous without bounded information; and minutes alone cannot establish completed mitigation. The test accommodates public-law substitutes, confidentiality constraints and proportionate non-escalation, thereby avoiding the claim that every outsourced system warrants the same board-level response.

The comparison supports a specific institutional proposition rather than a generalized AI-board liability theory. A credible warning is actionable only when it can travel lawfully to a legally competent decision-maker and generate an operational



response whose adequacy can later be tested. German AG organ rules, Delaware's stringent oversight cases and the Nepalese company-law provisions allocate different duties and remedies; none can be transplanted as binding law elsewhere. The capacity test identifies whether evidence, authority or execution is missing and the consequence-sensitive rule determines whether the appropriate first response is disclosure, delegated intervention, independent supervision or proportionate monitoring. The two findings explain why an inventory-forecasting update and a credible discriminatory screening alert should not attract identical governance machinery. Neither establishes a breach in a constructed case without the applicable legal predicates.

The unresolved empirical question is whether a rights-and-information architecture would improve outcomes across differently resourced Nepalese companies. That effectiveness question cannot be answered by the legal texts or three invented stress tests. It requires authentic organizational records, careful legal verification, disciplined case selection and observation of decisions rather than policy texts. Until then, the contribution is a conditional design proposition: when the entity using AI can access relevant warnings and exercise remedies at proportionate cost, outsourcing need not become an accountability void. When that entity has neither legal access nor practical control, additional declarations of board responsibility are unlikely to be enough.

References

1. Dana, Joshua (2025), 'Performative Actions and Profits: A New Test for Delaware Derivative Oversight Claims', Brooklyn Law Review 90(2). <https://brooklynworks.brooklaw.edu/blr/vol90/iss2/6/>
2. Delaware. In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996). <https://law.justia.com/cases/delaware/court-of-chancery/1996/13670-3.html>
3. Delaware. In re McDonald's Corporation Stockholder Derivative Litigation, C.A. No. 2021-0324-JTL, opinions of 25 January 2023 and 1 March 2023. <https://courts.delaware.gov/Opinions/Download.aspx?id=344560>
4. Delaware. In re The Boeing Company Derivative Litigation, C.A. No. 2019-0907-MTZ (Del. Ch. 7 September 2021). <https://law.justia.com/cases/delaware/court-of-chancery/2021/c-a-no-2019-0907-mtz-0.html>
5. Delaware. Marchand v. Barnhill, 212 A.3d 805 (Del. 2019). <https://courts.delaware.gov/Opinions/Download.aspx?id=291200>
6. Delaware. Stone v. Ritter, 911 A.2d 362 (Del. 2006). <https://law.justia.com/cases/delaware/supreme-court/2006/84060.html>
7. European Union. Regulation (EU) 2024/1689 (Artificial Intelligence Act), as amended including by Regulation (EU) 2026/1744. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>; <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>
8. Germany. Aktiengesetz, §§90, 91 and 93. Official federal legislative database. <https://www.gesetze-im-internet.de/aktg/>
9. Ishkhanyan, Artur (2026), 'Governing AI across Borders: Corporate Power, State Sovereignty and Global Regulation', Digital Policy, Regulation and Governance 28(3), 280–295. <https://doi.org/10.1108/DPRG-03-2025-0057>
10. National Institute of Standards and Technology (2023), Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1. <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>
11. Nepal. Companies Act 2063 and Companies (First Amendment) Act 2074. Nepal Law Commission statutory repository (original-language consolidation and section-specific amendment effect subject to further checking). <https://repository.lawcommission.gov.np/np/category/documents/prevaling-law/statutes-acts/>
12. OECD (2026), OECD Due Diligence Guidance for Responsible AI. Paris: OECD Publishing. <https://doi.org/10.1787/41671712-en>
13. Passador, Maria Lucia (2025), 'Governance Gambits and Business Judgment in In/Out-Sourcing Tactics', American Business Law Journal 62(3), 191–216. <https://doi.org/10.1111/ablj.70001>



Cover Page



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:10(1), October 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in
<https://doi.org/14.10/ijmer.10.2026>

14. Shiman, Yehonatan (2025), 'The Politics of Oversight: Caremark, Corporate Purpose and Delaware's Judicial Landscape', *American Business Law Journal* 62(3), 165–189. <https://doi.org/10.1111/ablj.70003>
15. Zhao, Jingchen (2024), 'Promoting More Accountable AI in the Boardroom through Smart Regulation', *Computer Law & Security Review* 52, 105939. <https://doi.org/10.1016/j.clsr.2024.105939>
16. Nepal Law Commission, Companies Act 2063, published original Nepali §99(4)–(5) original-text recovery distinction (current amendments separately to be checked).
<https://repository.lawcommission.gov.np/np/category/documents/prevailing-law/statutes-acts/कम्पनी-ऐन-२०६३-statutes-acts/>